



IMiS<sup>®</sup> / ARChive Server  
Priručnik

Verzija 10.3.2210

**IMAGING  
SYSTEMS**

Imaging Systems, informacijski sistemi, d.o.o.

Brnčičeva 41g

Ljubljana

## KAZALO VSEBINE

1	PREDGOVOR .....	13
1.1	O dokumentaciji .....	13
1.2	Ciljno občinstvo.....	13
1.3	Konvencije .....	13
1.4	Kratice in pojmi .....	14
2	UVOD .....	18
2.1	Predstavitev.....	18
2.2	Označevanje različic .....	19
2.3	Funkcionalnosti .....	22
2.4	Novosti v različici.....	24
3	TEHNIČNA DOKUMENTACIJA.....	26
3.1	Arhitektura strežnika.....	26
3.2	Atribut .....	33
3.2.1	Vrste atributov .....	34
3.2.2	Parametri atributov .....	42
3.2.3	Povezava s predlogami.....	44
3.2.4	Poimenovanje.....	49
3.2.5	Sistemske atributi .....	50
3.2.6	Atributi dokumentov elektronske pošte .....	63
3.2.7	Atributi upravljanja s fizičnim gradivom.....	66
3.2.8	Atributi prenesenega gradiva .....	70
3.2.9	Atributi politik hrambe in zadržanj .....	74
3.2.10	Atributi postopkov odbiranja in izločanja .....	78
3.2.11	Atributi verzioniranega gradiva.....	82
3.3	Entiteta.....	83
3.3.1	Vrste .....	84
3.3.2	Hierarhija.....	85
3.3.3	Komponente.....	86
3.3.4	Predloge.....	87
3.3.5	Dostopi.....	88
3.3.6	Identifikatorji .....	105
3.3.7	Življenjski cikel .....	109
3.3.8	Revizijska sled.....	123
3.3.9	Roki hrambe.....	137
3.3.10	Upravljanje z vsebinami .....	141
3.3.11	Reference .....	147
3.3.12	Kategorije.....	147
3.4	Razvrščanje .....	150

3.4.1	Klasifikacijske oznake.....	151
3.4.2	Nastavitve načrta razvrščanja gradiva.....	151
3.4.3	Premikanje gradiva v načrtu razvrščanja (reklasifikacija).....	153
3.5	Iskanje .....	155
3.5.1	Varnost in zaščita podatkov pri iskanju .....	155
3.5.2	Pravila iskalnega niza.....	156
3.6	Avtentičnost .....	160
3.6.1	Predpogoji.....	160
3.6.2	Koncept.....	161
3.6.3	Shramba digitalnih potrdil .....	164
3.6.4	ERS.....	169
3.6.5	AIP .....	190
3.6.6	Časovno žigosanje .....	196
3.6.7	Pravila .....	201
3.7	Odbiranje in izločanje .....	204
3.7.1	Postopek priprave za odbiranje in izločanje .....	205
3.7.2	Postopek odločanja pri odbiranju in izločanju.....	207
3.7.3	Izvedba postopka odbiranja in izločanja.....	207
3.7.4	Postopek filtriranja.....	210
3.7.5	XML format dokumentov .....	211
3.8	Imeniške storitve.....	220
3.8.1	Tipi.....	221
3.8.2	Sistemske določene entitete.....	223
3.8.3	Komponente entitete.....	224
3.8.4	Sinonimi.....	227
3.8.5	Avtentikacija.....	227
3.8.6	Življenjski cikel entitet imenika.....	239
3.8.7	Sinhronizacija.....	241
3.8.8	Vtičniki.....	243
3.9	Varnostno kopiranje in obnovitev podatkov .....	261
3.9.1	Varnostno kopiranje.....	266
3.9.2	Obnovitev podatkov .....	266
3.9.3	Primer.....	268
3.9.4	Težave pri obnovitvi podatkov .....	268
3.10	Skladiščenje vsebine .....	270
3.10.1	Profili .....	271
3.10.2	Volumni.....	273
3.11	Verzioranje .....	274
4	SISTEMSKÉ ZAHTEVE.....	276
4.1	Strojna oprema.....	276

4.1.1	Načrtovanje procesorske moči strežnika.....	276
4.1.2	Načrtovanje pomnilniških kapacitet strežnika.....	276
4.1.3	Načrtovanje diskovnih kapacitet strežnika .....	277
4.1.4	Komunikacijske poti .....	278
4.1.5	Priklop na mrežno opremo .....	278
4.1.6	Administratorske pravice .....	279
4.1.7	Nadzor delovanja strojne opreme .....	279
4.1.8	Minimalne zahteve.....	279
4.1.9	Priporočene zahteve .....	280
4.2	Programska oprema.....	281
4.2.1	Operacijski sistemi .....	281
4.2.2	Minimalne zahteve.....	281
4.2.3	Priporočene zahteve .....	282
4.2.4	Seznam obveznih sistemskih orodij.....	283
4.2.5	Seznam obveznih sistemskih knjižnic.....	283
5	NAMESTITEV .....	284
5.1	Postopek namestitve .....	284
5.2	Ponamestitveni postopki .....	287
5.2.1	Nastavitev števila hkrati odprtih datotek.....	287
5.2.2	Nastavitev samodejnega zagona.....	288
5.3	Preizkušanje namestitve in nastavitev .....	289
6	NADGRADNJA.....	290
6.1	Postopek nadgradnje .....	290
6.2	Možni zapleti pri nadgradnji.....	292
7	ODSTRANITEV .....	294
7.1	Postopek odstranitve.....	294
8	UPRAVLJANJE PRODUKTA.....	296
8.1	Postopek zagona in zaustavitve.....	296
8.2	Konfiguriranje .....	297
8.2.1	Predvidena opravila .....	298
8.3	Beleženje dogodkov delovanja.....	300
8.3.1	Postopki konfiguriranja s konzolnimi orodji .....	302
8.4	Administracija.....	305
8.4.1	Konfiguracijska datoteka iarc.conf.....	306
8.5	Administracijski vmesnik .....	315
8.5.1	Urejanje nastavitev strežnika.....	315
8.5.2	Prijava in odjava.....	325
8.5.3	Konfiguriranje strežnika.....	331
9	ODPRAVLJANJE TEŽAV .....	425
9.1	Kako se težavam izognemo? .....	425

9.2 Pogoste težave.....	426
9.3 Redkejšje težave .....	435
9.4 Seznam napak storitve, ki se beležijo v dnevnik delovanja .....	439
9.4.1 Nivo 0 – Emergency .....	439
9.4.2 Nivo 1 – Alert .....	439
9.4.3 Nivo 2 – Critical.....	439
9.4.4 Nivo 3 – Error .....	440
9.4.5 Nivo 4 – Warning.....	455

## KAZALO SLIK

V nadaljevanju je uporabniku na voljo seznam slik uporabljenih v tem priročniku.

Slika 1: Shematični prikaz arhitekture strežniške komponente IMiS®/ARChive Server .....	26
Slika 2: Logične povezave med atributi, predlogami in entitetami .....	44
Slika 3: Delovanje ACL.....	89
Slika 4: Hierarhija z razredom, zadevo in dvema dokumentoma .....	100
Slika 5: Življenjski cikel entitete .....	110
Slika 6: Življenjski cikel instance entitete v delovnem spominu strežnika .....	112
Slika 7: Umeščanje entitete v postopku za zagotavljanje avtentičnosti dolgoročno arhiviranih podatkov .....	160
Slika 8: Delovanje zgoščevalne funkcije .....	162
Slika 9: Generiranje in preverjanje elektronskega podpisa.....	162
Slika 10: Veriga digitalnih potrdil.....	164
Slika 11: Postopek dodajanja digitalnega potrdila v shrambo.....	165
Slika 12: Ustvarjanje AIP za postopek ustvarjanja dokazil.....	169
Slika 13: Podaljševanje zanesljivosti dokazil .....	170
Slika 14: Primer preverjanja avtentičnosti podatkov .....	170
Slika 15: Postopek časovnega žigosanja posameznega AIP-ja .....	171
Slika 16: Postopek časovnega žigosanja z uporabo Merklovega drevesa .....	172
Slika 17: Postopek enostavnega podaljševanja v kombinaciji z ustvarjanjem dokazil .....	173
Slika 18: Del postopka kompleksnega podaljševanja, opisanega v točkah 2, 3 in 4 .....	174
Slika 19: Primer Merklovega drevesa .....	176
Slika 20: Primer reduciranega drevesa za vozlišči H1 in H2.....	177
Slika 21: Enostavno podaljševanje arhivskega časovnega žiga.....	185
Slika 22: Postopek obdelave AIP in pripadajočega ERS .....	187
Slika 23: Postopek kompleksnega podaljševanja z Merklovim drevesom .....	187
Slika 24: Koncept vtičnikov .....	197
Slika 25: Diagram poteka izvajanja postopka odbiranja in izločanja.....	205
Slika 26: Priprava postopka odbiranja in izločanja .....	206
Slika 27: Pripadnost uporabnika v uporabniških skupinah .....	222
Slika 28: Primer gnezdenja uporabniških skupin.....	222
Slika 29: Primer napada na IMiS®/ARChive Server z vrinjenim napadalcem.....	230
Slika 30: LDAP avtentikacija .....	235
Slika 31: Kerberos avtentikacija .....	237
Slika 32: Povezovanje identitet.....	238
Slika 33: Povezava med postopki v življenjskem ciklu entitete v imeniku.....	240
Slika 34: Konfiguracijske etikete SOAP vtičnikov .....	249
Slika 35: Proces verzioniranja.....	275
Slika 36: Prikaz ikone za nastavitve strežnika.....	315

Slika 37: Seznam arhivskih strežnikov v nastavitvah.....	315
Slika 38: Zaščita nastavitve arhivskega strežnika z geslom.....	316
Slika 39: Izbira dejanja »Nov« v ukazni vrstici .....	317
Slika 40: Dodajanje arhivskega strežnika.....	317
Slika 41: Prikaz seznama po shranitvi arhivskega strežnika .....	318
Slika 42: Izbira arhivskega strežnika v načinu za urejanje .....	318
Slika 43: Pogovorno okno za urejanje nastavitve arhivskega strežnika .....	319
Slika 44: Dodajanje digitalnega potrdila za izbrani arhivski strežnik.....	319
Slika 45: Prenos digitalnega potrdila iz izbranega arhivskega strežnika .....	320
Slika 46: Dodajanje prstnega odtisa za izbrani arhivski strežnik.....	320
Slika 47: Izbira digitalnega potrdila za izbrane arhivske strežnike .....	321
Slika 48: Dodajanje in odstranitev digitalnega potrdila za izbrane arhivske strežnike.....	322
Slika 49: Odstranitev arhivskega strežnika .....	322
Slika 50: Dodajanje IP naslova za izbrane arhivske strežnike.....	323
Slika 51: Prikaz nastavitve IP naslova v seznamu .....	324
Slika 52: Izbira arhivskega strežnika za odstranitev .....	324
Slika 53: Odstranitev arhivskega strežnika .....	325
Slika 54: Izbira arhiva iz pojavnega menija .....	326
Slika 55: Vpis uporabniškega imena in gesla v prijavno okno.....	326
Slika 56: Različica administracijskega vmesnika IMiS®/wAdmin.....	326
Slika 57: Soglasje k uporabi piškotkov.....	327
Slika 58: Prijava v strežnik.....	328
Slika 59: Osnovni prikaz po prijavi .....	329
Slika 60: Prilagoditev prikaza manjšemu oknu brskalnika .....	330
Slika 61: Odjava uporabnika.....	330
Slika 62: Konfiguracijske mape v levem meniju IMiS®/wAdmin.....	333
Slika 63: Prikaz osnovnega pregleda v mapi »Domov« .....	334
Slika 64: Pregled nastavitve v razdelku »Podrobnosti« v načinu za branje .....	335
Slika 65: Pregled sistemskih vlog in pravic dostopa do konfiguracijskih map .....	335
Slika 66: Pregled nastavitve v razdelku »Shranjevalni profil« v načinu za urejanje .....	336
Slika 67: Pregled nastavitve v razdelku »Vrste prikaza« v načinu za urejanje.....	336
Slika 68: Prikaz osnovnega pregleda v mapi »Nadzor dostopov« .....	337
Slika 69: Izbira konteksta v konfiguracijski mapi »Nadzor dostopov« .....	337
Slika 70: Prikaz osnovnega pregleda v kontekstu prikaza po meri.....	338
Slika 71: Dodajanje nove imeniške entitete ali atributa tipa imeniška entiteta.....	339
Slika 72: Vpis iskalnega niza v iskalnik .....	339
Slika 73: Prikaz razdelkov po izbiri dejanja »Dodaj entiteto imenika«.....	340
Slika 74: Določanje dostopnih pravic do entitet za imeniško entiteto .....	342
Slika 75: Izbira atributa za določitev dostopnih pravic .....	342
Slika 76: Določanje pravic dostopa do atributov za imeniško entiteto.....	344

Slika 77: Določanje pravic dostopa za atribut tipa imeniška entiteta .....	344
Slika 78: Prikaz osnovnega pregleda v mapi »Revizijska sled«.....	345
Slika 79: Osnovne nastavitve profila .....	346
Slika 80: Seznam obveznih dogodkov revizijske sledi.....	347
Slika 81: Seznam dogodkov revizijske sledi na vsebini .....	347
Slika 82: Seznam dogodkov revizijske sledi na entiteti .....	349
Slika 83: Identifikator profila revizijske sledi .....	349
Slika 84: Prikaz osnovnega pregleda v razdelku »Osnovne nastavitve« .....	350
Slika 85: Prikaz osnovnega pregleda v razdelku »Priključki«.....	350
Slika 86: Prikaz osnovnega pregleda v razdelku »Zunanji imeniki«.....	350
Slika 87: Nastavitev parametrov v razdelku »Osnovne nastavitve«.....	351
Slika 88: Nastavitev parametrov v razdelku »Priključek« .....	352
Slika 89: Primer nastavitve priključka za dostop do zunanjega ponudnika identitete .....	353
Slika 90: Nastavitev parametrov v razdelku »Zunanji imeniki«.....	357
Slika 91: Nastavitev parametrov v razdelku »Avtentikacijska metoda«.....	357
Slika 92: Prikaz zunanjega imenika.....	358
Slika 93: Prikaz osnovnega pregleda v mapi »Vsebine« .....	359
Slika 94: Prikaz razdelka »Elektronski podpisi« v mapi »Vsebine«.....	359
Slika 95: Nastavitev parametrov v razdelku »Elektronski podpisi«.....	360
Slika 96: Prikaz razdelka »Indeksiranje besedila vsebin« v mapi »Vsebine« .....	360
Slika 97: Nastavitev parametrov v razdelku »Indeksiranje celotnega besedila« .....	361
Slika 98: Prikaz razdelka »Nastavitve upravljanja z vsebinami« v mapi »Vsebine«.....	362
Slika 99: Nastavitev parametrov v razdelku »Nastavitve upravljanja z vsebinami« .....	362
Slika 100: Prikaz razdelka »Pretvorniki« v mapi »Vsebine« .....	363
Slika 101: Nastavitev parametrov v razdelku »Pretvornik« .....	364
Slika 102: Nastavitev parametrov v razdelku »Izhodni format«.....	365
Slika 103: Prikaz pretvornika.....	366
Slika 104: Nastavitve osnovnih lastnosti in izhodnih parametrov.....	367
Slika 105: Primer pretvorbe vsebine dokumenta.....	368
Slika 106: Pretvorba iz BMP v JPG: nastavitve osnovnih lastnosti in izhodnih parametrov...	369
Slika 107: Pretvorba iz JPG v TIFF: nastavitve osnovnih lastnosti in izhodnih parametrov.....	370
Slika 108: Primer pretvorbe iz formata BMP v JPG in JPG v TIFF.....	370
Slika 109: Prikaz razdelka »Razčlenjevalniki« v mapi »Vsebine«.....	371
Slika 110: Nastavitev parametrov v razdelku »Razčlenjevalniki«.....	372
Slika 111: Prikaz razdelka »Vrste vsebin« v mapi »Vsebine« .....	372
Slika 112: Iskanje po seznamu podprtih MIME vrst vsebin .....	373
Slika 113: Iskalno polje za vpis iskalnega niza.....	373
Slika 114: Prikaz osnovnega pregleda mape »Imenik« .....	374
Slika 115: Kopiranje entitete imenika.....	375
Slika 116: Dodajanje podatkov o entiteti imenika iz odložišča .....	375



Slika 117: Prikaz osnovnega pregleda v mapi »Osnovne nastavitve«	377
Slika 118: Nastavitev parametrov v razdelku »Avtentikacija«	378
Slika 119: Nastavitev parametrov v razdelku »Imenik«	379
Slika 120: Nastavitev parametrov v razdelku »Zunanje identitete«	380
Slika 121: Dodajanje člana v skupino	380
Slika 122: Sprememba gesla	381
Slika 123: Nastavitev parametrov v razdelku »Sistemske vloge«	382
Slika 124: Nastavitev parametrov v razdelku »Konfiguracijske vloge«	383
Slika 125: Pregled efektivnih pravic za izbranega uporabnika	384
Slika 126: Prikaz osnovnega pregleda v mapi »Nestrukturirana hramba«	385
Slika 127: Nastavitev parametrov v razdelku »Shranjevalni profili«	387
Slika 128: Prikaz shranjevalnega profila	387
Slika 129: Nastavitev parametrov v razdelku »Vsebniki objektov«	388
Slika 130: Prikaz vsebnika objektov	388
Slika 131: Nastavitev parametrov v razdelku »Sinonimi vrst vsebin«	389
Slika 132: Prikaz sinonima vrste vsebine	389
Slika 133: Prikaz osnovnega pregleda v mapi »LTANS«	390
Slika 134: Nastavitev parametrov v razdelku »Nastavitve«	391
Slika 135: Nastavitev parametrov v razdelku »Ponudnik časovnega žigosanja«	392
Slika 136: Prikaz ponudnika časovnega žigosanja	393
Slika 137: Nastavitev parametrov v razdelku »Pravila časovnega žigosanja«	394
Slika 138: Prikaz pravila časovnega žigosanja	395
Slika 139: Nastavitev parametrov v razdelku »Pravila veriženja časovnih žigov«	396
Slika 140: Prikaz pravila veriženja časovnih žigov	396
Slika 141: Prikaz osnovnega pregleda v mapi »Varnost«	397
Slika 142: Nastavitev parametrov v razdelku »Javni atributi z neomejenim dostopom«	398
Slika 143: Nastavitev parametrov v razdelku »Shramba digitalnih potrdil«	399
Slika 144: Nastavitev parametra »Veljavnost hrambe digitalnih potrdil«	399
Slika 145: Prikaz lastnosti digitalnega potrdila	400
Slika 146: Prikaz seznama digitalnih potrdil	401
Slika 147: Prikaz osnovnega pregleda v mapi »Strežnik«	402
Slika 148: Izbira dejanja »Dodaj uporabljeno v«	403
Slika 149: Nastavitev parametrov shranjevalnega profila	403
Slika 150: Prikaz nastavitve volumna	405
Slika 151: Prikaz volumna v pregledu izbranega profila	405
Slika 152: Prikaz osnovnega pregleda v mapi »Atributi«	406
Slika 153: Dodajanje novega atributa	408
Slika 154: Vpis iskalnega niza v iskalno polje	409
Slika 155: Prikaz osnovnega pregleda v mapi »Šifranti«	410
Slika 156: Dodajanje novega šifranta	411

Slika 157: Prikaz osnovnega pregleda mape »Številčenje« .....	412
Slika 158: Dodajanje novega števca.....	413
Slika 159: Prikaz osnovnega pregleda v mapi »Hramba« .....	415
Slika 160: Dodajanje zadržanja uničenja.....	416
Slika 161: Dodajanje podatkov o politiki hrambe.....	417
Slika 162: Prikaz pooblastila za politiko hrambe.....	418
Slika 163: Prikaz osnovnega pregleda v mapi »Predloge« .....	418
Slika 164: Dodajanje nove predloge .....	419
Slika 165: Pregled podatkov o predlogi.....	420
Slika 166: Dodajanje ali spreminjanje podatkov in lastnosti atributa.....	422
Slika 167: Prikaz atributov povezanih na predlogo .....	423
Slika 168: Sprememba vrstnega reda atributov na predlogi .....	423
Slika 169: Prikaz podedovanih atributov povezanih na predlogo .....	424
Slika 170: Vpis iskalnega niza v iskalno polje .....	424

## KAZALO TABEL

V nadaljevanju je uporabniku na voljo seznam tabel uporabljenih v tem priročniku.

Tabela 1: Uporaba različnih stilov v dokumentaciji.....	13
Tabela 2: Uporaba kratic v dokumentaciji.....	16
Tabela 3: Seznam uporabljenih pojmov v dokumentaciji.....	17
Tabela 4: Tabela operacij in pravic .....	94
Tabela 5: Omejitev pravic vpogleda v javne metapodatke .....	96
Tabela 6: Primer konfiguracije politik hrambe.....	138
Tabela 7: Vrednosti etikete »SourceOperation« .....	144
Tabela 8: Atributi etikete »Output«.....	145
Tabela 9: Atributi etikete »Provider«.....	145
Tabela 10: Kategorizacija (primer 1).....	148
Tabela 11: Kategorizacija (primer 2).....	148
Tabela 12: Kategorizacija (primer 3).....	149
Tabela 13: Kategorizacija (primer 4).....	149
Tabela 14: Kategorizacija (primer 6).....	150
Tabela 15: XML elementi etikete »EvidenceRecord« .....	178
Tabela 16: XML elementi etikete »ArchiveTimeStampChain« .....	179
Tabela 17: XML elementi etikete »ArchiveTimeStamp« .....	180
Tabela 18: XML elementi etikete »Sequence«.....	181
Tabela 19: XML elementi etikete »TimeStamp« .....	182
Tabela 20: Podprti tipi časovnih žigov .....	182
Tabela 21: Podprti tipi kriptografskih elementov .....	182
Tabela 22: XML elementi etikete »Header«.....	190
Tabela 23: Interpretacija AIP v odvisnosti od vrednosti atributa »Version« .....	191
Tabela 24: XML elementi etikete »Attribute«.....	192
Tabela 25: XML elementi etikete »Digest« .....	192
Tabela 26: Algoritmi in pripadajoči URI .....	193
Tabela 27: XML elementi etikete »Signature«.....	194
Tabela 28: XML elementi etikete »RevocationData«.....	195
Tabela 29: Podprti tipi informacij o preklicu digitalnih potrdil .....	196
Tabela 30: XML elementi etikete "Review" .....	212
Tabela 31 XML elementi etikete "Header".....	212
Tabela 32: XML elementi etikete "Entity" .....	213
Tabela 33: Pozicija bitov ki predstavljajo dovoljene akcije.....	214
Tabela 34: Elementi etikete »Review«.....	215
Tabela 35: Elementi etikete »Header« .....	216
Tabela 36: Elementi etikete »Entity« .....	217
Tabela 37: Elementi etikete »Report« .....	218

Tabela 38: Elementi etikete »Header« .....	219
Tabela 39: Elementi etikete »Entity« .....	219
Tabela 40: Skupne konfiguracijske etikete LDAP vtičnikov .....	247
Tabela 41: Konfiguracijske etikete Active Directory vtičnika .....	247
Tabela 42: Konfiguracijske etikete SQL vtičnikov .....	248
Tabela 43: Konfiguracija preslikovalnih polj .....	250
Tabela 44: Tipi preslikav .....	251
Tabela 45: Vrednosti »typeExt« atributa .....	252
Tabela 46: Vrstni red izvajanja "typeExt" glede na tip preslikave .....	253
Tabela 47: Primer uporabniških atributov in njihove vrednosti .....	255
Tabela 48: Rezultati pretvorbe (Primer 2) .....	256
Tabela 49: Rezultati pretvorbe (Primer 3) .....	257
Tabela 50: Rezultati pretvorbe (Primer 4) .....	258
Tabela 51: Tabele z opisom podatkov za varnostno kopiranje in obnavljanje .....	265
Tabela 52: Povprečne velikosti skeniranega dokumenta glede na metode stiskanja .....	277

# 1 PREGOVOR

Priročnik opisuje delovanje modula IMiS®/ARChive Server dokumentacije in nudi koristne nasvete iz tehničnega in vsebinskega področja uporabe produkta.

## 1.1 O dokumentaciji

V priročniku je opisana arhitektura strežnika, posamezni gradniki objektov, mehanizmi za zagotavljanje avtentičnosti in varnosti, ter postopki nameščanja, konfiguriranja in upravljanja arhivskega strežnika IMiS®/ARChive Server.

V zadnjem delu priročnika je podrobno opisana administracija strežnika preko spletnega administracijskega vmesnika.

## 1.2 Ciljno občinstvo

Priročnik je namenjen izkušenim sistemskim administratorjem z dobrim poznavanjem različnih izvedb operacijskih sistemov Linux ter izkušnji pri nameščanju, konfiguriranju, administraciji in upravljanju strežnika IMiS®/ARChive Server.

## 1.3 Konvencije

V dokumentaciji uporabljamo različne stile in načine zapisa pomembnih informacij, ki so povzete v spodnji tabeli:

Vrsta pisave	Namen uporabe
Navadno	Osnovno besedilo v dokumentaciji
<b>Navadno krepko</b>	Naslovi poglavij v dokumentaciji (nivoji 1-6)
<u>Navadno podčrtano</u>	Dodatne možnosti izbora podpoglavij znotraj posameznega nivoja
»Navadno«	Nazivi funkcij ali akcij v okviru možnosti izbora
<i>Navadno ležeče</i>	Prehodi na druga poglavja
Enakomerna širina znakov (Monospace)	Prikaz konzolnih ukazov, datotek, imenikov, ...
<b>Enakomerna širina znakov (Monospace Bold)</b>	Prikaz uporabniškega vnosa

Tabela 1: Uporaba različnih stilov v dokumentaciji

## 1.4 Kratice in pojmi

Spodnja tabela opisuje kratice, uporabljene v tekstu in grafikah tega dokumenta:

Kratica	Opis
AES	Advanced Encryption Standard (napreden algoritem šifriranja)
AIP	Archival Information Package (»povzetek« vsebine in metapodatkov entitete združen v XML dokument)
ACL	Access Control List (lista dostopnih pravic)
CA	Certificate Authority (zaupanja vreden izdajatelj digitalnih potrdil)
CIFS	Common Internet File System (komunikacijski protokol za podatke, tiskanje in druge servisne storitve v omrežju)
CRL	Certificate Revocation List (seznam preklicanih digitalnih potrdil)
CRM	Customer Relationship Management (sistem za upravljanje odnosov s strankami)
DMS	Document Management System (sistem za upravljanje z dokumenti)
EML	E-Mail Message (format za shranjevanje elektronskih sporočil)
ERP	Enterprise Resource Planning (poslovno informacijski sistemi)
ERS	Evidence Record Syntax (oblika podatkov za zagotavljanje dolgoročne stabilnosti časovnih žigov)
FIPS	Federal Information Processing Standard (standard za procesiranje informacij)
HA	High Availability (značilnost sistema - visoka razpoložljivost)
HMAC	Hash-based Message Authentication Code (način avtentikacije, ki vključuje funkcijo prstnega odtisa, ki je namenjena preverjanju integritete podatkov in avtentikacije)
HSM	Hierarchical Storage Management (koncept shranjevanja objektov - hierarhično arhiviranje dokumentov)
ISUD	Informacijski sistem za upravljanje z dokumenti

LTANS	Long-Term Archive and Notary Services (skupina tehničnih postopkov in funkcionalnosti za zagotavljanje vzdržnosti arhiviranja skozi daljše časovno obdobje; tudi skupina, ki te standarde določa)
MIME	Multipurpose Internet Mail Extensions
NAS	Network Attached Storage
NAT	Network Address Translation (prevedba omrežnih naslovov, postopek skrivanja privatnih naslovov)
OCSP	Online Certificate Status Protocol (spletni protokol za preverjanje statusa veljavnosti digitalnih potrdil)
PDF/A	Portable Document Format) (format za dolgoročno hrambo dokumentov - .pdf)
POSIX	Portable Operating System Interface (standardni vmesnik med aplikacijsko programsko opremo in operacijskim sistemom)
RAID 5	Redundant Array of Independent Disks (sistem za uporabo in organizacijo diskovnih pogonov)
RFC	Request for Comments (tehnični in organizacijski dokument, specifikacija, javni dokument, namenjen izmenjavi mnenj o opisani tematiki)
RHEL	Red Hat Enterprise Linux (Linux strežniška platforma podjetja RedHat)
RPM	RedHat Package Manager (aplikacija za upravljanje nameščene programske opreme na platformi Linux RedHat; tudi namestitveni paket programske opreme za isto imenovano aplikacijo za upravljanje)
SCSI/SAS	Serial Attached Small Computer System Interface (standardni vmesnik diskovnega pogona)
RSA	Ronald <b>R</b> ivest, Adi <b>S</b> hamir, Leonard <b>A</b> dleman (algoritem za šifriranje z javnim ključem)
SLES	SUSE Linux Enterprise Server (Linux strežniška platforma podjetja Novell)
SRP	Secure Remote Password (šifrirni protokol za varno avtentikacijo uporabnika)
SHA	Secure Hash Algorithm (algoritmi za izračun prstnega odtisa vsebine)
TCP/IP	Transmission Control Protocol / Internet Protocol (družina omrežnih protokolov)
TSA	Time Stamp Authority (agencija za izdajo kvalificiranih časovnih žigov)

TIFF	Tagged Image File Format (format za dolgoročno hrambo dokumentov)
URI	Uniform Resource Identifier (enotni označevalnik vira, ki predpisuje algoritem za pretvorbo AIP v normalizirano obliko)
X.509	(ITU-T standard za uporabo infrastrukture javnih ključev)
XML	Extensible Markup Language (označevalni jezik za hierarhično strukturiranje podatkov v obliki tekstovne datoteke)
XMLDSIG	XML Signature (specifikacija, ki določa XML zapis za elektronske podpise)
XSD	XML Schema Definition (priporočilo W3C za opredelitev strukture XML dokumentov)
W3C	World Wide Web Consortium (organ za standardizacijo ustreznih spletnih tehnik)
WORM	Write Once Read Many (princip shranjevanja objektov v arhivskem strežniku)
Container Vsebnik	Generičen element za shranjevanje podatkov

Tabela 2: Uporaba kratic v dokumentaciji

Spodnja tabela opisuje pojme, uporabljene v besedilu in slikah v priročniku:

Pojem	Opis
Attribute	Atribut - je osnovna celica ali vsebnik (angl. Container) metapodatka. Ta predpisuje pravila in okvirje za vnos, vzdrževanje in hrambo vrednosti metapodatkov, ki pripadajo entiteti.
Document	Dokument - osnovna enota arhivskega gradiva na IMiS®/ARChive Server, ki lahko hrani različne vrste digitalnih vsebin (npr. besedilo, slika, video). Navadno je vsebovan v zadevah, lahko pa nastopa tudi samostojno v razredu.
Entity	Entiteta - vsebovalnik (angl. Container) podatkov in vsebin na IMiS®/ARChive Server. Ločimo naslednje vrste entitet: razredi, zadeve in dokumenti.
IMiS®/ARChive Server	IMiS®/ARChive Storage Server strežnik (arhivski strežnik za shranjevanje objektov)
IMiS®/Scan	IMiS®/Scan odjemalec (IMiS® odjemalec za skeniranje papirnih dokumentov)
IMiS®/Storage Connector	IMiS®/Storage Connector vmesnik (vmesnik za prenos arhiviranih objektov med aplikativnim in arhivskim strežnikom)



IMiS®/View	IMiS®/View odjemalec (IMiS® odjemalec za prikazovanje skeniranih dokumentov)
Linux	Različni odprtokodni računalniški operacijski sistemi podobni operacijskemu sistemu Unix.
Mac OS X	Računalniški operacijski sistem podjetja Apple, ki temelji na operacijskem sistemu Unix.
Metadata	Metapodatek - predstavlja »informacije o informaciji« oziroma »podatke o podatku«, ki je predmet hrambe.
Microsoft .NET Framework	Microsoftovo okolje za razvoj spletnih storitev in drugih programskih komponent
Microsoft Excel	Program za delo z razpredelnicami, ki se med drugim lahko uporabi pri pregledovanju CSV datotek
Class	Razred - osnoven gradnik načrta razvrščanja gradiva na IMiS®/ARChive Server. Razredi lahko združujejo zadeve ali dokumente npr. po vrsti ali lastniku vsebine dokumentov.
Template	Predloga - predpisuje metapodatkovno shemo - zahtevane in dovoljene attribute za ustvarjanje entitet. Vsaka predloga vsebuje vgrajene in vnaprej določene sistemske attribute.
Unix	Družina računalniških operacijskih sistemov, ki izhajajo iz originalnega operacijskega sistema Unix podjetja Bell Labs.
Windows	Računalniški operacijski sistem podjetja Microsoft.
Windows Explorer	Windows Raziskovalec - program v operacijskem sistemu Windows, v katerega je vgrajen odjemalec IMiS®/Client

Tabela 3: Seznam uporabljenih pojmov v dokumentaciji

## 2 UVOD

### 2.1 Predstavitev

IMiS®/ARChive Server je programski modul za varno dolgoročno hrambo vseh vrst objektov elektronskega izvora ali digitaliziranih preko različnih postopkov digitalizacije (npr. skeniranja). Zagotavlja varno dolgoročno hrambo dokumentarnega gradiva in s tem: trajnosti, nespremenljivosti, urejenosti, dokazljivosti izvora gradiva in dostopnosti gradiva ves čas trajanja hrambe.

Strežnik je skalabilen. Arhiviramo lahko praktično neomejene količine binarnih objektov.

Hitrost posredovanja in prikazovanja arhiviranih objektov je praktično neodvisna od velikosti arhiva.

S tehnološkimi prijemi, ki jih zagotavljamo, je onemogočeno brisanje ali spreminjanje arhiviranega gradiva. Z upravljanjem dostopnih pravic zagotavljamo varnost dostopa kadarkoli in od kjerkoli.

Za zagotavljanje avtentičnosti arhiviranega gradiva uporabljamo ustrezna dokazila (prstni odtis, elektronski podpis z digitalnim potrdilom, časovni žig). Struktura, ustvarjanje in preverjanje teh dokazil je izvedeno po najsodobnejšem standardu ERS.

V revizijski sledi so zabeleženi vsi dostopi, dogodki, poizvedbe in spremembe na strežniku.

V svojem celotnem življenjskem ciklu je popolnoma nespremenljiva in zaščitena pred dovoljenimi in nedovoljenimi posegi.

Na osnovi preprostega iskalnega niza lahko v trenutku dostopamo do gradiva, ki bi ga sicer s težavo v fizičnem arhivu. K večji učinkovitosti bistveno prispeva uporaba naprednih tehnologij (OCR, FTS), saj omogoča iskanje po polnem besedilu dokumentov.

Elektronski arhiv ima v primerjavi s fizični arhivom številne prednosti. Obvladovanje arhiviranega gradiva v elektronski obliki je lažje in bistveno učinkovitejše

- Iskanje gradiva po elektronskem arhivu je neprimerno hitrejšo.
- Dostop do arhiviranega gradiva je hkrati omogočen neomejenemu številu prijavljenih uporabnikov iz različnih lokacij in aplikacij. Čas od pojavitve potrebe po nekem gradivu do dostopa do informacije je krajši kot pri fizičnem gradivu.
- Stroški hrambe in upravljanja s fizičnim gradivom naraščajo s količino hranjenega gradiva in hitro presežejo stroške elektronskega arhiviranja.

- Za razliko od arhiviranega gradiva se fizično gradivo lahko založi, izgubi, ali pa pride celo do namerne odtujitve.
- Pogoste so tudi poškodbe fizičnega gradiva, ki lahko povzročijo nenadomestljivo izgubo ključnih informacij.

Zaradi visoko zmogljivih povezovalnih modulov lahko aplikacije tretjih ponudnikov izvajajo vse postopke arhiviranja, izvajajo postopke življenjskega cikla arhiviranih entitet, upravljajo z dostopnimi pravicami, izvajajo poizvedbe (iskanja) po metapodatkih in polnem besedilu, itd.

Strežnik IMiS®/ARChive Server lahko deluje kot samostojen elektronski arhiv ali se preko programskega vmesnika povezuje z različnimi aplikacijskimi strežniki.

Arhitektura arhivskega sistema je fleksibilna in omogoča postavitve večjega števila arhivskih strežnikov in vzpostavitve različnih vlog v hierarhiji.

Spletni administracijski vmesnik omogoča prijavljenim uporabnikom nastavitve določenih funkcionalnosti arhivskega strežnika IMiS®/ARChive Server.

Prijavljeni uporabnik ima dostop samo do funkcionalnosti administracijskega vmesnika, do katerih je glede na pravice za pregledovanje in urejanje administracijskih področij upravičen.

## 2.2 Označevanje različic

Označevanje verzij programskega modula IMiS®/ARChive Server je osnovano na sekvenčni shemi s štirimi ločenimi numeričnimi identifikatorji (MAJOR, MINOR, RELEASE, BUILD) in končnim identifikatorjem tarčne arhitekture procesorja (ARCHITECTURE) (Linux standard).

Takšna shema je v svetu tudi najširše sprejeta.

Imenu namestitvene datoteke (RPM) so dodani še modulu specifični dodatni atributi, ki vsebujejo unikaten identifikator arhiva (ARCHIVEID) in identifikator namestitvene platforme (PLATFORM). Ti se ne beležijo v RPM podatkovno bazo in so na voljo le zaradi lažjega ločevanja in umeščanja namestitvene datoteke:

*imisarc.MAJOR.MINOR.RELEASE-BUILD.ARCHIVEID.PLATFORM.ARCHITECURE.rpm*

*Primer: imisarc.10.3.2210-750.0001.el8.x86\_64.rpm*

Shema je sestavljena iz imena IMiS® modula (»imisarc«) in naslednjih elementov:

- **MAJOR:** Identifikator na mestu MAJOR označuje glavno/veliko verzijo produkta, ki se spreminja skladno z vsakokratno arbitrarno odločitvijo glede na obseg izvedenih sprememb in funkcionalnosti. Na tem mestu se identifikator spreminja najredkeje in v primeru spremembe označuje veliko razliko v produktu glede na predhodno izdane verzije z manjšo MAJOR verzijo. Identifikator ima nabor vrednosti od 1-n, je zvezen in se izključno povečuje.
- **MINOR:** Identifikator na mestu MINOR označuje manjšo verzijo produkta, ki se spreminja skladno z vsakokratno arbitrarno odločitvijo glede na obseg izvedenih sprememb, funkcionalnosti in popravkov. Identifikator se spreminja pogosto in označuje manjše spremembe in popravke v okviru iste generacije produkta, ki jo označuje neka MAJOR verzija. Nabor vrednosti je od 1-n, ni zvezen in se z vsako spremembo MAJOR verzije postavi na izhodišče (1).
- **RELEASE:** Pri tem identifikatorju gre v nasprotju z arbitrarnim naborom vrednosti, ki velja po svetu, pri našem za specifikko, saj označuje časovno komponento izdaje produkta po shemi »LLMM«. MM označuje mesec izdaje (nabor 01-12), LL označuje zadnji dve številki leta; primer izdaja produkta »oktober 2022« je v RELEASE identifikatorju označena kot 2210.
- **BUILD:** Identifikator na tem mestu označuje zaporedno unikatno številko izgradnje produkta, ki se nikoli ne ponovi. V primeru minimalne spremembe produkta znotraj enega meseca lahko pride le do zamenjave tega identifikatorja medtem, ko vsi ostali ostanejo enaki. Nabor vrednosti je od 1-n, ni zvezen in se izključno povečuje.
- **ARCHIVE ID:** Vsaki instanci nameščenega produkta je dodeljen unikatni identifikator, ki se uporablja tudi v segmentu zaščite produkta in objektnih identifikatorjev. Strankam dostavljamo RPM datoteke, ki niso prenosljive in namenjene le konkretni instanci produkta. Nabor vrednosti je od 0001 – nnnn.
- **DATABASE:** Identifikator označuje s katero bazo je produkt distribuiran. Nabor vrednosti je v času izdaje te verzije BDB in RDM.

- **PLATFORM:** Identifikator označuje tip namestitvene platforme, kateri je namestitveni paket namenjen. Nabor vrednosti sles8, el3 in el4, označuje tarčno platformo pri čemer je za neko diskretno platformo potrebno poiskati ustrezen ekvivalent glede na okolje zahtevanih sistemskih knjižnic. Stranki pri tej izbiri pomagamo, lahko pa si pomaga tudi z uporabo kompatibilnih sistemskih knjižnic, ki omogočajo izvajanje glede na platformo starejšega produkta tudi na novejših platformah (npr. el3 namestitveni paket + kompatibilne knjižnice za rhel3 na rhel4 platformi).
- **ARCHITECTURE:** označuje tarčno arhitekturo procesorja. Možni vrednosti sta »x32« za 32-bitne Windows sisteme, ter »x64« za 64-bitne sisteme.

Podobno kot pri označevanju verzij programskega modula IMiS®/ARChive Server, lahko verzijo spletnega administracijskega vmesnika razberemo iz imena namestitvenega paketa, ki je sestavljen po naslednji shemi:

*IMiS.wAdmin.MAJOR.MINOR.RELEASE.BUILD.zip*

Primer imena namestitvenega paketa:

*IMiS.wAdmin.2.4.2210.7.zip*

Verzija spletne storitve administracijskega vmesnika namestitvenega paketa, je sestavljena po naslednji shemi :

*iaasvc-MAJOR.MINOR.RELEASE.BUILD.war*

Primer imena namestitvenega paketa za REST vmesnik:

*iaasvc-2.4.2210.7.war*

Kriteriji za določanje arbitrarno določljivih identifikatorjev so opredeljeni v notranjih pravilih družbe in so predmet postopka upravljanja s spremembami.

## 2.3 Funkcionalnosti

- Strukturirano arhiviranje vsebin elektronskega izvora ali digitaliziranih preko postopka skeniranja.
- Hramba metapodatkov arhiviranih vsebin preko strukturiranih atributov, povezanih v metapodatkovne sheme, določene v okviru hierarhičnih entitetnih predlog.
- Hramba sistemsko pomembnih atributov, ki vplivajo na življenjski cikel hranjenega gradiva.
- Hramba metapodatkov in elektronske pošte.
- Upravljanje z metapodatki hrambe fizičnega gradiva.
- Hramba nespremenljivih metapodatkov prenesenega gradiva.
- Iskanje po metapodatkih preko poizvedb z logičnimi in prednostnimi operatorji.
- Iskanje hranjenih vsebin po elementih njihove vsebine (iskanje po celotnem besedilu).
- Priklic vsebin preko uporabe zunanjih in notranjih identifikatorjev ter z uporabo klasifikacijske oznake.
- Upravljanje s hierarhičnim načrtom razvrščanja gradiva.
- Razvrščanje arhiviranih vsebin v načrtu razvrščanja gradiva z možnostjo dodajanja, brisanja, spreminjanja in premeščanja entitet.
- Upravljanje z stopnjami tajnosti hranjenega gradiva.
- Upravljanje z hierarhičnimi pravicami dostopa do hranjenih vsebin vse do nivoja posamičnega metapodatka.
- Zagotavljanje avtentičnosti hranjenega gradiva preko ustvarjanja in dolgoročnega vzdrževanja dokaznih elementov o nespremenjenosti hranjenega gradiva (LTANS).
- Imeniške storitve za podporo prijavi uporabnika, upravljanje z dostopnimi pravicami do hranjenih vsebin in razširitev podatkov entitet imenika v primeru uporabe v metapodatkovnih atributih.
- Beleženje in vzdrževanje revizijske sledi dejanj nad hranjenimi vsebinami ter zaščiten vpogled v sledi s strani za to pooblaščenih oseb.
- Zajem in preverjanje avtentičnosti vsebin preko preverjanja veljavnosti vgrajenih elektronskih podpisov.
- Verzioniranje dokumentov.
- Zmožnost uporabe IPv4 in IPv6 komunikacijskih skladov.
- Šifriranje povezav med storitvijo in njenimi odjemalci.
- Visoko skalabilen arhivski sistem s praktično nezaznavnim zamikom obdelave transakcij v primeru velikih inventarjev arhiviranih vsebin (nad 10 milijoni entitet).

- Konfiguracija in administracija (strežnika IMiS®/ARChive Server):
  - zapisovanja klasifikacijskih oznak in vrst entitet;
  - dostopnih pravic za entitete in attribute;
  - beleženja revizijske sledi;
  - avtentikacije, avtorizacije, vtičnikov in zunanjih imenikov;
  - uporabniško določenih atributov ter pregled sistemskih atributov;
  - nabora vrednosti uporabniško določenih atributov;
  - upravljanja z vsebinami (dostop, elektronsko podpisovanje in preverjanje, indeksiranje, pretvorba);
  - številčenja entitet na posameznem nivoju klasifikacijskega načrta;
  - podatkov o uporabniku ali skupini, avtentikaciji, vlogah in pravicah dostopa do konfiguracijskih map;
  - parametrov nestrukturiranega arhiviranja;
  - lastnosti in ponudnikov časovnega žigosanja vsebin ter pravil;
  - politik hrambe in zadržanj uničenja;
  - varnostnih mehanizmov (javni atributi, digitalna potrdila);
  - profilov in volumnov na strežniku;
  - predlog, katerim uporabniki določijo attribute.

## 2.4 Novosti v različici

Od zadnje različice 10.2.2110 programskega modula IMiS®/ARChive Server in spletnega vmesnika IMiS®/wAdmin, smo izvedli naslednje izboljšave:

### **IMiS®/ARChive Server 10.3.2210**

#### Nove funkcionalnosti:

- Avtentikacija s SAML2 žetonom
- Avtentikacija z OpenID Connect mehanizmom
- Lokacija objekta v nestrukturirani hrambi.

#### Izboljšave

- Preverjanje veljavnosti vdelanega časovnega žiga v okviru preverjanja veljavnosti digitalnega podpisa gradiva
- Dodaten opsijski časovni pogoj za začetek obdelave AIP paketa
- Pri branju entitete se vrne identifikator osnutka brez pravice dostopa.
- Prehod iz Lucene na Elasticsearch

#### Manjše izboljšave:

- Sprememba izvedbe shrambe digitalnih potrdil
- Implementacija filtriranja po tipu vsebine v zalednih sistemih za procesiranje
- Prilagoditev kode na GCC11 (EL9) in OpenSSL 3.



**IMiS®/wAdmin 2.4.2210**Nove funkcionalnosti:

- Uvedba seznama dovoljenih IP naslovov
- Podpora "Stateless" seji
- Urejanje zunanjih identitet entitete imenika
- Dodane sistemske nastavitve logiranja
- Izvoz/uvoz nastavitvev.

Izboljšave:

- Izboljšava prikaza pri zmanjšanju okna brskalnika
- Omogočanje kopiranja besedila v administracijskih mapah
- Dodajanje in odstranjevanje digitalnih potrdil arhiva
- Izboljšava zapisov dnevniških datotek.

Manjše izboljšave:

- Prilagoditev konfiguracije za indeksiranje besedila
- Posodobitev CodeMirror knjižnice
- Posodobitev ogrodja na Angular 14 in PrimeNG 14.

## 3 TEHNIČNA DOKUMENTACIJA

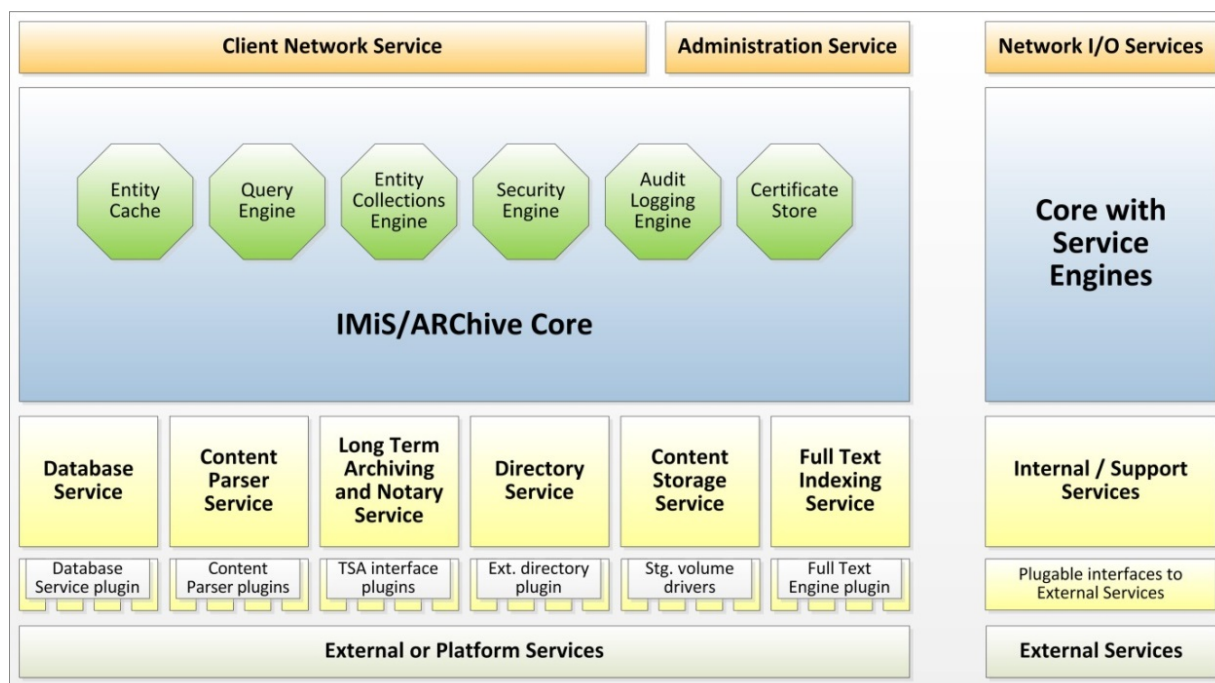
### 3.1 Arhitektura strežnika

IMiS®/ARChive Server predstavlja strežniško komponento sistema za upravljanje z gradivom v elektronski obliki IMiS®. Njegova modularna zasnova omogoča visok nivo prilagoditve na različne informacijske sisteme, katere danes večja podjetja uporabljajo za svoje poslovanje. Z uporabo 64-bitne različice lahko strežnik v celoti izkoristi 64-bitno strojno podporo, kar privede do pohitritve večine operacij napram 32-bitnem sistemom.

Jedro sistema predstavlja logično jedro, ki povezuje:

- Podporne servise, povezane z zunanjimi viri informacij ali samostojno delujoče v okviru instance strežnika.
- Notranje logične servise, ki jedru zagotavljajo podporo odločitvam glede sicer prilagodljive poslovne logike in prispevajo k visoki zmogljivosti in propustnosti sistema.
- Omrežne servise, ki na eni strani skrbijo za izmenjavo informacij z odjemalci strežnika in jedrom ter na drugi strani nudijo točko integracije z zalednimi aplikacijami.

Slednje z jedrom izmenjujejo statistične informacije o delovanju in nastavitvene informacije.



Slika 1: Shematični prikaz arhitekture strežniške komponente IMiS®/ARChive Server

- Glavni proces »iarcd«, ki s funkcionalnostjo »Boost« knjižnice upravlja s podpornimi procesi:
  - Sprejemanje zahteve po novih povezavah s strani odjemalcev.
  - Izbiranje logičnih procesov za obdelavo odjemalskih povezav.
  - Zbiranje statističnih podatkov o delovanju strežnika.
  - Indeksiranje po besedilu vsebin.
  - Vzdrževanje avtentičnosti arhiviranih vsebin.
  - Sinhronizacija imenika z zunanjimi viri imeniških storitev, ... (opcijsko).

Logični nivo strežnika sestavljajo samostojne ali med seboj odvisne storitve, ki jedru nudijo:

- Podporo pri odločitvah glede načina obdelave dogodkov.
- Medpomnjenje aktualnih objektov za katere je smiselno, da so naloženi v spominu.
- Podporo odločanju glede dostopov.
- Podporo vzdrževanju revizijske sledi.
- Komunikacijski nivo storitve, ki izmenjuje informacije z odjemalci storitve, ... .

Storitve so strukturirane na:

- Nivo vmesnikov do storitev fizičnega nivoja platforme ali zunanjih storitev, ki preko vtičnikov omogoča uporabo virov informacij, ki niso del sistema.
- Nivo podpornih storitev, ki jedru sistema nudijo nujne in ne-nujne storitve za njegovo delo. Omogočajo samostojno izvajanje določenih storitev, ki niso neposredno vezane na jedro. Na eni strani komunicirajo z jedrom, na drugi strani pa preko vtičnikov do virov platforme in zunanjih storitev.
- Jedro sistema z notranjimi storitvami in pogoni, ki jedru nudijo logične celote za funkcionalnosti, ki jih podpirajo. So neločljivi del jedra in z njimi razen v izjemnih primerih ni mogoče upravljati.
- Komunikacijski nivo, ki skrbi za izmenjavo podatkov med jedrom in odjemalci sistemi. Podpira različne omrežne protokole, šifriranje prometa in standarde kodiranja informacij.

Nadaljevanje poglavja obravnava posamične storitve v smislu njenega pomena za delovanje strežnika.

#### Database service [storitev podatkovne baze]

Pomen: Kritičen

Opis: Storitev sistemu nudi nivo podatkovne zbirke tabel in indeksov, potrebnih za delovanje. Storitev je zasnovana abstraktno in deluje preko vsakokratnega vtičnika podatkovne baze, specifičnega za tehnologijo in ponudnika podatkovne zbirke.

Trenutno podprti vtičniki podatkovnih zbirk so:

- Raima Embedded Database: vgrajena baza podatkov, do katere prijavljeni uporabniki dostopajo lokalno preko knjižnic okolja za delo z bazo.

Sistem v podatkovno zbirko shranjuje večino informacij, povezanih s hranjenimi entitetami, razen hranjenih vsebin, ki so shranjene v okviru druge storitve in na drugih nosilcih.

#### Content Parser Service [storitev obdelave hranjenih vsebin]

Pomen: Obvezen

Opis: Sistem storitev se uporablja za obdelavo vsebin, ki jih odjemalci arhivirajo.

Zasnovan je na principu vtičnikov, ki zna vsak zase obdelati določeno vrsto vsebine, glede na njen »ContentType«(MIME tip).

Vsak vtičnik lahko storitvi nuditi naslednje funkcionalnosti:

- Izvoz besedila vsebine.
- Izvoz metapodatkov vsebine.
- Izvoz vgrajenih elektronskih podpisov.
- Izvoz digitalnih potrdil vgrajenih elektronskih podpisov.
- Preverjanje veljavnosti vgrajenih elektronskih podpisov.

Sistem uporablja funkcionalnosti:

- Obdelave vsebin za potrebe preverjanja veljavnosti vsebin.
- Zajema vgrajenih elektronskih podpisov in z njimi povezanimi digitalnimi potrdili.
- Podpore storitvi indeksiranja po polnem besedilu.

Trenutno storitev za vtičnike uporablja vgrajene tehnologije Apache projekta Tika in iText (obdelava »application/pdf« vsebin) ter lastno tehnologijo za obdelavo vsebin formata »image/tiff« in »text/xml«.

### Long term Archiving and Notary Service - LTANS [Sistem za zagotavljanje avtentičnosti hranjenih vsebin]

Pomen: Neobvezen

Opis: Sistem (opcijsko) zagotavlja izdelavo in dolgoročno vzdrževanje dokaznih elementov nespremenljivosti hranjenih vsebin. Sistem ni ključen za delovanje arhivskega sistema, v kolikor uporabnik tovrstnih storitev ne potrebuje.

Storitev zajame vse zaključene entitete in jih glede na nastavitvene parametre vključi v inventar entitet, katerim se zagotavljajo elementi avtentičnosti.

Hkrati samodejno vzdržuje že obstoječe elemente avtentičnosti in skupaj z novimi elementi gradi drevesa zgoščenih dokaznih elementov. Te štiti s časovnimi žigi različnih ponudnikov zaupanja vrednih časovnih žigov. Pridobi jih preko vtičnikov, specifičnih za vsakokratnega ponudnika časovnega žiga. Dodatno zaščito pred zlomom veljavnosti časovnega žiga lahko zagotovimo z uporabo več vzporednih časovnih žigov različnih ponudnikov zaupanja vrednih časovnih žigov.

S tem sistem zagotovi veljavnost dokaznih elementov avtentičnosti tudi v redkih primerih preklica veljavnosti časovnih žigov pred njihovim iztekom veljavnosti.

Več informacij se nahaja v poglavju [Avtentičnost](#).

### Directory Service [Imeniška storitev]

Pomen: Kritičen

Opis: Storitev zagotavlja podporo različnim storitvam imenika, katere uporabljajo:

- Podsistem za dostopno logiko do hranjenih vsebin.
- Podsistem za hrambo vrednosti metapodatkovnih atributov.

Storitev omogoča vzdrževanje atributov imeniških entitet (podatki o uporabniku, njegovih varnostnih komponent, ki se uporabljajo pri prijavi/avtentikaciji, podatki o skupinah, katerim uporabnik pripada, ...) in članstva entitet imenika (uporabniki, skupine) v različnih skupinah.

Opcijsko se preko vtičnikov lahko imeniška storitev poveže z zunanjimi viri imeniških storitev v smislu konsolidiranih in centralno orientiranih imeniških storitev,

ki se distribuirano uporabljajo v okviru različnih sistemov.

Več informacij se nahaja v poglavju [Imeniške storitve](#).

### Content Storage Service [Storitev hrambe hranjenih vsebin]

**Pomen:** Obvezen

**Opis:** Sistem storitev uporablja za trajno hrambo digitalnih vsebin, ki jih odjemalci arhivirajo. Zasnovan je na principu vtičnikov, ki zna vsak zase optimalno upravljati z različnimi vrstami nosilcev digitalnih vsebin. Tako sistem loči med različnimi vrstami lokalnih nosilcev vsebin in različnimi vrstami oddaljenih nosilcev vsebin. Tehnologijam primerno, jedru zagotavlja enoten nivo hrambe digitalnih vsebin. Inventar arhiviranih vsebin je hranjen po principih hierarhične hrambe ([http://en.wikipedia.org/wiki/Hierarchical\\_storage\\_management](http://en.wikipedia.org/wiki/Hierarchical_storage_management)) na logičnem nivoju storitve za optimalno izrabo in nizke stroške arhiviranja. Brez pravilno nameščene storitve sistem sicer lahko deluje in hrani attribute entitet, digitalnih vsebin pa ne. Storitev je bila z ukinitvijo procesa za upravljanje z volumni »iavol« prenešana na glavni proces »iarcd«, ki posredno uporablja storitev preko zahtev odjemalcev.

Do te storitve dostopajo tudi druge storitve, kot na primer storitev indeksiranja po besedilu vsebin, ... ipd.

### Full Text Indexing Service [Storitev indeksiranja po celotnem besedilu hranjenih vsebin]

**Pomen:** Neobvezen

**Opis:** Storitev sistemu in njegovim uporabnikom zagotavlja funkcionalnost iskanja po besedilu hranjenih vsebin. Zasnovana je na modelu vtičnikov, ki sistemu na abstraktnem nivoju nudijo poenoten dostop do storitev indeksiranja vsebin in kasnejšemu iskanju po indeksu besedil hranjenih vsebin. Trenutno sistem preko vtičnika uporablja vgrajeno tehnologijo Apache projekta Lucene. V kolikor uporabnik ne potrebuje funkcije iskanja po celotnem besedilu arhiviranih vsebin, je možno storitev onemogočiti, saj ni ključna za delovanje sistema.

### Entity Cache [Medpomnilnik odprtih entitet]

**Pomen:** Kritičen

**Opis:** Gre za notranjo storitev s katero ni mogoče upravljati. Sistem uporablja visoko zmogljiv model medpomnjenja za vse entitete, ki so v neki časovni točki odprte s strani uporabnikov ali notranje za potrebe njihove obdelave. Sistem skladno s svojim modelom notranje odpre celotno vejo entitete do korenskega nivoja in instance entitet drži odprte skladno z obstoječimi sklici na njih. Ko se zapre zadnji sklic na entiteto, se ta iz medpomnilnika odstrani. Enako velja za vse njene starševske entitete do korena. Tako sistem zagotavlja visok nivo odzivnosti za vzporedna odpiranja entitet oziroma pridobivanja podatkov iz le-teh.

Celoten model medpomnjenja informacij temelji na konceptu »lenega« nalaganja informacij, vse v smeri visokega nivoja odzivnosti sistema. Informacije se namreč nalagajo pri prvi dejanski potrebi po informaciji in ne na zalogo.

V primeru spreminjanja entitet so vrednosti atributov instance za vpogled in instance za spreminjanje v spominu naložene le enkrat in se podvojijo šele ob dejanski spremembi vrednosti atributa, vse zaradi minimalne porabe spomina za medpomnilnik.

Zaradi vseh uporabljenih konceptov algoritma medpomnjenja pripomorejo k sistemu, ki nudi visoko zmogljiv, hiter in učinkovit sistem dostopa do hranjenih vsebin ob minimalni porabi delavnega spomina.

#### Query Engine [Podsystem za iskanje po metapodatkih]

Pomen: Obvezen

Opis: Gre za notranjo storitev, preko katere uporabniki in sam sistem išče entitete glede na vrednosti njihovih indeksiranih atributov. Sistem nudi gramatičen pogon za spremembo opisne oblike poizvedbe z njegovo logično obliko, primerno za izvajanje podsistema za iskanje po vrednostih atributov. Gramatična pravila omogočajo poljubne poizvedbe z različnimi logičnimi in prednostnimi operatorji. Sistem omogoča tudi učinkovito iskanje po praznih vrednostih atributov. Deluje v povezavi s Entity Collections storitvijo.

#### Entity Collections Engine [Podsystem za izgradnjo ad-hoc zbirk entitet]

Pomen: Kritičen

Opis: Storitev sistemu omogoča gradnjo zbirk entitet na podlagi različnih vrst poizvedb. Po teh ad-hoc zbirkah je možno naključno poizvedovati in pridobivati informacije o zbranih entitetah. Ta podsistem pogosto uporabljajo funkcije odjemalcev za hierarhični vpogled v drevo arhiviranih entitet (vse pod-entitete neke starševske entitete, ipd.) in podsistem za iskanje po metapodatkih, ki zgradi ad-hoc zbirko entitet na podlagi specifične poizvedbe.

Ker so lahko zbirke entitet obsežne in ker jih je lahko vzporedno odprtih več, je ključno dobro upravljanje sistema s spominskimi viri platforme, ki so mu na voljo v smeri minimalnega vpliva na obseg porabljenega delovnega spomina.

### Security Engine [Podsistem za izračun dostopnih pravic do arhiviranih vsebin]

Pomen: Kritičen

Opis: Vsakokratno odpiranje entitete v sistemu povzroči ustvaritev instance entitete, če ta ni že prisotna v medpomnilniku. Takrat se v instanco naložijo tudi shranjena pravila dostopa, ki hierarhično omogočajo visoko zmogljiv sistem določanja dostopnih pravic po modelu liste dostopnih pravic (t.i. Access Control List - ACL).

Pravice se dedujejo od nadrejenih entitet, lahko pa se tudi nadomestijo z eksplicitnimi pravicami. Pravila za izračun so ločena od jedra zato govorimo o podsistemu.

Na pravila ni mogoče vplivati in z njimi upravljati, omogočen je le omejen nabor nastavitvev, ki bistveno ne vplivajo na zaščito informacij.

### Audit Logging Engine [Podsistem za beleženje in vzdrževanje revizijske sledi dogodkov na arhiviranih vsebinah in njen vpogled]

Pomen: Neobvezen

Opis: Podsistem jedru sistema omogoča natančno beleženje dogodkov nad arhiviranimi vsebinami v realnem času, ki so del transakcij samih operacij.

Operacije so v sistemu za razliko od beleženja revizijskih sledi podatkovnih strežnikov logično zaokrožene, celovite, konsolidirane in za to poklicanemu osebju jasne.

Z nivojem beleženja revizijske sledi in obsegom podatkov, ki se zajemajo, je možno upravljati skozi profile revizijske sledi. Profili predstavljajo zaokroženo celoto nastavitvev revizijske sledi, ki velja za posamezen sklop entitet. Nastavitvev globalnega profila velja za vse entitete. Z določitvijo dodatnih profilov, pa lahko spreminjamo nivo beleženja revizijske sledi za posamezne entitete. Vse spremembe revizijskih profilov so zabeležene v revizijski sledi.

V kolikor uporabnik ne potrebuje funkcije beleženja revizijske sledi, jo je mogoče onemogočiti.

### Certificate Store [Podsistem za upravljanje z digitalnimi potrdili]

Pomen: Obvezen

Opis: Podsistem jedru sistema omogoča storitve povezane z digitalnimi potrdili, ki jih uporablja jedro in/ali z njim povezane storitve. Hrani digitalna potrdila zaupanja vrednih izdajateljev digitalnih potrdil in nudi logično podporo pri preverjanju veljavnosti različnih digitalnih potrdil, ki jih sistem pri svojem delu srečuje.

Podsistem nudi funkcionalnosti pridobivanja podatkov o preklicih digitalnih potrdil s tehnologijami CRL in OSCP. V kolikor je skladišče digitalnih potrdil zaupanja vrednih izdajateljev digitalnih potrdil prazno, operacije v smislu preverjanja veljavnosti digitalnih potrdil ne delujejo.



### Client Network Service [Podsistem za izmenjavo informacij med jedrom in odjemalci sistema]

**Pomen:** Kritičen

**Opis:** Podsistem jedru sistema omogoča varno izmenjavo informacij z njegovimi odjemalci. Uporabljen asinhron omrežni model omogoča visoko propustno in učinkovito delovanje storitve. Šifriranje prometa med storitvijo in odjemalci ščiti prenesene informacije pred nepooblaščenim dostopom. Storitve omogoča povezovanje preko več nastavljivih TCP/IP vrat in naslovov obeh IPv4 in IPv6 skladov.

### Content Conversion Service [Podsistem za samodejno pretvorbo vsebin]

**Pomen:** Neobvezen

**Opis:** Podsistem omogoča samodejno pretvorbo vsebin entitet. Zasnovan je na principu vtičnikov, katere lahko povežemo v verige. Na podlagi teh se samodejno pretvarjajo vsebine. Za več informacij glej poglavje [Samodejno pretvarjanje vsebin](#).

## **3.2 Atribut**

V svetu velikih količin posamičnih, med seboj povezanih ali nepovezanih informacij, jih je za uspešno hrambo in učinkovit dostop nujno logično opisati in jih povezati.

Za to uporabljamo t.i. metapodatke, ki abstraktno predstavljajo »informacije o informaciji«, oziroma »podatke o podatku«, ki je predmet hrambe.

Da bi vzpostavili in dolgoročno ohranili strukturo in normalizacijo posameznih metapodatkov, jih je potrebno uokviriti in jim predpisati pravila.

To v strežniku IMiS®/ARChive Server dosežemo z uporabo koncepta Atribut, katerih skupine pripišemo entiteti. Za več informacij glej poglavje [Entiteta](#).

Atribut je osnovna celica ali vsebnik (angl. Container) metapodatka.

Ta predpisuje pravila in okvirje za vnos, vzdrževanje in hrambo vrednosti metapodatkov, ki pripadajo entiteti. Lahko ga označimo tudi za model metapodatka, kateremu se morajo vrednosti prilagoditi, če jih želimo v atribut shraniti.

Poznamo več tipov atributov, ki primarno določajo tip vrednosti, katere je možno shraniti v atribut. Atributi vsebujejo tudi kontrolne parametre, ki določajo razpone vrednosti, njihovo formo, zmožnost iskanja po vrednostih, ...

Atribute po določitvi povežemo v t.i. metapodatkovne ali atributne sheme, ki jih združujemo v predlogah entitet. Za več informacij glej poglavje [Predloge](#).

Povezave med atributi in predlogami določajo kontrolne parametre, specifične za povezavo med atributom in entiteto, kot so:

- obveznost
- zmožnost vsebovanja več vrednosti
- nespremenljivost
- forma in razpon vrednosti, ki je specifična za atribut v okviru nekega tipa entitete
- drugi parametri.

Atribut je ključen gradnik in steber učinkovitega elektronskega arhiva, saj hranjeno informacijo (vsebino) normalizirano opisuje in uporabnikom omogoča dostop do vsebine, ko telo vsebine ne omogoča neposrednega dostopa. Razlog za to je lahko sama narava vsebine (zvočni ali slikovni zapis) ali njen obseg.

### 3.2.1 Vrste atributov

Identifikator: 1

Naziv: DirectoryEntity

Opis: Predstavlja identifikator entitete iz imenika. Podatek lahko smiselno uporabimo za pridobitev podatkov entitete iz imenika.

Razpon vrednosti: Registrirana entiteta imenika

Reference: /

Identifikator: 2

Naziv: Bool

Opis: Logična oziroma bitna vrednost, uporabna v logični in Boolean algebri.

Označuje resnično (pozitivno) in neresnično (negativno) stanje.

Razpon vrednosti: True, False ali 1, 0

Reference: [http://en.wikipedia.org/wiki/Boolean\\_data\\_type](http://en.wikipedia.org/wiki/Boolean_data_type)

Identifikator: 3

Naziv: Int8

Opis: Predznačeno 8 bitno celo število.

Razpon vrednosti: Min: -128, Max: 127

Reference: [http://en.wikipedia.org/wiki/Character\\_%28computing%29](http://en.wikipedia.org/wiki/Character_%28computing%29)

Identifikator: 4

Naziv: UInt8

Opis: Ne-predznačeno 8 bitno celo število.

Razpon vrednosti: Min: 0, Max: 255

Reference: <http://en.wikipedia.org/wiki/Byte>

Identifikator: 5

Naziv: Int16

Opis: Predznačeno 16 bitno celo število.

Razpon vrednosti: Min: -32768, Max: 32767

Reference: [http://en.wikipedia.org/wiki/Integer\\_%28computing%29#Short\\_integer](http://en.wikipedia.org/wiki/Integer_%28computing%29#Short_integer)

Identifikator: 6

Naziv: UInt16

Opis: Ne-predznačeno 16 bitno celo število.

Razpon vrednosti: Min: 0, Max: 65535

Reference: [http://en.wikipedia.org/wiki/Integer\\_%28computing%29#Short\\_integer](http://en.wikipedia.org/wiki/Integer_%28computing%29#Short_integer)

Identifikator: 7

Naziv: Int32

Opis: Predznačeno 32 bitno celo število.

Razpon vrednosti: Min: -2147483648, Max: 2147483647

Reference: [http://en.wikipedia.org/wiki/Integer\\_%28computing%29#Long\\_integer](http://en.wikipedia.org/wiki/Integer_%28computing%29#Long_integer)

Identifikator: 8

Naziv: UInt32

Opis: Ne-predznačeno 32 bitno celo število.

Razpon vrednosti: Min: 0, Max: 4294967295

Reference: [http://en.wikipedia.org/wiki/Integer\\_%28computing%29#Long\\_integer](http://en.wikipedia.org/wiki/Integer_%28computing%29#Long_integer)

Identifikator: 9

Naziv: Int64

Opis: Predznačeno 64 bitno celo število.

Razpon vrednosti: Min: -9223372036854775808, Max: 9223372036854775807

Reference: [http://en.wikipedia.org/wiki/Integer\\_%28computing%29#Long\\_integer](http://en.wikipedia.org/wiki/Integer_%28computing%29#Long_integer)

Identifikator: 10

Naziv: UInt64

Opis: Nepredznačeno 64 bitno celo število.

Razpon vrednosti: Min: 0, Max: 18446744073709551615

Reference: [http://en.wikipedia.org/wiki/Integer\\_%28computing%29#Long\\_integer](http://en.wikipedia.org/wiki/Integer_%28computing%29#Long_integer)

Identifikator: 11

Naziv: Int128

Opis: Predznačeno 128 bitno celo število.

Razpon vrednosti: Min: -170141183460469231731687303715884105728,  
Max: 170141183460469231731687303715884105727

Reference: [http://en.wikipedia.org/wiki/Integer\\_%28computing%29#Long\\_integer](http://en.wikipedia.org/wiki/Integer_%28computing%29#Long_integer)

Identifikator: 12

Naziv: UInt128

Opis: Nepredznačeno 128 bitno celo število.

Razpon vrednosti: Min: 0, Max: 340282366920938463463374607431768211455

Reference: [http://en.wikipedia.org/wiki/Integer\\_%28computing%29#Long\\_integer](http://en.wikipedia.org/wiki/Integer_%28computing%29#Long_integer)

Identifikator: 13

Naziv: Double

Opis: Realno (racionalno) število v plavajoči vejici z dvojno natančnostjo.

Ni primeren za vrednosti kjer je nujna absolutna natančnost (npr. bančne transakcije).

V takšnih primerih je primernejši tip Decimal.

Razpon vrednosti: / (dinamični razpon)

Reference: [http://en.wikipedia.org/wiki/Double-precision\\_floating-point\\_format](http://en.wikipedia.org/wiki/Double-precision_floating-point_format)

Identifikator: 14

Naziv: Date

Opis: Datumsko vrednost brez časovne komponente.

Razpon vrednosti: Min: 1.1.8192 pr. n. š., Max: 31.12.8191

Reference: [http://en.wikipedia.org/wiki/ISO\\_8601](http://en.wikipedia.org/wiki/ISO_8601)

Identifikator: 15

Naziv: Time

Opis: Časovna vrednost brez datumske komponente.

Razpon vrednosti: Vseh 24 ur natančno na 1 milisekundo.

Reference: [http://en.wikipedia.org/wiki/ISO\\_8601](http://en.wikipedia.org/wiki/ISO_8601)

Identifikator: 16

Naziv: DateTime

Opis: Datumsko vrednost s časovno komponento.

Razpon vrednosti: Min: 1.1.8192 pr. n. š. s časovno komponento (glej Date + Time),

Max: 31.12.8191 s časovno komponento (glej Date + Time)

Reference: [http://en.wikipedia.org/wiki/ISO\\_8601](http://en.wikipedia.org/wiki/ISO_8601)

Identifikator: 17

Naziv: StringMax

Opis: Neomejen niz UTF-8 znakov.

Razpon vrednosti: / (omejeno z zmogljnostjo platforme)

Reference: [http://en.wikipedia.org/wiki/String\\_%28computer\\_science%29](http://en.wikipedia.org/wiki/String_%28computer_science%29)

<http://en.wikipedia.org/wiki/UTF-8>

Identifikator: 18

Naziv: String10

Opis: Niz UTF-8 znakov, dolgih 10 bajtov.

Razpon vrednosti: 10 bajtov UTF-8 znakov

Reference: [http://en.wikipedia.org/wiki/String\\_%28computer\\_science%29](http://en.wikipedia.org/wiki/String_%28computer_science%29)

<http://en.wikipedia.org/wiki/UTF-8>

Identifikator: 19

Naziv: String20

Opis: Niz UTF-8 znakov, dolgih 20 bajtov.

Razpon vrednosti: 20 bajtov UTF-8 znakov

Reference: [http://en.wikipedia.org/wiki/String\\_%28computer\\_science%29](http://en.wikipedia.org/wiki/String_%28computer_science%29)

<http://en.wikipedia.org/wiki/UTF-8>

Identifikator: 20

Naziv: String30

Opis: Niz UTF-8 znakov, dolgih 30 bajtov.

Razpon vrednosti: 30 bajtov UTF-8 znakov

Reference: [http://en.wikipedia.org/wiki/String\\_%28computer\\_science%29](http://en.wikipedia.org/wiki/String_%28computer_science%29)

<http://en.wikipedia.org/wiki/UTF-8>

Identifikator: 21

Naziv: String40

Opis: Niz UTF-8 znakov, dolgih 40 bajtov.

Razpon vrednosti: 40 bajtov UTF-8 znakov

Reference: [http://en.wikipedia.org/wiki/String\\_%28computer\\_science%29](http://en.wikipedia.org/wiki/String_%28computer_science%29)

<http://en.wikipedia.org/wiki/UTF-8>

Identifikator: 22

Naziv: String50

Opis: Niz UTF-8 znakov, dolgih 50 bajtov.

Razpon vrednosti: 50 bajtov UTF-8 znakov

Reference: [http://en.wikipedia.org/wiki/String\\_%28computer\\_science%29](http://en.wikipedia.org/wiki/String_%28computer_science%29)

<http://en.wikipedia.org/wiki/UTF-8>

Identifikator: 23

Naziv: String100

Opis: Niz UTF-8 znakov, dolgih 100 bajtov.

Razpon vrednosti: 100 bajtov UTF-8 znakov

Reference: [http://en.wikipedia.org/wiki/String\\_%28computer\\_science%29](http://en.wikipedia.org/wiki/String_%28computer_science%29)

<http://en.wikipedia.org/wiki/UTF-8>

Identifikator: 24

Naziv: String200

Opis: Niz UTF-8 znakov, dolgih 200 bajtov.

Razpon vrednosti: 200 bajtov UTF-8 znakov

Reference: [http://en.wikipedia.org/wiki/String\\_%28computer\\_science%29](http://en.wikipedia.org/wiki/String_%28computer_science%29)

<http://en.wikipedia.org/wiki/UTF-8>

Identifikator: 25

Naziv: EntityReference

Opis: Predstavlja identifikator entitete na strežniku.

Razpon vrednosti: Vse ustvarjene entitete na strežniku.

Reference: /

Identifikator: 31

Naziv: Decimal1

Opis: Predznačeno realno (racionalno) število, natančno na 1 decimalno mesto.

Razpon vrednosti: Min: -9223372036854775807.8, Max: 9223372036854775808.7

Reference: <http://en.wikipedia.org/wiki/Decimal>

Identifikator: 32

Naziv: Decimal2

Opis: Predznačeno realno (racionalno) število, natančno na 2 decimalni mesti.

Razpon vrednosti: Min: -922337203685477580.78, Max: 922337203685477580.87

Reference: <http://en.wikipedia.org/wiki/Decimal>

Identifikator: 33

Naziv: Decimal3

Opis: Predznačeno realno (racionalno) število, natančno na 3 decimalna mesta.

Razpon vrednosti: Min: -92233720368547758.078, Max: 92233720368547758.087

Reference: <http://en.wikipedia.org/wiki/Decimal>

Identifikator: 34

Naziv: Decimal4

Opis: Predznačeno realno (racionalno) število, natančno na 4 decimalna mesta.

Razpon vrednosti: Min: -9223372036854775.8078, Max: 9223372036854775.8087

Reference: <http://en.wikipedia.org/wiki/Decimal>

Identifikator: 35

Naziv: Decimal5

Opis: Predznačeno realno (racionalno) število, natančno na 5 decimalnih mest.

Razpon vrednosti: Min: -922337203685477.58078, Max: 922337203685477.58087

Reference: <http://en.wikipedia.org/wiki/Decimal>

Identifikator: 36

Naziv: Decimal6

Opis: Predznačeno realno (racionalno) število, natančno na 6 decimalnih mest.

Razpon vrednosti: Min: -92233720368547.758078, Max: 92233720368547.758087

Reference: <http://en.wikipedia.org/wiki/Decimal>

Identifikator: 37

Naziv: Decimal7

Opis: Predznačeno realno (racionalno) število, natančno na 7 decimalnih mest.

Razpon vrednosti: Min: -9223372036854.7758078, Max: 9223372036854.7758087

Reference: <http://en.wikipedia.org/wiki/Decimal>

Identifikator: 38

Naziv: Decimal8

Opis: Predznačeno realno (racionalno) število, natančno na 8 decimalnih mest.

Razpon vrednosti: Min: -922337203685.47758078, Max: 922337203685.47758087

Reference: <http://en.wikipedia.org/wiki/Decimal>



Identifikator: 39

Naziv: Decimal9

Opis: Predznačeno realno (racionalno) število, natančno na 9 decimalnih mest.

Razpon vrednosti: Min: -92233720368.547758078, Max: 92233720368.547758087

Reference: <http://en.wikipedia.org/wiki/Decimal>

Identifikator: 40

Naziv: Decimal10

Opis: Predznačeno realno (racionalno) število, natančno na 10 decimalnih mest.

Razpon vrednosti: Min: -9223372036.8547758078, Max: 9223372036.8547758087

Reference: <http://en.wikipedia.org/wiki/Decimal>

Identifikator: 41

Naziv: Binary

Opis: Neomejen niz zlogov s podatkom o tipu vsebine (MIME). Zmožen je posredovanja velikosti hranjenega niza.

Razpon vrednosti: / (omejeno z zmožnostjo platforme)

Reference: <http://en.wikipedia.org/wiki/Bitstring>

[http://en.wikipedia.org/wiki/Internet\\_media\\_type](http://en.wikipedia.org/wiki/Internet_media_type)

Identifikator: 42

Naziv: File

Opis: Atribut je zmožen hrambe datotek s: podatkom o tipu vsebine (MIME), opisom, časom nastanka, zadnje spremembe in zadnjega dostopa.

Zmožen je tudi posredovanja velikosti hranjenega niza.

Razpon vrednosti: Vsebina z velikostjo do 9223372036854775807 bajtov,

opis z velikostjo do 4096 bajtov UTF-8 znakov.

Reference: [http://en.wikipedia.org/wiki/Internet\\_media\\_type](http://en.wikipedia.org/wiki/Internet_media_type)

### 3.2.2 Parametri atributov

Atribut poleg njegovega tipa opisujejo še naslednji podatki:

- »Ime« (angl. Name): naziv, obvezen unikatni niz UTF-8 znakov, dolg do 256 bajtov UTF-8 znakov.
- »Oznaka« (angl. Label): oznaka atributa, opcijski niz UTF-8 znakov, dolg do 256 bajtov.
- »Opis« (angl. Description): opis atributa, opcijski niz UTF-8 znakov, dolg do 512 bajtov UTF-8 znakov.
- »Preverjanje ustrezne vrednosti« (angl. Validation expression): niz UTF-8 znakov, ki predstavljajo regularni izraz (angl. Regular expression) s katerim se nove ali spremenjene vrednosti atributa preverjajo.  
Več o sintaksi in pravilih: [http://en.wikipedia.org/wiki/Regular\\_expression](http://en.wikipedia.org/wiki/Regular_expression).
- »Parametri« (angl. Parameters): dodatni parametri atributa, ki poleg njegovega podatkovnega tipa dodatno uokvirjajo pripisane vrednosti: »Searchable«, »Unique« in »PickList«.

#### Searchable

Vrednosti atributa postanejo del indeksa, po katerem je možno s funkcijami iskanja iskati entitete, katerim vrednosti so pripisane. Nasprotno pa, po vrednostih atributov, ki niso označeni kot »Searchable« ni mogoče iskati s funkcijami iskanja.

Na podlagi tega dejstva se je zato potrebno ob nastavitvi strežnika IMiS®/ARChive Server in atributov odločati, ali atributu ta parameter pripisati.

Ko atribut dobi prvo vrednost, tega parametra ni mogoče spreminjati.

Ta parameter lahko bistveno vpliva na delovanje in zmoglosti (angl. Performance) strežnika.

Podatki se namreč shranjujejo v iskalna drevesa, ki lahko postanejo velika in počasna.

Na drugi strani se vrednosti »Non-searchable« atributov le shranijo, zato njihova količina bistveno ne vpliva na delovanje strežnika.

#### Unique

Vsaka vrednost atributa je unikatna skozi celoten arhiv. Ta parameter vključimo,

ko želimo zagotoviti, da ne pride do vnosa vrednosti atributa, ki ga že določa druga entiteta.

Kršitev tega pravila onemogoča shranitev entitete. S tem parametrom je možno upravljati tudi, ko so atributu že pripisane vrednosti. Možno ga je le izključiti. Dokler atribut nima pripisanih vrednosti je s parametrom možno prosto upravljati.

## PickList

Vrednosti atributa so vnaprej določene zato ročni vnos izven seznama dovoljenih vrednosti ni možen. Seznam dovoljenih vrednosti atributa določimo ob nastavitvi strežnika IMiS®/ARChive Server.

Ko so seznamu enkrat pripisane vrednosti, jih lahko le dodajamo. Dokler atribut nima vrednosti lahko vrednosti tudi odvezujemo.

Dodatno lahko vsaki vrednosti določimo:

- **Atribute:**
  - »alias«: sinonim, uporabniku prijazen naziv vrednosti, ki ga odjemalci lahko uporabijo za izbire vrednosti.
  - »alias.xx\_YY«: preveden sinonim, uporabniku prijazen naziv vrednosti, preveden v področje, ki ga identificira identifikator xx\_YY. Odjemalci lahko uporabijo to vrednost za izbiro vrednosti, ko odjemalec deluje v področnih nastavitvah xx\_YY. Področni identifikatorji xx\_YY so strukturirani po ISO standardu 639 ([http://en.wikipedia.org/wiki/ISO\\_639](http://en.wikipedia.org/wiki/ISO_639)).
  - »default«: privzeta vrednost atributa v primeru novih entitet. To lastnost atributa lahko odjemalci uporabijo v uporabniških vmesnikih za prikaz privzete vrednosti atributa.
- **Pogoje:** Navedemo pogoje, pod katerimi je neka vrednost dovoljena. Uporabimo lahko sintakso parov pogojev ali samo vrednost, če želimo, da se nanaša na atribut, kateremu so pripisani pogoji.

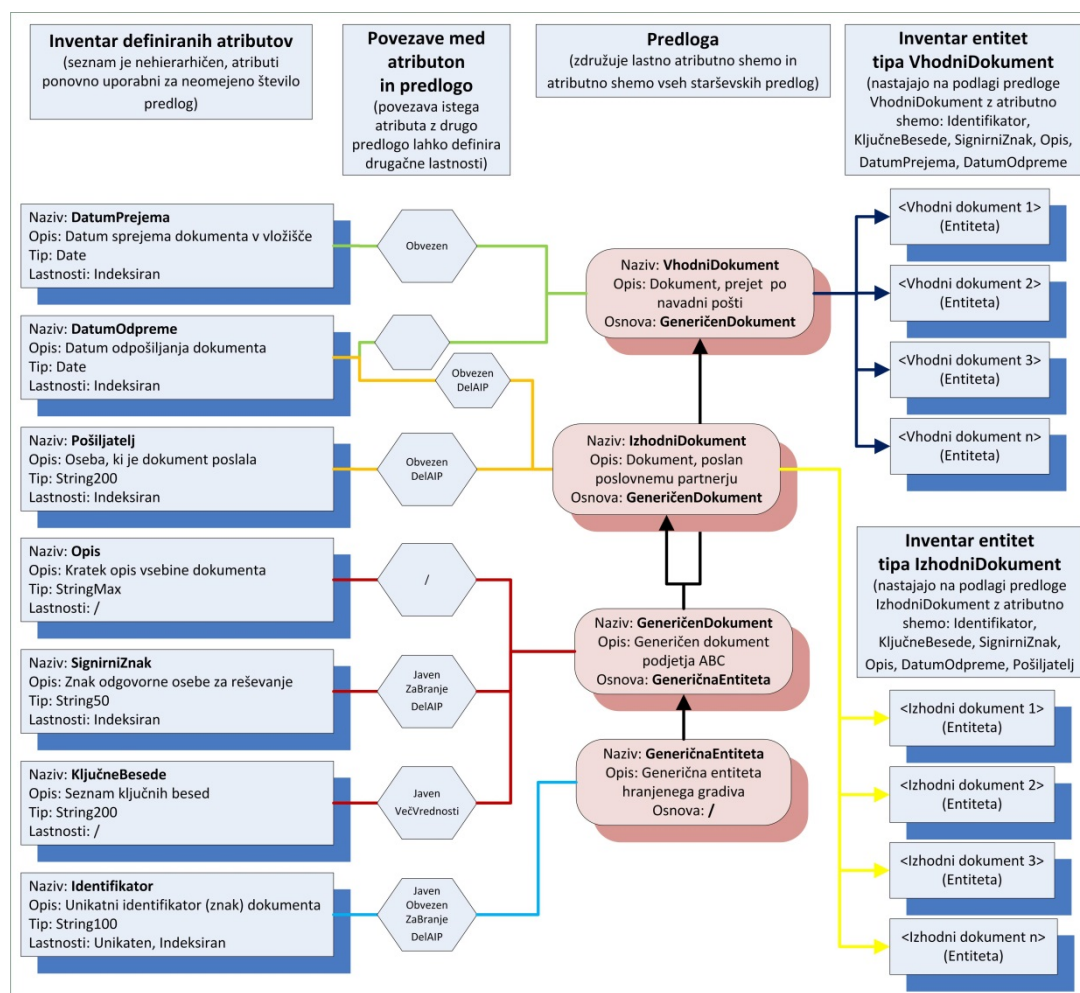
### Primeri:

- *"1:{default,alias="Opened",alias.sl\_SI="Odprto"} – Vrednost atributa »1« identificirata njegova sinonima "Opened" in preveden v slovenščino "Odprto" in je privzet za nove entitete. Pogojev, kdaj je na voljo, nima določenih.*
- *"2:{alias="Closed",alias.sl\_SI="Zaprto"}:{"": "1"} – Vrednost atributa »2« identificirata njegova sinonima "Closed" in preveden v slovenščino "Zaprto".  
Na voljo je pod pogojem, da atribut nima vrednosti (nova entiteta) ali ko je njegova vrednost 1.*

### 3.2.3 Povezava s predlogami

Atribut samostojno ni sposoben hrambe metapodatkov, je le osnova, oziroma izvor kontejnerja (angl. Container) podatkov. Kontejner vrednosti metapodatka dokončno določa vzpostavljena povezava med atributom in predlogo. Poenostavljeno gledano so predloge nastavitve, na podlagi katerih nastajajo v arhivu entitete. Za več informacij glej poglavje [Predloge](#). V povezavi z atributom se je potrebno zavedati tudi koncepta dedovanja predlog.

Dedovanje bistveno vpliva na razumevanje metapodatkovnih shem izvedenih predlog. Osnovni element metapodatkovne sheme entitete je povezava med predlogo in atributom. Ta določa t.i. »pogodbo« oziroma vse parametre in omejitve, ki se jih morajo vnesele metapodatkovne vrednosti za nek atribut držati, če se jih želi vnesti v atribut, ki jih vsebuje.



Slika 2: Logične povezave med atributi, predlogami in entitetami

Model omogoča ponovno uporabo istega atributa v različnih predlogah, pri čemer je možno nekatere parametre atributa določati na nivoju povezave.

Ti parametri so:

- »Validation expression«: Niz UTF-8 znakov, ki predstavljajo regularni izraz (angl. Regular expression) s katerim se nove ali spremenjene vrednosti atributa preverjajo. Več o sintaksi in pravilih na naslovu: [http://en.wikipedia.org/wiki/Regular\\_expression](http://en.wikipedia.org/wiki/Regular_expression). Ta izraz nadomesti izraz, nastavljen na nivoju atributa. Tako se preverjanje glede na izraz atributa nadomesti z izrazom na nivoju povezave med atributom in predlogo.
- »Sequence«: Sekvenca atributa v metapodatkovni shemi predloge.  
Gre za vrstni red atributa v shemi pri čemer je potrebno upoštevati naslednja pravila:
  1. shema vsake starševske predloge ima svoj sekvenčni red, ki ni odvisen od starševske predloge in/ali morebitnih predlog, ki iz nje nastanejo;
  2. atributi sheme korenske starševske predloge so na začetku konsolidirane atributne sheme;
  3. atributi sheme izvedene predloge, iz katere nastajajo entitete, so na koncu konsolidirane atributne sheme te predloge.
- »PickList values«: V kolikor je to potrebno, je možno nadomestiti nabor vnaprej določenih vrednosti atributa, ki so mu določene globalno. Seznam je shranjen v kontekstu povezave med atributom in predlogo. Ročni vnos vrednosti izven seznama dovoljenih vrednosti ni dovoljen. Seznam dovoljenih vrednosti atributa določamo ob nastavitvi produkta pri čemer lahko seznamu vrednosti le dodajamo, ko so mu enkrat pripisane vrednosti. Dokler vrednosti nima, je možno tudi odvzemanje vrednosti.  
Za več informacij glej poglavje [Parametri atributov / PickList](#).
- »Parameters«: dodatni parametri atributa, ki poleg njegovega podatkovnega tipa dodatno uokvirjajo pripisane vrednosti so opisne v nadaljevanju.

## Public

Javni atribut. Vrednosti atributa v okviru neke entitete so javnega značaja in dostopne tudi entitetam imenika (uporabniki, skupine), ki sicer nimajo pravic dostopa do entitete.

S tem parametrom je možno upravljati v celotnem življenjskem ciklu atributa in/ali predloge, s katero je atribut povezan. Upošteva se pri prvem odpiranju entitete s strani uporabnika po spremembi nastavitve.

### Multivalue

Atribut, ki lahko vsebuje več vrednosti. Atributu je v okviru ene entitete možno pripisati več vrednosti. V kolikor ta parameter ni določen, je možno atributu v okviru ene entitete pripisati natančno eno ali nobene vrednosti. S tem parametrom je možno upravljati v celotnem življenjskem ciklu atributa in/ali predloge s katero je atribut povezan, dokler ni ustvarjena prva entiteta na podlagi predloge.

Po tem je možno parameter kadarkoli vključiti in nikoli izključiti. Upošteva se pri prvem odpiranju entitete s strani uporabnika po spremembi nastavitve.

### Required

Vrednost atributa mora biti ob shranjevanju entitete nujno prisotna. Shranjevanje entitete bo torej zavrnjeno, če shranjevalec entitete v okviru atributa ne določi vsaj ene veljavne vrednosti. S tem parametrom je možno upravljati v celotnem življenjskem ciklu atributa in/ali predloge, s katero je atribut povezan dokler ni ustvarjena prva entiteta na podlagi predloge.

Po tem je možno parameter kadarkoli izključiti in nikoli vključiti. Upošteva se pri prvem odpiranju entitete s strani uporabnika po spremembi nastavitve.

### ReadOnly

Parameter »samo za branje« (angl. ReadOnly) označuje, ali se vrednost atributa lahko spreminja ali ne. Veljavne vrednosti parametra so naslednje:

- »0« (ReadOnlyDisabled): vrednost atributa se kadarkoli lahko spreminja.
- »1« (ReadOnlyAfterCreate): vrednost atributa se po prvi shranitvi dokumenta ne sme več spreminjati.
- »2« (ReadOnlyAfterCheckin): vrednost atributa se lahko spreminja samo, ko je entiteta nova, ali pa skozi proces verzioniranja (izdelava in vložitev osnutka).
- »3« (ReadOnlyAlways): vrednosti atributa se ne sme spreminjati.

S tem parametrom je možno upravljati v celotnem življenjskem ciklu atributa in/ali predloge, s katero je atribut povezan. Upošteva se pri prvem odpiranju entitete s strani uporabnika po spremembi nastavitve.

### Inherited

Vrednosti atributa dedujejo vrednosti iz nadrejene hierarhije. V kolikor v entiteti niso določene eksplicitne vrednosti, se te dedujejo iz prve nadrejene entitete, ki ima določene eksplicitne vrednosti. Eksplicitne vrednosti v celoti nadredijo podedovane vrednosti in učinkujejo za vse podrejene entitete.

Dedovanje vrednosti deluje po principu referenc. Če se vrednost podedovanega atributa spremeni v nadrejeni hierarhiji neke entitete, začne nemudoma učinkovati za vse spremenjeni entiteti podrejene entitete, ki nimajo pripisanih eksplicitnih vrednosti.

Vrednosti atributa se dedujejo le v primeru, ko ima entiteta in njej neposredno nadrejena entiteta atribut v svoji shemi atributov. Na dedovanje vrednosti atributov ne vplivajo dostopne pravice za metapodatke. Za več informacij glej poglavje [Dostopne pravice za metapodatke](#).

S tem parametrom je možno upravljati v celotnem življenjskem ciklu atributa in/ali predloge, s katero je atribut povezan. Upošteva se pri prvem odpiranju entitete s strani uporabnika po spremembi nastavitve.

### AppendOnly

Vrednosti atributa je možno k obstoječim le dodajati. Odjemalec s strani strežnika dobi vse vrednosti, pri zapisu pa sprejema le nove vrednosti, ki jih doda obstoječim.

S tem parametrom je možno upravljati v celotnem življenjskem ciklu atributa in/ali predloge, s katero je atribut povezan. Upošteva se pri prvem odpiranju entitete s strani uporabnika po spremembi nastavitve.

### IncludeInAIP

Vrednosti atributa so del arhivskega informacijskega paketa. V postopku zagotavljanja avtentičnosti hranjenega gradiva, postanejo vrednosti atributov, katerim je ta parameter vključen, del arhivskega informacijskega paketa. Za več informacij glej poglavje [AIP](#).

S tem parametrom je možno upravljati v celotnem življenjskem ciklu atributa in/ali predloge, s katero je atribut povezan. Nastavitev strežnik upošteva, ko začne postopek zagotavljanja avtentičnosti in nespremenjenosti gradiva, v času njegove hrambe.

### IsNonEmpty

Vrednost atributa ne sme biti prazna. Definicija prazne vrednosti je odvisna od vrste atributa. Tako je prazna vrednost za vrsto »String10« prazen niz, prazna vrednost za vrsto »File« pa predstavlja prazno datoteko (datoteko velikosti 0 bajtov). S tem parametrom je možno upravljati v celotnem življenjskem ciklu atributa in/ali predloge. To velja za atribut, ki je povezan dokler ni ustvarjena prva entiteta na podlagi predloge. Po tem je možno parameter kadarkoli izključiti in nikoli vključiti. Upošteva se pri prvem odpiranju entitete s strani uporabnika po spremembi nastavitve.

### Versionable

Vrednosti atributa se lahko verzionira. Verzioniranje pomeni, da atribut za določeno različico dokumenta vsebuje nabor vrednosti, ki so lahko enake ali različne od nabora vrednosti druge različice. S tem parametrom je možno upravljati v celotnem življenjskem ciklu atributa in/ali predloge, s katero je atribut povezan.

Slednje velja vse dokler ni ustvarjena prva entiteta na podlagi predloge (parameter se lahko spreminja samo na predlogah, iz katerih lahko nastanejo dokumenti). Parameter ni kompatibilen z »Required« in »Unique« parametri.

#### Omejitve:

*Pri konfiguraciji atributov na predlogah za katere že obstajajo entitete, veljajo naslednje omejitve:*

- *Pri dodajanju novega atributa, lastnost »Required« ne sme biti nastavljena na »True«.*  
*V kolikor je nastavljena na »False«, to povzroči nekonsistenco z vsemi obstoječimi entitetami, saj le-te ne smejo imeti vrednosti za nov atribut.*
- *Pri spreminjanju obstoječega atributa na predlogi veljajo naslednje omejitve:*
  - *sprememba lastnosti atributa »Multivalued« iz »True« v »False« ni dovoljena zaradi nekonsistence z vsemi obstoječimi entitetami, ki imajo nastavljenih več vrednosti za ta atribut;*
  - *sprememba lastnosti atributa »Required« iz »False« v »True« ni dovoljena zaradi nekonsistence z vsemi obstoječimi entitetami, ki nimajo vrednosti za ta atribut;*
  - *sprememba lastnosti atributa »Inherited« iz »True« v »False« ni dovoljena zaradi nekonsistence z vsemi obstoječimi entitetami, ki nimajo eksplicitne vrednosti za ta atribut.*
- *Brisanje atributa iz predloge, za katerega obstajajo entitete ni dovoljeno.*

*Vse ostale kombinacije so dovoljene.*



### SignatureDisposition

Parameter določa stanje digitalno podpisane vsebine, katera se lahko shranjuje v atribut.

Veljavne so naslednje vrednosti:

- »0« (None): dovoljena je vsaka vsebina (podpisana ali nepodpisana).
- »1« (Signed): dovoljena je samo vsebina, ki je digitalno podpisana in jo strežnik IMiS ARChive lahko preveri.
- »2« (Valid): dovoljena je samo vsebina, ki je digitalno podpisana, ki jo strežnik IMiS ARChive lahko preveri in je ob preverjanju veljavna (veljaven digitalni podpis, veljaven certifikat v času preverjanja...).

Parameter je trenutno veljaven samo za attribute tipa »FILE«. S tem parametrom je možno upravljati v celotnem življenjskem ciklu atributa in/ali predloge,

### **3.2.4 Poimenovanje**

Vsak atribut je potrebno poimenovati s poljubnim unikatnim nizom UTF-8 znakov, dolgim do 256 bajtov UTF-8 znakov. Dovoljeni so vsi znaki, upoštevati pa je potrebno naslednje omejitve:

- Naziv atributa ne sme biti prazen.
- Predpone (imenski prostori) »int:«, »sys:«, »imp:«, »trf:« so rezervirane in uporaba ni dovoljena. Poizkus ustvarjanja tako imenovanega atributa bo zavrnjen.
- Imena atributov naj bodo smiselna in primerno kratka.
- Dovoljene so predpone oziroma imenski prostori, ki jih od imena delimo z znakom »:«. Dovoljene so gnezdene predpone (npr. »global:accounting:InvoiceNo«).
- Sistem ne predpisuje pravil poimenovanja atributov vendar je smiselno, da ga določite na nivoju internega pravilnika upravljanja s strežnikom IMiS®/ARChive Server.

Dodatno je smiselno atributu določiti opis, opcijski niz UTF-8 znakov, dolg do 512 bajtov UTF-8 znakov, ki naj bo logičen opis, kaj atribut predstavlja in kakšne vrednosti so dovoljene, če obstajajo omejitve. Podatek se prenaša na odjemalce, ki ga lahko prikazujejo v uporabniškem vmesniku. Lokalizacija na nivoju strežnika ni podprta.

V ta namen lahko uporabimo nize znakov kot konstante, ki jih glede na regionalne nastavitve na odjemalcih primerno prevajate.

### 3.2.5 Sistemski atributi

Na delovanje arhivskega sistema močno vplivajo tudi nekateri atributi in njihove vrednosti. Te attribute imenujemo »Sistemski atributi«, ki so v nasprotju z nastavljivimi atributi v sistemu vnaprej določeni, njihove lastnosti pa nespremenljive.

Razlog za to je, da njihova prisotnost/odsotnost, vrednosti in lastnosti vplivajo na delovanje strežnika, življenjski cikel entitet in postopke hrambe gradiva.

Sistemski atributi so vgrajeni v strežnik IMiS®/ARChive Server in z njimi ni potrebno upravljati.

Povezani so na sistemske predloge, iz katerih izvedemo predloge,

s katerimi ustvarjamo entitete. Ustvarjene entitete jih zato implicitno pridobijo v atributne sheme. Tako lahko vplivajo na njihov življenjski cikel in prisotnost sistemskih metapodatkov.

Vrednosti nekaterih sistemskih atributov določa strežnik v postopkih ustvarjanja, spreminjanja in shranjevanja entitet. Nekaterim pa je uporabnik dolžan vnesti vrednost(i), saj le tako lahko uspešno upravlja z življenjskim ciklom entitete.

V nadaljevanju so podrobneje opisani sistemski atributi:

#### Atribut »sys:ExternalIds«

Tip: String100

Lastnosti: Unique, Searchable, Public, MultiValue, IsNonEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti. Ena entiteta lahko vsebuje do 65536 zunanjih identifikatorjev.

Uporaba: Razred, Zadeva, Dokument, Dokument v postopku odbiranja in izločanja

Opis: Unikatni zunanji identifikatorji entitete. Uporabni kot podatki za dostop do entitete (odpiranje). Klicatelj je odgovoren za unikatnost identifikatorja, shranitev ni dovoljena, v kolikor ima druga entiteta že pripisan enak zunanji identifikator.

### Atribut »sys:Title«

Tip: String200

Lastnosti: Searchable, Public, Required (razen pri referencah), IsNotEmpty (razen pri referencah), ReadOnlyAlways (samo pri kopijah politik hrambe in izbrisanih entitetah).

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument, Dokument v postopku odbiranja in izločanja, Politike hrambe, Postopek odbiranja in izločanja, Kopija politike hrambe, Zadržanje postopka odbiranja in izločanja, Kontejner sistemskih entitet, Reference.

Opis: Obvezen naziv (naslov) entitete, ki jo opisuje. Spremenljiv v celotnem življenjskem ciklu entitete. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:Description«

Tip: String200

Lastnosti: Public, ReadOnlyAlways (samo pri kopijah politik hrambe in izbrisanih entitetah).

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument, Dokument v postopku odbiranja in izločanja, Politike hrambe, Postopek odbiranja in izločanja, Kopija politike hrambe, Zadržanje postopka odbiranja in izločanja, Kontejner sistemskih entitet.

Opis: Neobvezen kratek opis entitete. Spremenljiv v celotnem življenjskem ciklu entitete. Če pride do izbrisa entitete, postane obvezen. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:Content«

Tip: File

Lastnosti: Public (samo v Pregledu postopkov odbiranja in izločanja in Kopijah politike hrambe), Multivalued, IncludeInAip, Searchable, ReadOnlyAlways (samo pri Kopijah politike hrambe).

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti. Ena entiteta lahko vsebuje do 65536 vrednosti.

Uporaba: Dokument, Dokument v postopku odbiranja in izločanja, Politike hrambe, Postopek odbiranja in izločanja, Kopija politike hrambe.

Opis: Atribut predstavlja kontejner digitalnih vsebin, zmožen hranjenja opisovalnih struktur vsebin. Atribut je vključen v skupino atributov, ki se indeksirajo. Specifično za File atribut je, da to predstavlja indeks po polnem besedilu (Full Text Index).

V kolikor je vključen sistem za zagotavljanje avtentičnosti in nespremenljivosti v času hrambe gradiva, postanejo prstni odtisi vrednosti iz tega kontejnerja del arhivskega informacijskega paketa (AIP). Spremenljiv je v celotnem življenjskem ciklu entitete. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:Keywords«

Tip: String30

Lastnosti: Searchable, Public, MultiValue, IsNotEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti. Ena entiteta lahko vsebuje do 65536 vrednosti.

Uporaba: Razred, Zadeva, Dokument, Dokument v postopku odbiranja in izločanja, Postopek odbiranja in izločanja.

Opis: Neobvezne ključne besede, ki določajo entiteto. Spremenljiv je v celotnem življenjskem ciklu entitete. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:SecurityClass«

Tip: UInt32

Lastnosti: Searchable, Public, ReadOnly, Inherited, PickList, IsNonEmpty

Omejitve: Veljavne vrednosti (prednastavljene):

- 1, alias »Unclassified«: Entiteta nima posebej določene stopnje tajnosti.
- 2, alias »Restricted«: Entiteta je interne narave. Do nje lahko dostopajo le uporabniki s stopnjo tajnosti »Restricted« ali višjo.
- 3, alias »Confidential«: Entiteta je zaupne narave. Do nje lahko dostopajo le uporabniki s stopnjo tajnosti »Confidential« ali višjo.
- 4, alias »Secret«: Entiteta je tajne narave. Do nje lahko dostopajo le uporabniki s stopnjo tajnosti »Secret« ali višjo.
- 5, alias »Top Secret«: Entiteta je strogo tajne narave. Do nje lahko dostopajo le uporabniki s stopnjo tajnosti »Top Secret« ali višjo.

Stopnje tajnosti so sicer nastavljive glede na pravilnike arhiviranja uporabnika arhiva.

Neveljavna vrednost je 0, ki je rezervirana in interne narave, zato se med veljavne vrednosti ne sme vnašati.

Uporaba: Razred, Zadeva, Dokument

Opis: Sistemski atribut omejuje dostop do entitete, ki ga določa. Entitete, do katere uporabnik z svojo stopnjo tajnosti nima dostopa, se uporabniku v celoti skrije. Uporabnik ne more potrditi njenega obstoja ali izvajati katerekoli aktivnosti, ki bi njen obstoj potrdila. To poleg branja njenih atributov, odpiranja, brisanja, premikanja ipd., velja tudi za ustvarjanje entitet pod njo.

Vrednost stopnje tajnosti se deduje po podrejenih entitetah, če jih same ne določajo.

Podrejenim entitetam je možno določiti lastno stopnjo tajnosti, vendar le do nivoja nadrejene, torej lahko je enaka ali nižja od stopnje tajnosti nadrejene entitete.

### Atribut »sys:Status«

Tip: UInt32

Lastnosti: Public, Required, ReadOnlyAfterCreate, IsNotEmpty, Searchable, PickList, Inherited, [Inherited lastnost v primeru Postopkov odbiranja in izločanja ne velja].

Omejitve: Veljavne vrednosti:

- 1, alias »Opened«: entiteto je dovoljeno spreminjati in pod njo ustvariti podrejene entitete.
- 2, alias »Closed«: entiteta ne dovoljuje spreminjana in ustvarjanja podrejenih entitet.

Prisotnost atributa je obvezna na razredu, dokumentu pod razredom ter zadevah.

Uporaba: Razred, Zadeva, Dokument, Postopek odbiranja in izločanja

Opis: Atribut predstavlja stanje entitete, oziroma njen status. Ta se odraža v postopkih, ki so dovoljeni ali prepovedani na entiteti. V odprtem stanju je entiteto možno spreminjati in z njo prosto upravljati. Nivo dostopa določajo dostopne pravice.

Ko je statusno entiteta enkrat zaprta, so ne glede na dostopne pravice spreminjanja onemogočene. V kolikor je omogočen servis za zagotavljanje avtentičnosti in nespremenjenosti v času hrambe, je zapiranje entitete signal za začetek postopka zagotavljanja avtentičnosti za konkretno entiteto in morebitne podrejene entitete. Za več informacij glej poglavje [Življenjski cikel](#).

### Atribut »sys:Creator«

Tip: DirectoryEntity

Lastnosti: Searchable, Public, Required, ReadOnly, IsNonEmpty, Inherited (v primeru Kontejnerja sistemskih entitet).

Omejitve: Vrednost določa strežnik in ni spremenljiva. Vrednost vedno predstavlja registrirano entiteto iz imenika.

Uporaba: Razred, Zadeva, Dokument, Dokument v postopku odbiranja in izločanja, Politike hrambe, Postopek odbiranja in izločanja, Kopija politike hrambe, Zadržanje postopka odbiranja in izločanja, Kontejner sistemskih entitet.

Opis: Vrednost predstavlja entiteto imenika - uporabnika, ki je entiteto ustvaril. Podatek je nespremenljiv, določen pri ustvaritvi entitete s strani strežnika. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:Owner«

Tip: DirectoryEntity

Lastnosti: Searchable, Public, IsNonEmpty

Omejitve: Dovoljene vrednosti so identifikatorji registriranih entitet iz imenika.

Uporaba: Razred, Zadeva, Dokument, Dokument v postopku odbiranja in izločanja, Postopek odbiranja in izločanja.

Opis: Vrednost predstavlja entiteto imenika – uporabnika ali skupino, ki je odgovorna za entiteto (lastnik). Podatek je spremenljiv v celotnem življenjskem ciklu entitete.

Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije. Izjema je operacija »Vložitev osnutka«, kjer se preverja ali je uporabnik, ki akcijo izvaja prisoten v tem atributu.

### Atribut »sys:Significance«

Tip: UInt32

Lastnosti: Searchable, Public, Inherited, PickList, IsNonEmpty

Omejitve: Veljavne vrednosti:

- 1, alias »Vital«: Entiteta, vitalnega pomena za lastnika arhiva. Entiteto je prepovedano izbrisati preko administratorskega zahtevka ali v postopku odbiranja in izločanja. Entiteta je opsijsko pod posebnim režimom varnostnega arhiviranja.

- 2, alias »Permanent«: Entitete ni dovoljeno izbrisati ali preko administratorskega zahtevka ali v postopku odbiranja in izločanja. Gre le za opozorilo, ki ga administrator lahko upošteva ali se odloči drugače.
- 3, alias »Retain«: Predstavlja opozorilo odgovorni osebi, ki izvaja odbiranje in izločanje. V postopku izločanja, da naj postopek izločitve na dotični entiteti zadrži.
- 4, alias »Delete«: Priporočilo administratorju, naj entiteto izbriše mimo postopka odbiranja in izločanja. Priporočilo lahko izda vsakokratni urejevalec entitete. Navadno se na tak način izbrišejo entitete, ki so bile napačno vnesene ali pa gre za zahtevan izbris na zahtevo lastnika dokumenta (v primeru osebnih podatkov, ...).

Uporaba: Razred, Zadeva, Dokument

Opis: Atribut predstavlja pomembnost entitete v kontekstu lastnika arhiva.

#### Atribut »sys:Opened«

Tip: DateTime

Lastnosti: Searchable, Public, ReadOnly, IsNotEmpty

Omejitve: Vrednost določa strežnik in ni spremenljiva. Vedno je prisoten ob sistemskem atributu »sys:Status«.

Uporaba: Razred, Zadeva, Dokument, Postopek odbiranja in izločanja.

Opis: Vrednost predstavlja datum in čas ko je atribut »sys:Status« dotične entitete dobil vrednost »Opened«. Za več informacij glej poglavje [Sistemski atribut »sys:Status«](#).

Podatek je nespremenljiv, določen s strani strežnika. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:Closed«

Tip: DateTime

Lastnosti: Searchable, Public, ReadOnly, Inherited, IsNotEmpty, Inherited (lastnost v primeru Postopkov odbiranja in izločanja ne velja).

Omejitve: Vrednost določa strežnik in ni spremenljiva. Vedno je prisoten ob sistemskem atributu »sys:Status«.

Uporaba: Razred, Zadeva, Dokument, Postopek odbiranja in izločanja.

Opis: Vrednost predstavlja datum in čas ko je atribut »sys:Status« dotične entitete dobi vrednost »Closed«. Za več informacij glej poglavje [Sistemski atribut »sys:Status«](#).

Podatek je nespremenljiv, določen s strani strežnika. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:CommitLog«

Tip: StringMax

Lastnosti: ReadOnlyAlways, MultiValue, AppendOnly, IncludeInAIP, IsNonEmpty

Omejitve: Vrednost določa strežnik in ni spremenljiva.

Uporaba: Razred, Zadeva, Dokument, Dokument v postopku odbiranja in izločanja, Politike hrambe, Postopek odbiranja in izločanja, Kopija politike hrambe.

Opis: Vrednost predstavlja vsakokratni dnevnik dogodkov samodejnih dejanj preverjanja strežnika ob shranitvi entitete. Poleg samega tekstovnega dnevnika, vsebuje še zajete elektronske podpise, vsebovane v arhiviranih vsebinah, elektronska potrdila celotne verige potrdil, ki so izdale potrdilo, s katerim je bil elektronski podpis ustvarjen ter trenutne sezname preklicanih potrdil vseh izdajateljev omenjenih potrdil. Podatki so nespremenljivi, določeni s strani strežnika. Podatki tega atributa se vključijo v arhivski informacijski paket in so predmet dolgoročne hrambe gradiva v postopku zagotavljanja avtentičnosti. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:move:Reason«

Tip: String200

Lastnosti: Searchable, MultiValue, ReadOnlyAlways, AppendOnly, IsNonEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednosti predstavljajo razloge za vsakokratni premik (re-klasifikacijo) entitete. Gre za vrednost, ki je posredovana s strani uporabnika ob premiku entitete v hierarhiji razvrščanja gradiva. Istoležne vrednosti lahko povezujemo z atributoma »sys:move:Agent«, »sys:move:DateTime« in »sys:move:ClassificationCode« za popolnejšo informacijo o premiku entitete v hierarhiji razvrščanja gradiva.

Vrednost se vnese v metapodatke entitete, ki se premika, ne pa tudi v vse njej podrejene entitete. Za več informacij glej poglavje [Življenjski cikel](#).

Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.



### Atribut »sys:move:Agent«

Tip: DirectoryEntity

Lastnosti: Searchable, MultiValue, ReadOnlyAlways, AppendOnly, IsNotEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Vrednosti vedno predstavljajo identifikatorje registriranih entitet iz imenika.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednosti predstavljajo vsakokratne entitete imenika (uporabnike), ki so izvajali premike (reklasifikacijo) entitete. Gre za vrednost, ki jo strežnik samodejno določi iz uporabniške seje, oziroma iz prijavnih podatkov uporabnika, ki je vsakokratni premik izvedel. Isto ležne vrednosti lahko uporabnik povezuje z atributoma »sys:move:Reason«, »sys:move:DateTime« in »sys:move:ClassificationCode« za popolnejšo informacijo o premiku entitete v hierarhiji razvrščanja gradiva.

Vrednost se vnese v metapodatke entitete, ki se premika, ne pa tudi v vse njej podrejene entitete. Za več informacij glej poglavje [Življenjski cikel](#). Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:move:DateTime«

Tip: DateTime

Lastnosti: Searchable, MultiValue, ReadOnlyAlways, AppendOnly, IsNotEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednosti predstavljajo vsakokratni datum in čas, ko se je izvedel premik (reklasifikacija) entitete. Gre za vrednost, ki jo strežnik samodejno določi.

Isto ležne vrednosti lahko uporabnik povezuje z atributoma »sys:move:Reason«, »sys:move:Agent« in »sys:move:ClassificationCode« za popolnejšo informacijo o premiku entitete v hierarhiji razvrščanja gradiva. Vrednost se vnese v metapodatke entitete, ki se premika, ne pa tudi v vse njej podrejene entitete.

Za več informacij glej poglavje [Življenjski cikel](#). Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:move:ClassificationCode«

Tip: String200

Lastnosti: Searchable, MultiValue, ReadOnlyAlways, AppendOnly, IsNotEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednosti predstavljajo vsakokratno klasifikacijsko oznako entitete ob premiku (reklasifikaciji). Gre za vrednost, ki jo strežnik samodejno določi.

Isto ležne vrednosti lahko uporabnik povezuje z atributoma »sys:move:Reason«, »sys:move:Agent« in »sys:move:DateTime« za popolnejšo informacijo o premiku entitete v hierarhiji razvrščanja gradiva. Vrednost se vnese v metapodatke entitete, ki se premika, ne pa tudi v vse njej podrejene entitete.

Za več informacij glej poglavje [Življenjski cikel](#). Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:del:Reason«

Tip: String200

Lastnosti: Searchable, Public, Required, ReadOnlyAlways, IsNotEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednost predstavlja razlog za izločanje ali izbris entitete. Gre za vrednost, ki je posredovana s strani uporabnika ob izbrisu entitete, v primeru izločanja pa se prenese iz postopka odbiranja in izločanja. Za več informacij glej poglavje [Življenjski cikel](#).

Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:del:Agent«

Tip: DirectoryEntity

Lastnosti: Searchable, Public, Required, ReadOnlyAlways, IsNotEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Vrednosti vedno predstavljajo identifikatorje registriranih entitet iz imenika.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednost predstavlja entiteto imenika (uporabnike), ki je izvedel izločanje ali izbris entitete. Gre za vrednost, ki jo strežnik samodejno določi iz uporabniške seje, oziroma prijavnih podatkov uporabnika, ki je akcijo izvedel. Za več informacij glej poglavje [Življenjski cikel](#). Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:del:DateTime«

Tip: DateTime

Lastnosti: Searchable, Public, Required, ReadOnlyAlways, IsNonEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednost predstavlja datum in čas, ko je izvedeno izločanje ali izbris entitete. Gre za vrednost, ki jo strežnik samodejno določi.

Za več informacij glej poglavje [Življenjski cikel](#). Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:del:ClassificationCode«

Tip: String200

Lastnosti: Searchable, Public, Required, ReadOnlyAlways, IsNonEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednost predstavlja klasifikacijsko oznako entitete v času izbrisa ali izločanja.

Gre za vrednost, ki jo strežnik samodejno zajame.

Za več informacij glej poglavje [Življenjski cikel](#). Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:del:Reference«

Tip: String200

Lastnosti: Searchable, Public, ReadOnlyAlways

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednost predstavlja referenco na prenešeno entiteto. Gre za vrednost, ki jo uporabnik vnese po uspešnem prenosu entitete v postopku odbiranja in izločanja. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:scc: Reason«

Tip: String200

Lastnosti: Searchable, MultiValue, ReadOnlyAlways, AppendOnly, IsNonEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednosti predstavljajo razloge za vsakokratno spremembo stopnje tajnosti entitete.

Gre za vrednost, ki je posredovana s strani uporabnika ob spremembi stopnje tajnosti.

Istoležne vrednosti lahko povežemo z atributoma »sys:scc:Agent«, »sys:scc:DateTime«,

»sys:scc:From« in »sys:scc:To« za popolnejšo informacijo o spremembi stopnje tajnosti entitete.

Vrednost se vnese v metapodatke entitete, ki se ji spremeni stopnja tajnosti, ne pa tudi v vse njej podrejene entitete. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:scc:Agent«

Tip: DirectoryEntity

Lastnosti: Searchable, MultiValue, ReadOnlyAlways, AppendOnly, IsNonEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Vrednosti vedno predstavljajo identifikatorje registriranih entitet iz imenika.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednosti predstavljajo vsakokratne entitete imenika (uporabnike), ki so izvajali spremembe stopenj tajnosti entitete. Gre za vrednost, ki jo strežnik samodejno določi iz uporabniške seje, oziroma iz prijavnih podatkov uporabnika, ki je stopnjo tajnosti vsakokrat izvedel. Isto ležne vrednosti lahko uporabnik povezuje z atributoma »sys:scc:Reason«,

»sys:scc:DateTime«, »sys:scc:From« in »sys:scc:To« za popolnejšo informacijo o spremembi stopnje tajnosti entitete. Vrednost se vnese v metapodatke entitete, ki se ji spremeni stopnja tajnosti, ne pa tudi v vse njej podrejene entitete. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:scc: DateTime«

Tip: DateTime

Lastnosti: Searchable, MultiValue, ReadOnlyAlways, AppendOnly, IsNonEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

**Opis:** Vrednosti predstavljajo vsakokratni datum in čas, ko se je izvedela sprememba stopnje tajnosti entitete. Gre za vrednost, ki jo strežnik samodejno določi. Isto ležne vrednosti lahko administrator povezuje z atributoma »sys:scc: Reason«, »sys:scc: Agent«, »sys:scc: From« in »sys:scc: To« za popolnejšo informacijo o spremembi stopnje tajnosti entitete. Vrednost se vnese v metapodatke entitete, ki se ji spremeni stopnja tajnosti, ne pa tudi v vse njej podrejene entitete. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:scc:From«

**Tip:** UInt32

**Lastnosti:** Searchable, MultiValue, ReadOnlyAlways, AppendOnly, PickList

**Omejitve:** Vrednosti morajo ustrezati vsem vrednostim iz atributa "sys:SecurityClass", ki so kadarkoli od namestitve produkta obstajale. Dodatno je potrebno določiti vrednost za "0", ki je vnaprej nastavljena na sinonim »Unspecified«, možno pa jo je tudi spremeniti.

**Uporaba:** Razred, Zadeva, Dokument

**Opis:** Vrednosti predstavljajo vsakokratno stopnjo tajnosti pred spremembo le-te. Gre za vrednost, ki jo strežnik samodejno določi iz vrednosti atributa "sys:scc" pred njegovo spremembo. Isto ležne vrednosti lahko uporabnik povezuje z atributoma »sys:scc: Reason«, »sys:scc: Agent«, »sys:scc: DateTime« in »sys:scc: To« za popolnejšo informacijo o spremembi stopnje tajnosti entitete. Vrednost se vnese v metapodatke entitete, ki se ji spremeni stopnja tajnosti, ne pa tudi v vse njej podrejene entitete. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:scc:To«

**Tip:** UInt32

**Lastnosti:** Searchable, MultiValue, ReadOnlyAlways, AppendOnly, PickList

**Omejitve:** Vrednosti morajo ustrezati vsem vrednostim iz atributa »sys:SecurityClass«, ki so kadarkoli od namestitve produkta obstajale. Dodatno je potrebno določiti vrednost za »0«, ki je vnaprej nastavljena na sinonim »Unspecified«, možno pa jo je tudi spremeniti.

**Uporaba:** Razred, Zadeva, Dokument.

Opis: Vrednosti predstavljajo vsakokratno stopnjo tajnosti po spremembi le-te.

Gre za vrednost, ki jo strežnik samodejno določi iz vrednosti atributa »sys:scc« po njegovi spremembi. Isto ležne vrednosti lahko administrator povezuje z atributoma »sys:scc: Reason«, »sys:scc: Agent«, »sys:scc: DateTime« in »sys:scc: From« za popolnejšo informacijo o spremembi stopnje tajnosti entitete. Vrednost se vnese v metapodatke entitete, ki se ji spremeni stopnja tajnosti, ne pa tudi v vse njej podrejene entitete. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:EntityReference«

Tip: EntityReference

Lastnosti: Public, Multivalued, Required, Searchable

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Referenca (dokument).

Opis: Vrednosti predstavljajo unikatne identifikatorje entitet, ki so med seboj povezane kot reference. Za več informacij glej poglavje [Reference](#).

#### Atribut »sys:Category«

Tip: String200

Lastnosti: Public, Multivalued, Searchable

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Zadeva, Dokument.

Opis: Vrednosti atributa predstavljajo kategorije, po katerih se lahko entitete kategorizira. Za več informacij glej poglavje [Kategorije](#).

### 3.2.6 Atributi dokumentov elektronske pošte

Za arhiviranje elektronske pošte so v strežniku IMiS®/ARChive Server vnaprej določeni atributi in predloge, ki so namenjeni za hrambo metapodatkov o elektronskih sporočilih.

Ti atributi so na strežniku vnaprej določeni in z njihovimi lastnostmi ni možno upravljati.

#### Atribut »sys:eml:MessageId«

Tip: String100

Lastnosti: Searchable, ReadOnlyAlways.

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Dokument

Opis: Vrednost predstavlja unikatni identifikator sporočila, določenega s strani poštnega strežnika ob dostavi. Vrednost posreduje odjemalec, navadno ga izlušči iz samega sporočila elektronske pošte, čeprav je natančnost informacije odvisna od samega odjemalca.

Vrednost predstavlja vrednost iz atributa »message-id« sporočila po specifikaciji RFC 2822.

Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:eml:Date«

Tip: DateTime

Lastnosti: Searchable, ReadOnlyAlways.

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Dokument

Opis: Vrednost predstavlja datum in čas pošiljanja sporočila. Po specifikacijah je to trenutek, ko se pošiljatelj odloči, da je sporočilo primerno za pošiljanje in začne postopek pošiljanja sporočila. Vrednost posreduje odjemalec, navadno ga izlušči iz samega sporočila elektronske pošte, čeprav je natančnost informacije odvisna od samega odjemalca. Vrednost predstavlja vrednost iz atributa »orig-date« sporočila po specifikaciji RFC 2822. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:eml:From«

Tip: String200

Lastnosti: Searchable, MultiValue, ReadOnlyAlways, IsNonEmpty.

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Dokument

Opis: Vrednost predstavlja veljaven elektronski naslov pošiljatelja elektronskega sporočila. Vrednost posreduje odjemalec, navadno ga izlušči iz samega sporočila elektronske pošte, čeprav je natančnost informacije odvisna od samega odjemalca. Vrednost predstavlja vrednost iz atributa »from« sporočila po specifikaciji RFC 2822. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:eml:To«

Tip: String200

Lastnosti: Searchable, MultiValue, ReadOnlyAlways, IsNonEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Dokument

Opis: Vrednosti predstavljajo veljavne elektronske naslove prejemnikov elektronskega sporočila. Vrednosti posreduje odjemalec, navadno jih izlušči iz samega sporočila elektronske pošte, čeprav je natančnost informacije odvisna od samega odjemalca.

Vrednosti predstavljajo vrednosti iz atributa »to« sporočila po specifikaciji RFC 2822.

Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:eml:ToCC«

Tip: String200

Lastnosti: Searchable, MultiValue, ReadOnlyAlways, IsNonEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Dokument

Opis: Vrednosti predstavljajo veljavne elektronske naslove prejemnikov kopije elektronskega sporočila. Vrednosti posreduje odjemalec, navadno jih izlušči iz samega sporočila elektronske pošte, čeprav je natančnost informacije odvisna od samega odjemalca. Vrednosti predstavljajo vrednosti iz atributa »cc« sporočila po specifikaciji RFC 2822.

Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.



### Atribut »sys:eml:ToBCC«

Tip: String200

Lastnosti: Searchable, MultiValue, ReadOnlyAlways, IsNonEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Dokument

Opis: Vrednosti predstavljajo veljavne elektronske naslove skritih prejemnikov kopije elektronskega sporočila. Vrednosti posreduje odjemalec, navadno jih izlušči iz samega sporočila elektronske pošte, čeprav je natančnost informacije odvisna od samega odjemalca.

Vrednosti predstavljajo vrednosti iz atributa »bcc« sporočila po specifikaciji RFC 2822.

Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:eml:Subject«

Tip: String200

Lastnosti: Searchable, ReadOnlyAlways, IsNonEmpty.

Omejitve: ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Dokument

Opis: Vrednost predstavlja naziv zadeve elektronskega sporočila. Vrednost posreduje odjemalec, navadno ga izlušči iz samega sporočila elektronske pošte, čeprav je natančnost informacije odvisna od samega odjemalca.

Vrednost predstavlja vrednost iz atributa »subject« sporočila po specifikaciji RFC 2822.

Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:eml:Priority«

Tip: String20

Lastnosti: Searchable, PickList, ReadOnlyAlways.

Omejitve: Veljavne vrednosti:

- Normal: običajna prioriteta dostave elektronskega sporočila (RFC 1327: »normal«).
- Low: nizka prioriteta dostave elektronskega sporočila (RFC 1327: »non-urgent«).
- High: visoka prioriteta dostave elektronskega sporočila (RFC 1327: »urgent«).

Uporaba: Dokument

Opis: Vrednost predstavlja prioriteto dostave in obdelave sporočila elektronske pošte. Vrednost posreduje odjemalec, navadno ga izlušči iz samega sporočila, čeprav je natančnost informacije odvisna od samega odjemalca. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:eml:Signed«

Tip: Bool

Lastnosti: Searchable, ReadOnlyAlways.

Omejitve: ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Dokument

Opis: Vrednost predstavlja podatek, ali je elektronsko sporočilo elektronsko podpisano. Vrednost posreduje odjemalec, navadno ga izlušči iz samega sporočila elektronske pošte, čeprav je natančnost informacije odvisna od samega odjemalca. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### **3.2.7 Atributi upravljanja s fizičnim gradivom**

V kolikor elektronski arhiv hrani digitalizirane vsebine/gradivo ali le njihove metapodatke, je nujno vzpostaviti učinkovit sistem povezave elektronskega dela gradiva s povezanim fizičnim gradivom. V ta namen sistem nudi t.i. attribute upravljanja s fizičnim gradivom (angl. Physical Records Management Attributes).

Vzdrževanje aktualnih vrednosti v teh atributih omogoča enostavno, natančno in sledljivo upravljanje s fizičnim gradivom. Za to vzdrževanje so odgovorni skrbniki fizičnega gradiva, ki morebitne izposoje ali prenose vestno beležijo v sistem.

Vsaka sprememba atributov fizičnega gradiva se vnese v revizijsko sled elektronske entitete, ki fizično gradivo opisuje. Zato je sledljivost v tem primeru zagotovljena.

Vsi atributi upravljanja s fizičnim gradivom so registrirani v naslovnem prostoru »prm«. Teh atributov ni mogoče spreminjati ali jim dodeljevati dodatne lastnosti. Povezani so na systemske predloge iz katerih izpeljemo predloge, zmožne arhiviranja zadev in/ali dokumentov. Razen vpliva na vnose v revizijsko sled, atributi upravljanja s fizičnim gradivom nimajo vpliva na poslovno logiko strežnika v smislu operacij nad entitetami. Služijo le kot nosilci informacij.

### Atribut »sys:prm:Identifier«

Tip: String100

Lastnosti: Searchable, IsNonEmpty, Inherited

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Zadeva, Dokument

Opis: Vrednost predstavlja unikatni identifikator fizičnega gradiva.

Enolično označuje pripadajoče fizično gradivo. Vrednost je spremenljiva v celotnem življenjskem ciklu entitete. Določa jo skrbnik fizičnega gradiva, ki mora imeti možnost spreminjanja metapodatkov entitete. Podatek je neobvezen. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:prm:Description«

Tip: String200

Lastnosti: Searchable, Inherited

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Zadeva, Dokument

Opis: Vrednost predstavlja opis fizičnega gradiva. V podatek kar se da natančno zapišemo opis gradiva, njegov format, fizične nosilce, obseg, ipd. Vrednost je spremenljiva v celotnem življenjskem ciklu entitete. Določa jo skrbnik fizičnega gradiva, ki mora imeti možnost spreminjanja metapodatkov entitete. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami. Služi le kot nosilec informacije.

### Atribut »sys:prm:Status«

Tip: String20

Lastnosti: Searchable, PickList, IsNonEmpty, Inherited

Omejitve: Veljavne vrednosti:

- CheckedIn: Fizično gradivo je v hrambi na domači lokaciji. Vrednost se določi, ko fizično gradivo hranimo na njegovi »domači lokaciji«, lokaciji trajne hrambe. Podatek spreminjamo v primeru izposoje ali posredovanja gradiva tretjim osebam.

- **CheckedOut:** Fizično gradivo je posredovano tretji osebi in NI v hrambi na domači lokaciji. Vrednost se določi, ko fizično gradivo posredujemo, oziroma posodimo tretji osebi in ni v hrambi na njegovi »domači lokaciji«, lokaciji trajne hrambe. Podatek spreminjamo v primeru izposoje ali posredovanja gradiva tretjim osebam. V tem primeru je smiselno osvežiti tudi metapodatek »sys:prm:CurrentLocation«, »sys:prm:Custodian« in »sys:prm:ReturnDue«.

**Uporaba:** Zadeva, Dokument

**Opis:** Vrednost predstavlja status fizičnega gradiva glede na njegovo trenutno lokacijo oziroma hrambo. Določa ali spreminja se v primeru izposoje, oziroma posredovanja fizičnega gradiva tretji osebi, ki ga hrani izven domače lokacije. Vrednost je spremenljiva v celotnem življenjskem ciklu entitete. Določa jo skrbnik fizičnega gradiva, ki mora imeti možnost spreminjanja metapodatkov entitete. Datum in čas zadnje spremembe se zabeleži v metapodatek »sys:prm:StatusChange«. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:prm:StatusChange«

**Tip:** DateTime

**Lastnosti:** Searchable, ReadOnlyAlways, IsNonEmpty, Inherited

**Omejitve:** Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

**Uporaba:** Zadeva, Dokument

**Opis:** Vrednost predstavlja datum in čas zadnje spremembe statusa fizičnega gradiva, ostale spremembe so vidne v revizijski sledi entitete. Vrednost se določi samodejno s strani strežnika ob spremembi vrednosti atributa »sys:prm:Status« in ni spremenljiva. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:prm:HomeLocation«

**Tip:** String100

**Lastnosti:** Searchable, Inherited

**Omejitve:** Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

**Uporaba:** Zadeva, Dokument

Opis: Vrednost predstavlja opis domače lokacije fizičnega gradiva.

V podatek kar se da natančno zapišemo »domačo lokacijo« gradiva, kjer je gradivo v trajni hrambi (naslov, soba, omara, fascikel, ...). Vrednost je spremenljiva v celotnem življenjskem ciklu entitete. Določa jo skrbnik fizičnega gradiva, ki mora imeti možnost spreminjanja metapodatkov entitete. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:prm:CurrentLocation«

Tip: String100

Lastnosti: Searchable, Inherited

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Zadeva, Dokument

Opis: Vrednost predstavlja opis trenutne lokacije fizičnega gradiva, če ta ni domača in če fizično gradivo izposojamo oziroma dajemo v hrambo tretji osebi.

V podatek kar se da natančno zapišemo zunanjo lokacijo gradiva, kjer je gradivo v trenutni hrambi (naslov, soba, omara, fascikel, ...).

V tem primeru smiselno spremenimo tudi vrednost atributa »sys:prm:Status« v »CheckedOut«.

Vrednost je spremenljiva v celotnem življenjskem ciklu entitete.

Določa jo skrbnik fizičnega gradiva, ki mora imeti možnost spreminjanja metapodatkov entitete. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:prm:Custodian«

Tip: String100

Lastnosti: Searchable, Inherited

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Zadeva, Dokument

Opis: Vrednost predstavlja identifikacijo trenutnega skrbnika fizičnega gradiva.

Če je ta domača (vrednost atributa »sys:prm:Status« je »CheckedIn«), je to navadno skrbnik fizičnega gradiva. Če je zunanja (vrednost atributa »sys:prm:Status« je »CheckedOut«) je to oseba, ki ji je bilo gradivo zaupano za omejen čas.

Vrednost je spremenljiva v celotnem življenjskem ciklu entitete.

Določa jo skrbnik fizičnega gradiva, ki mora imeti možnost spreminjanja metapodatkov entitete. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:prm:ReturnDue«

Tip: Date

Lastnosti: Searchable, Inherited

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Zadeva, Dokument

Opis: Vrednost predstavlja datum in čas do katerega je potrebno fizično gradivo vrniti v domačo hrambo. Za vračilo je odgovoren skrbnik gradiva, naveden v atributu »sys:prm:Custodian«. Vrednost je spremenljiva v celotnem življenjskem ciklu entitete.

Določa jo skrbnik fizičnega gradiva, ki mora imeti možnost spreminjanja metapodatkov entitete. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### **3.2.8 Atributi prenesenega gradiva**

Pri prenosu hranjenega gradiva iz drugih elektronskih arhivov je potrebno nekatere attribute prenesenega gradiva hraniti v t.i. sistemskih atributih, da zagotavljamo kontinuiteto življenjskega cikla hranjenega gradiva. Nekateri sistemski atributi tretjih sistemov se vnašajo v sistemske attribute strežnika IMiS®/ARChive Server.

Za določene to ni možno, oziroma zaradi standardov ni dovoljeno.

V ta namen so v strežniku vnaprej določeni atributi, ki hranijo tovrstne metapodatkovne vrednosti.

Pri postopku »Uvoza« ali »Prenosa« gradiva v IMiS®/ARChive Server, strežnik samodejno dodeljuje vrednosti tem atributom na podlagi informacij, ki jih prejema s strani odjemalca, ki izvaja operacijo.

Pravico operaciji »Uvoza« določa prisotnost vloge »Uvozlzvoz« (angl. ImportExport).

Pravico operaciji »Prenosa« določa prisotnost vloge »Pregledi« (angl. Reviews).

Atributi prenesenega gradiva nimajo vpliva na poslovno logiko strežnika v smislu operacij nad entitetami, služijo le kot nosilci informacij.

### Atribut »sys:trf:AuditLog«

Tip: StringMax

Lastnosti: ReadOnlyAfterCreate

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednost predstavlja revizijsko sled entitete iz prejšnjega sistema.

Kljub temu, da je informacija ključna za kontinuiteto in revizijo življenjskega cikla entitete, podatek ni obvezen. Ni namreč nujno, da jo tretji sistem pri izvozu doda v metapodatkovno shemo izvožene entitete.

V primeru izvoza iz ISUD se podatek izvozi v metapodatkovno shemo in ga lahko tretji ISUD ponovno uvozi v attribute prenesenih entitet. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:trf:SystemId«

Tip: String100

Lastnosti: ReadOnlyAfterCreate

Omejitve: ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednost predstavlja sistemski identifikator entitete iz prejšnjega sistema.

Kljub temu, da je informacija ključna za kontinuiteto in revizijo življenjskega cikla entitete, podatek ni obvezen. Ni namreč nujno, da jo tretji sistem pri izvozu doda v metapodatkovno shemo izvožene entitete. Podatek je možno uporabiti za sledljivost instance entitete iz prejšnjega ISUD z instanco entitete v tem ISUD.

V primeru izvoza iz ISUD se podatek izvozi v metapodatkovno shemo in ga lahko tretji ISUD ponovno uvozi v attribute prenesenih entitet. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:trf:ClassificationCode«

Tip: String100

Lastnosti: ReadOnlyAfterCreate, IsNonEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednost predstavlja klasifikacijsko oznako entitete iz prejšnjega sistema.

Kljub temu, da je informacija ključna za kontinuiteto in revizijo življenjskega cikla entitete, podatek ni obvezen. Ni nujno namreč, da jo tretji sistem pri izvozu doda v metapodatkovno shemo izvožene entitete. Podatek je možno uporabiti za sledljivost instance entitete iz prejšnjega ISUD z instanco entitete v tem ISUD.

V primeru izvoza iz ISUD se podatek izvozi v metapodatkovno shemo in ga lahko tretji ISUD ponovno uvozi v attribute prenesenih entitet. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:trf:Imported«

Tip: DateTime

Lastnosti: ReadOnlyAfterCreate, Searchable, IsNonEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednost predstavlja datum in čas uvoza v primeru, da gre za »Uvoz«.

Ker se v sistemskem atributu »sys:Created« zabeleži dejanski čas nastanka entitete (prenos iz prejšnjega ISUD) je nujno, da novi ISUD v primeru »Uvoza« ali »Prenosa« zabeleži tudi datum in čas ustvarjanja instance entitete v novem ISUD.

Vrednost določi ISUD samodejno in ni posredovana s strani odjemalca.

V primeru izvoza iz ISUD se podatek izvozi v metapodatkovno shemo in ga lahko tretji ISUD ponovno uvozi v attribute prenesenih entitet. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:trf:Evidence«

Tip: StringMax

Lastnosti: ReadOnlyAfterCreate

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednost predstavlja dokazni zapis avtentičnosti entitete iz prejšnjega ISUD v primeru, da gre za »Uvoz«.

V primeru izvoza iz ISUD se podatek izvozi v metapodatkovno shemo in ga lahko tretji ISUD ponovno uvozi v attribute prenesenih entitet. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.



### Atribut »sys:trf:MoveReason«

Tip: String200

Lastnosti: Searchable, ReadOnlyAfterCreate, Multivalued

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednosti predstavljajo razloge za vsakokratni premik (re-klasifikacijo) entitete v prejšnjem ISUD (v primeru, da gre za »Uvoz«). Isto ležne vrednosti lahko uporabnik povezuje z atributoma »sys:trf:MoveAgent«, »sys:trf:MoveDateTime« in »sys:trf:MoveClassificationCode« za popolnejšo informacijo o premiku entitete v hierarhiji razvrščanja gradiva prejšnjega ISUD. V primeru izvoza iz ISUD se podatek izvozi v metapodatkovno shemo in ga lahko tretji ISUD ponovno uvozi v attribute prenesenih entitet. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:trf:MoveAgent«

Tip: String200

Lastnosti: Searchable, ReadOnlyAfterCreate, Multivalued

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

Opis: Vrednosti predstavljajo vsakokratne entitete imenika (uporabnike), ki so izvajali premike (reklasifikacijo) entitete v prejšnjem ISUD (v primeru, da gre za »Uvoz«). Isto ležne vrednosti lahko uporabnik povezuje z atributoma »sys:trf:MoveReason«, »sys:trf:MoveDateTime« in »sys:trf:MoveClassificationCode« za popolnejšo informacijo o premiku entitete v hierarhiji razvrščanja gradiva prejšnjega ISUD. V primeru izvoza iz ISUD se podatek izvozi v metapodatkovno shemo in ga lahko tretji ISUD ponovno uvozi v attribute prenesenih entitet. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:trf:MoveDateTime«

Tip: DateTime

Lastnosti: Searchable, ReadOnlyAfterCreate, Multivalued

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Razred, Zadeva, Dokument

**Opis:** Vrednosti predstavljajo vsakokratni datum in čas, ko se je izvedel premik (reklasifikacija) entitete v prejšnjem ISUD (v primeru, da gre za »Uvoz«). Isto ležne vrednosti lahko uporabnik povezuje z atributoma »sys:trf:MoveAgent«, »sys:trf:MoveReason« in »sys:trf:MoveClassificationCode« za popolnejšo informacijo o premiku entitete v hierarhiji razvrščanja gradiva prejšnjega ISUD. V primeru izvoza iz ISUD se podatek izvozi v metapodatkovno shemo in ga lahko tretji ISUD ponovno uvozi v attribute prenesenih entitet. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

#### Atribut »sys:trf:MoveClassificationCode«

**Tip:** String200

**Lastnosti:** Searchable, ReadOnlyAfterCreate, Multivalue

**Omejitve:** Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

**Uporaba:** Razred, Zadeva, Dokument

**Opis:** Vrednosti predstavljajo vsakokratno klasifikacijsko oznako entitete ob premiku (reklasifikaciji) entitete v prejšnjem ISUD (v primeru, da gre za »Uvoz«). Isto ležne vrednosti lahko povežemo z atributoma »sys:trf:MoveAgent«, »sys:trf:MoveReason« in »sys:trf:MoveDateTime« za popolnejšo informacijo o premiku entitete v hierarhiji razvrščanja gradiva prejšnjega ISUD. V primeru izvoza iz ISUD se podatek izvozi v metapodatkovno shemo in ga lahko tretji ISUD ponovno uvozi v attribute prenesenih entitet. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### **3.2.9 Atributi politik hrambe in zadržanj**

Za politike hrambe (angl. Retention policies) so na strežniku IMiS®/ARChive Server vnaprej določeni atributi in predloge, ki so namenjeni shranjevanju metapodatkov politik hrambe.

Atribute lahko razdelimo v naslednji skupini:

- Atributi, ki vplivajo na delovanje politik hrambe.
- Atributi, ki ne vplivajo na delovanje in so samo nosilci informacije o politikah hrambe.

V nadaljevanju so podrobneje opisani posamezni atributi in njihov pomen:

### Atribut »sys:ret:pol:Action«

Tip: Uint32

Lastnosti: Public, Required, Searchable, Picklist, IsNonEmpty, ReadOnlyAlways (v primeru Kopije politik hrambe)

Omejitve: Veljavne vrednosti:

- 1, alias »Dispose«: privzeta akcija politike hrambe je uničenje entitet.
- 2, alias »Permanent«: privzeta akcija politike hrambe je trajna hramba entitet.
- 3, alias »Transfer«: privzeta akcija politike hrambe je prenos entitet v tretji arhivski sistem, ter po potrditvi o uspešnem prenosu njihovo uničenje.
- 4, alias »Review«: privzeta akcija politike hrambe je, da se entiteto pusti za naslednji postopek odbiranja in izločanja.

Uporaba: Politike hrambe, Kopija politike hrambe

Opis: Obvezen atribut, ki predstavlja privzeto akcijo politike hrambe, ki se uporablja v postopku odbiranja in izločanja. Operacije, ki se za posamezno akcijo zgodijo so naslednje:

- Akcija »Dispose«: če ima uporabnik v imenu katerega se izvaja akcija pravico brisanja na entiteti, se entiteta nepreklicno izbriše, izbrišejo se vsi njeni metapodatki razen tistih, ki jih vsebuje izbrisana entiteta. Operacija je nepovratna kar pomeni, da se take entitete in njenih metapodatkov ne da več povrniti.
- Akcija »Permanent«: če ima uporabnik v imenu katerega se izvaja akcija pravico branja in pisanja na entiteti, se entiteta označi kot trajna. Take entitete ni mogoče več urejati, prav tako je onemogočeno ustvarjanje vsebovanih entitet.
- Akcija »Transfer«: če ima uporabnik, v imenu katerega se izvaja akcija pravico brisanja na entiteti in je v postopku odbiranja in izločanja potrdil uspešen prenos entitete, se entiteta nepovratno uniči. V atribut »sys:ret:pol:Reference« na izbrisani entiteti se zapiše referenca na preneseno entiteto, v kolikor je referenca vpisana v postopku odbiranja in izločanja.
- Akcija »Review«: entiteto se pusti za naslednji postopek odbiranja in izločanja.

Vse našteve akcije se zabeležijo v revizijsko sled entitete z razlogom, ki je naveden v postopku odbiranja in izločanja in komentarjem (v kolikor je prisoten).

### Atribut »sys:ret:pol:DetailedDescription«

Tip: StringMax

Lastnosti: Public, ReadOnlyAlways (v primeru Kopije politik hrambe)

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Politike hrambe, Kopija politik hrambe

Opis: Neobvezen podroben opis rokov hrambe entitete, ki je spremenljiv v celotnem življenjskem ciklu entitete. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:ret:pol:Reason«

Tip: String200

Lastnosti: Public, Required, IsNotEmpty, ReadOnlyAlways (v primeru Kopije politik hrambe)

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Politike hrambe, Kopija politik hrambe

Opis: Obvezen atribut, njegova vrednost se uporabi kot privzet komentar za akcijo v postopku odbiranja in izločanja. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:ret:pol:Reference«

Tip: String200

Lastnosti: Public, ReadOnlyAlways, Searchable

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Kopija politike hrambe

Opis: Obvezen atribut, ki ga v postopku priprave odbiranja in izločanja določi strežnik in je nespremenljiv. Vsebuje referenco na politike hrambe, ki je vključena v pripravo odbiranja in izločanja. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:ret:pol:Trigger«

Tip: String200

Lastnosti: Public, ReadOnlyAlways (v primeru Kopije politik hrambe)

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Politike hrambe, Kopija politik hrambe

Opis: Atribut mora vsebovati veljaven pogoj za iskanje po metapodatkih. Če pogoj v tem atributu ni prisoten, mora biti prisoten v »sys:ret:pol:TriggerEx« (glej poglavje [Pravila iskalnega niza](#)). V nasprotnem primeru se priprava postopka odbiranja in izločanja, ki vsebuje politiko hrambe z neveljavnim pogojem prekine z napako.

### Atribut »sys:ret:pol:TriggerEx«

Tip: StringMax

Lastnosti: Public, ReadOnlyAlways (v primeru Kopije politik hrambe)

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Politike hrambe, Kopija politik hrambe

Opis: Atribut mora vsebovati veljaven pogoj za iskanje po metapodatkih. Če pogoj v tem atributu ni prisoten, mora biti prisoten v »sys:ret:pol:Trigger« (glej poglavje [Pravila iskalnega niza](#)). V nasprotnem primeru se priprava postopka odbiranja in izločanja, ki vsebuje politiko hrambe z neveljavnim pogojem prekine z napako.

### Atribut »sys:ret:hold:Reason«

Tip: String200

Lastnosti: Public, Required, ReadOnlyAfterCreate

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Zadržanje postopkov odbiranja in izločanja

Opis: Obvezen atribut, ki vsebuje razlog, zakaj je prišlo do zadržanja postopkov odbiranja in izločanja. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### 3.2.10 Atributi postopkov odbiranja in izločanja

Za politike hrambe (angl. Retention policies) so na strežniku IMiS®/ARChive Server vnaprej določeni atributi in predloge, ki so namenjeni shranjevanju metapodatkov o samem postopku odbiranja in izločanja. Kot pri politikah hrambe in zadržanju odbiranja (glej poglavje [Roki hrambe](#)) lahko attribute razdelimo na tiste, ki vplivajo na samo izvajanje postopkov odbiranja in izločanja in na tiste, ki so samo nosilci informacij.

V nadaljevanju so podrobneje opisani posamezni atributi in njihov pomen:

#### Atribut »sys:ret:rev:Action«

Tip: UInt32

Lastnosti: Searchable, Picklist, IsNotEmpty

Omejitve: Veljavne vrednosti:

- 1, alias »Reviewing«: vrednost predstavlja akcijo pregleda v postopku odbiranja in izločanja in na strežniku nima vpliva.
- 2, alias »Complete«: vrednost predstavlja akcijo zaključka v postopku odbiranja in izločanja na strežniku.
- 3, alias »Discard«: vrednost predstavlja akcijo preklica v postopku odbiranja in izločanja na strežniku.

Uporaba: Postopek odbiranja in izločanja

Opis: Neobvezen atribut, ki pa je ključen za končanje ali zavrženje postopka odbiranja in izločanja na strežniku. Uporaba atributa je naslednja:

- Ob ustvarjanju postopka odbiranja in izločanja je atribut nima vrednosti.
- Ob pregledu postopka odbiranja in izločanja se lahko atribut postavi na »Reviewing«, kar pa ni nujno. S tem je postopek odbiranja in izločanja označen, da je v postopku pregledovanja.
- Po končanem pregledu se vrednost postavi na »Complete« ali »Discard«.

V vsakem primeru gre zahtevek v čakalno vrsto za izvršitev akcije.

V primeru vrednosti »Complete« se bo postopek odbiranja in izločanja izvršil, v primeru vrednosti »Discard« pa se postopek zavrže. V obeh primerih se status odbiranja in izločanja postavi na »Closed«. Kakršno koli spreminjanje postopka odbiranja in izločanja je onemogočeno.

### Atribut »sys:ret:rev:Comments«

Tip: StringMax

Lastnosti: /

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti.

Uporaba: Postopek odbiranja in izločanja

Opis: Neobvezen atribut, uporablja se ga za vpis različnih komentarjev, obrazložitev ter ostalih informacij, ki so kakor koli povezane s postopkom odbiranja in izločanja. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:ret:rev:Lists«

Tip: File

Lastnosti: Multivalued, ReadOnlyAfterCreate, AppendOnly, IncludeInAIP, Searchable

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti. Ena entiteta lahko vsebuje do 65536 vrednosti.

Uporaba: Postopek odbiranja in izločanja

Opis: Atribut predstavlja kontejner digitalnih vsebin. V primeru postopka odbiranja in izločanja so to XML dokumenti, ki predstavljajo rezultat postopka priprave odbiranja in izločanja. XML dokumente pripravi in zapiše strežnik in so za uporabnika nespremenljivi.

Atribut je vključen v skupino atributov, ki se indeksirajo. Posebnost tipa atributa »File« je, da to predstavlja indeks po polnem besedilu (Full Text Index). V kolikor je vključen sistem za zagotavljanje avtentičnosti in nespremenljivosti v času hrambe gradiva, postanejo prstni odtisi vrednosti iz tega kontejnerja del arhivskega informacijskega paketa (AIP).

### Atribut »sys:ret:rev:Members«

Tip: String200

Lastnosti: Multivalued, Required, Searchable, IsNonEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti

Uporaba: Postopek odbiranja in izločanja

Opis: Atribut je obvezen in predstavlja člane komisije, ki so prisotni v postopku odbiranja in izločanja. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:ret:rev:Message«

Tip: String200

Lastnosti: Public, ReadOnly

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti

Uporaba: Postopek odbiranja in izločanja

Opis: Atribut ni obvezen in je namenjen strežniku, da zapiše kratek opis napake v primeru, da je pri izdelavi ali izvajanju postopka odbiranja in izločanja prišlo do napake.

V primeru, da je izvajanje postopka odbiranja in izločanja uspešno, se to zabeleži v vrednost atributa. Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

### Atribut »sys:ret:rev:Query«

Tip: String200

Lastnosti: ReadOnlyAfterCreate, Searchable

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti

Uporaba: Postopek odbiranja in izločanja

Opis: Vrednost atributa ni obvezna, mora pa biti prisotna pri izdelavi postopka odbiranja in izločanja, če vrednost atributa »sys:ret:rev:Schedules« ali »sys:ret:rev:Query« ni prisotna.

Prav tako ni dovoljeno, da imata oba atributa »sys:ret:rev:Query« in »sys:ret:rev:Schedules« nastavljene vrednosti. Vrednost mora vsebovati veljaven pogoj za iskanje po metapodatkih. Za več informacij glej poglavje [Pravila iskalnega niza](#). V nasprotnem primeru se priprava postopka odbiranja in izločanja, ki vsebuje politike hrambe z neveljavnim pogojem prekine z napako.

### Atribut »sys:ret:rev:QueryEx«

Tip: StringMax

Lastnosti: ReadOnlyAfterCreate

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti

Uporaba: Postopek odbiranja in izločanja

Opis: Vrednost atributa ni obvezna, mora pa biti prisotna pri izdelavi postopka odbiranja in izločanja, če vrednost atributa »sys:ret:rev:Schedules« ali »sys:ret:rev:Query« ni prisotna.

Prav tako ni dovoljeno, da imata oba atributa »sys:ret:rev:Query« in »sys:ret:rev:Schedules« nastavljene vrednosti. Vrednost mora vsebovati veljaven pogoj za iskanje po metapodatkih. Za več informacij glej poglavje [Pravila iskalnega niza](#). V nasprotnem primeru se priprava postopka odbiranja in izločanja, ki vsebuje politike hrambe z neveljavnim pogojem prekine z napako.



### Atribut »sys:ret:rev:Schedules«

Tip: String200

Lastnosti: Multivalued, ReadOnlyAfterCreate, Searchable, IsNotEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti

Uporaba: Postopek odbiranja in izločanja

Opis: Vrednost atribut ni obvezna, mora pa biti prisotna pri izdelavi postopka odbiranja in izločanja, če vrednost atributa »sys:ret:rev:Query« ni prisotna. Prav tako ni dovoljeno, da imata oba atributa »sys:ret:rev:Query« in »sys:ret:rev:Schedules« nastavljene vrednosti. Vrednost mora vsebovati veljaven pogoj za iskanje po metapodatkih. Za več informacij glej poglavje [Pravila iskalnega niza](#). V nasprotnem primeru se postopek priprave odbiranja in izločanja, ki vsebuje politike hrambe z neveljavnim pogojem prekine z napako.

### Atribut »sys:ret:rev:Scope«

Tip: String200

Lastnosti: ReadOnlyAfterCreate, Searchable, IsNotEmpty

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti

Uporaba: Postopek odbiranja in izločanja

Opis: Vrednost atributa ni obvezna, predstavlja pa klasifikacijsko oznako entitete, pod katero se bo izvedel postopek priprave odbiranja in izločanja. Če vrednost ni prisotna, potem se priprava izvede na celotnem arhivu.

### Atribut »sys:ret:rev:State«

Tip: Uint32

Lastnosti: Public, Required, ReadOnlyAlways, Searchable, Picklist, IsNotEmpty

Omejitve: Veljavne vrednosti:

- 0, alias »Unknown«: vrednost atributa predstavlja neveljavno stanje postopka odbiranja in izločanja;
- 1, alias »Created«: vrednost atributa nastavi strežnik, ko uporabnik ustvari nov postopek odbiranja in izločanja;
- 2, alias »Preparing«: vrednost atributa nastavi strežnik v postopku izdelave vsebine za postopek odbiranja in izločanja;

- 3, alias »InReview«: vrednost atributa nastavi strežnik ob uspešni izdelavi vsebine za postopek odbiranja in izločanja;
- 4, alias »Completing«: vrednost atributa nastavi strežnik ob začetku izvajanja postopka odbiranja in izločanja;
- 5, alias »Completed«: vrednost atributa nastavi strežnik ob uspešno izvedenem postopku odbiranja in izločanja;
- 6, alias »Discarded«: vrednost atributa nastavi strežnik ob uspešnem zavrženju postopka odbiranja in izločanja;
- 7, alias »Failed«: vrednost atributa nastavi strežnik v primeru, da je pri izvedbi ali zavrženju prišlo do nepopravljive napake.

Uporaba: Postopek odbiranja in izločanja

Opis: Vrednost atributa predstavlja stanje postopka odbiranja in izločanja. Vrednost »Preparing« pomeni, da strežnik trenutno izdeluje vsebino za postopek odbiranja in izločanja. Vrednost »Completing« pomeni, da strežnik izvaja postopek odbiranja in izločanja.

Vrednost »InReview« pomeni, da je strežnik uspešno izdelal vsebino za postopek odbiranja in izločanja ter da jo uporabnik lahko pregleda, nastavi zelene akcije ipd.

Spreminjanje postopka odbiranja in izločanja (npr. spremembe akcij, vnos komentarjev ali razlogov, ipd.) je dovoljeno samo, če je vrednost atributa postavljena na »Created« ali na »InReview«, v vseh ostalih primerih spreminjanje postopka odbiranja in izločanja ni dovoljeno. V primeru vrednosti »Failed« se v atribut »sys:ret:rev:Message« zapiše sporočilo, zakaj izvedba ali izdelava postopka odbiranja in izločanja ni bila uspešna.

### 3.2.11 Atributi verzioniranega gradiva

Za potrebe verzioniranja so na strežniku IMiS®/ARChive Server vnaprej določeni atributi, ki so namenjeni shranjevanju metapodatkov o samem postopku verzioniranja.

V nadaljevanju so podrobneje opisani posamezni atributi in njihov pomen:

#### Atribut »sys:ver:SeriesId«

Tip: EntityReference

Lastnosti: Public, ReadOnlyAlways, Searchable

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti

Uporaba: Verzioniranje gradiva (dokumenti)

Opis: Vrednost atributa je identifikator entitete, iz katere je bil izdelan osnutek, in se zapiše ob izdelavi le-tega.

### Atribut »sys:ver:Label«

Tip: String20

Lastnosti: Public, ReadOnlyAlways, Versionable, Searchable

Omejitve: Oznaka je sestavljena iz največ 10 nivojev (primer: »1.0.0.0.0.0.0.0.1«), od katerih ima lahko posamezen nivo največjo vrednost »9999« (primer: »1.0.9999«).

Uporaba: Verzioniranje gradiva (dokumenti)

Opis: Vrednost atributa predstavlja oznako različice v seriji. Vrednost se samodejno ustvari ob vložitvi osnutka in predstavlja naslednjo različico v seriji.

### Atribut »sys:ver:Comment«

Tip: String200

Lastnosti: Public, ReadOnlyAlways, Versionable

Omejitve: Ni omejitev razen tistih, ki izhajajo iz tipa in lastnosti

Uporaba: Verzioniranje gradiva (dokumenti)

Opis: Vrednost atributa predstavlja komentar uporabnika, ki se zapiše ob vložitvi osnutka.

Atribut nima vpliva na poslovno logiko strežnika pri operacijah z entitetami, služi le kot nosilec informacije.

## 3.3 Entiteta

Entiteta je samostojni kontejner (angl. Container) podatkov in vsebin, ki zaokrožujejo logične celote informacije. Enolično jo identificiramo preko naslednjih treh različnih identifikatorjev:

- Notranji ali sistemski (obvezen, samodejno določen ob ustvarjanju).
- Klasifikacijska oznaka (obvezna, samodejno ali ročno določena ob ustvarjanju).
- Zunanji (1 ali več, neobvezen, zunanje določen in spremenljiv skozi celoten časovni cikel).

Vsako entiteto določajo:

- vrsta (tip)
- klasifikacijska oznaka
- sistemski atributi (naziv, opis, podatki življenjskega cikla, status, avtor, ...)
- lastnosti specifične za entiteto.

Entiteta je abstrakten konstrukt, ki hrani podatke in vsebine objekta, ki ga hrani (npr. zadeva, fizičen dokument, skupina dokumentov, ...).

Različne vrste entitet so specializirane glede na vrste objektov, ki jih opisujejo ali hranijo in zaradi tega poleg sistemskih lastnosti, dobijo še objektu prilagojene lastnosti.

Obenem je entiteta tudi nosilec dostopnih pravic, ki uporabnikom določajo dovoljena in nedovoljena dejanja nad objekti, ki jih hranijo.

Vsaka entiteta ima svoj življenjski cikel, ki se beleži v njeni revizijski sledi.

### 3.3.1 Vrste

V strežniku IMiS®/ARChive Server so določene naslednje vrste entitet:

- razred
- zadeva in vsebovana zadeva
- dokument.

#### Razred

Razredi so namenjeni razvrščanju gradiva glede na njegovo vsebino, oziroma poslovne dejavnosti organizacije. So osnovni gradniki načrta razvrščanja gradiva.

Razredi lahko združujejo zadeve ali dokumente po:

- Tipu vsebovanih dokumentov (npr. vsi računi se nahajajo v enem razredu, vse naročilnice pa v drugem).
- Lastniku vsebovanih dokumentov (npr. kadrovski oddelek ima svoje dokumente v enem razredu, prodajnega oddelka pa v drugem).

Število razredov in njihova vsebina ni predpisana s strani strežnika IMiS®/ARChive Server.

Upravitelj načrta razvrščanja gradiva jih lahko poljubno konfigurira glede na potrebe organizacije, ki arhivski strežnik uporablja.

#### Zadeva

Zadeva predstavlja skupino entitet (vsebovane zadeve, dokumenti), ki vsebinsko zaokrožujejo celoto. Predstavljajo dosje obravnavane zadeve (vsebinsko vprašanje, tema, naloga, projekt, ...) z vsemi pripadajočimi lastnostmi in vsebinami.

Je osnovna enota združevanja, evidentiranja, razvrščanja in arhiviranja dokumentov.

## Dokument

Dokument predstavlja kontejner lastnosti in vsebine, ki jo hrani. En dokument lahko hrani več digitalnih vsebin (npr. besedilo, slika, video). Navadno je vsebovan v zadevah in podrejenih zadevah, lahko pa nastopa tudi samostojno v razredu. Predstavlja osnovno enoto arhivskega gradiva, ki hrani vsebine.

### **3.3.2 Hierarhija**

Vsak elektronski arhiv je organiziran drevesno, ki se začneja z več debli (razredi na prvem nivoju) in vejami, ki jih predstavljajo posamezne entitete.

Končni razredi vsebujejo entitete vsebine (zadeva, vsebovana zadeva, dokument).

Strežnik IMiS®/ARChive Server ne omejuje globine hierarhije načrta razvrščanja gradiva.

Privzeto ima strežnik naslednje omejitve pri razvrščanja gradiva, določene v specifikacijah Moreq2 13.2. in 13.3:

- Na prvem nivoju načrta razvrščanja gradiva moramo obvezno določiti enega ali več razredov. Onemogočeno je dodajanje zadev ali dokumentov v koren drevesa.
- Vsaka entiteta, ki je zmožna vsebovanja lahko vsebuje podrejene entitete ene vrste.
- Razred lahko vsebuje podrazrede.
- Končni razred lahko vsebuje zadeve ali dokumente.
- Zadeva lahko vsebuje podrejene zadeve.
- Končne zadeve lahko vsebujejo samo dokumente.
- Dokument ni zmožen vsebovanja podrejenih entitet.

Strežnik lahko nastavimo tudi tako, da dovoljuje mešanje različnih entitet na istem nivoju.

Omejitve so naslednje:

- Na prvem nivoju načrta razvrščanja gradiva moramo obvezno določiti enega ali več razredov. Onemogočeno je dodajanje zadev ali dokumentov v koren drevesa.
- Vsaka entiteta, ki je zmožna vsebovanja lahko vsebuje podrejene entitete različnih vrst (razred ali zadeva lahko vsebuje razrede, zadeve in dokumente).
- Dokument ni zmožen vsebovanja podrejenih entitet.

Hierarhija entitet v načrtu razvrščanja gradiva obenem lahko določa tudi dostopne pravice vseh vsebovanih podrejenih entitet (glej poglavje [Dostopi](#)), razen kadar so dostopne pravice natančneje določene v samih podrejenih entitetah. Za več informacij glej poglavje [Eksplisitna dovoljenja ali prepovedi](#). Istočasno hierarhija določa še stopnjo tajnosti (če ni eksplicitno določena glej poglavje [Stopnje tajnosti](#)) ter obveznost statusa entitete (sistemski atribut »sys:Status«).

Status je določen na:

- razredih
- zadevah in vsebovanih zadevah
- dokumentih uvrščenih neposredno pod razredi.

Če vrednost statusa ni eksplicitno nastavljena, potem se podeduje od nadrejene entitete. To velja tudi za razrede na prvem nivoju, ki dobijo podedovano vrednost »Opened« v primeru, da nimajo eksplicitno nastavljene vrednosti.

### 3.3.3 Komponente

Entitete sestavljajo različne komponente, med njimi:

- shema sistemskih atributov;
- shema specializiranih atributov, specifičnih za vrsto entitete;
- shema atributov upravljanja fizičnega gradiva;
- shema atributov prenesenega gradiva;
- skladišče arhiviranih vsebin s pripadajočimi metapodatki o vsebinah;
- komponente dostopnih pravic;
- komponente elementov avtentičnosti;
- reference;
- roki hrambe.

Strukturo večini komponent določa predloga, ki je osnova za nastanek entitete (shema specializiranih atributov). Druge komponente so sistemske narave in so vedno prisotne, saj so ključne za obstoj in življenjski cikel entitet (shema sistemskih atributov, itd). Entiteta je tudi nosilec njenih dostopnih pravic, revizijske sledi in elementov dokaza avtentičnosti.

### 3.3.4 Predloge

Predloge predpisujejo metapodatkovno shemo - zahtevane in dovoljene attribute.

Hkrati so osnova za izdelavo specializiranih predlog entitet istega tipa, ki podedujejo atributno shemo.

Vsaka predloga vsebuje vgrajene in vnaprej določene systemske attribute.

Ti so potrebni za pravilno delovanje strežnika IMiS®/ARChive Server in jih ni mogoče spreminjati. Njihovi nazivi prihajajo iz naslovnega področja »int:«, »sys:«, »trf:«, ...

Vse ostale attribute lahko administrator poljubno dodaja in briše iz predloge, dokler ni ustvarjena prva entiteta. Potem so možnosti spremembe predloge omejene, omejitve so navedene v nadaljevanju.

Pri dodajanju atributa na predlogo lahko uporabnik z ustreznimi pravicami določi ali:

- je vrednost atributa v okviru neke entitete javnega značaja (angl. Public);
- ima lahko atribut več kot eno vrednost (angl. Multivalue);
- je atribut obvezen oziroma neobvezen (angl. Required);
- se vrednosti atributa po prvi shranitvi lahko spreminjajo (angl. ReadOnly);
- se vrednost atributa deduje iz nadrejene entitete (angl. Inherited). V kolikor v entiteti niso določene eksplicitne vrednosti, se te dedujejo iz prve nadrejene entitete, ki ima določene eksplicitne vrednosti;
- lahko uporabnik spreminja že zapisan atribut oz. dovoli samo dodajanje vsebine atributa brez brisanja že obstoječih vrednosti (angl. Append Only);
- se vrednost atributa v postopku zagotavljanja avtentičnosti hranjenega gradiva vključi v arhivski informacijski paket (angl. IncludeInAIP);
- vrednost atributa ne sme biti prazna (angl. IsNotEmpty);
- atribut je verzionabilen (angl. Versionable);
- mora biti vrednost atributa elektronsko podpisana in veljavna (angl. SignatureDisposition);

Brisanje predloge je dovoljeno samo v primeru, ko ne obstaja entiteta, ki bi po brisanju postala neveljavna.

Ostalim vrstam entitet (razred, zadeva, dokument) je potrebno dodeliti predlogo in morajo biti zgrajeni po pravilih, ki jih določa metapodatkovna shema predloge. Predloge lahko administrator ustvari na novo ali jih izvede iz kakšne druge predloge pod pogojem, da sta vrsti entitete isti.

*Primer:* Iz predloge »Račun« izpeljemo predlogi »Vhodni račun« in »Izhodni račun«. Vsaki predlogi posebej tako ni potrebno dodeljevati skupnih atributov.

Prav tako se vse bodoče spremembe predloge »Račun« samodejno upoštevajo v izpeljanih predlogah »Vhodni račun« in »Izhodni račun«.

### 3.3.5 Dostopi

Dostop do entitet in njihovo upravljanje je ključnega pomena, saj zagotavlja osnovna načela informacijske varnosti:

- Celovitost (angl. Integrity): zagotavlja nespremenjenosti informacij.
- Zaupnost (angl. Confidentiality): zagotavlja, da so informacije dostopne samo pooblaščenim osebam.
- Razpoložljivost (angl. Availability): zagotavlja razpoložljivosti informacij pooblaščenim osebam.

Preverjanje pravic dostopa poteka v dveh korakih:

- Preverjanje stopnje tajnosti (angl. Security Class).
- Preverjanje dostopa do entitet (angl. Access Control Lists - ACL).

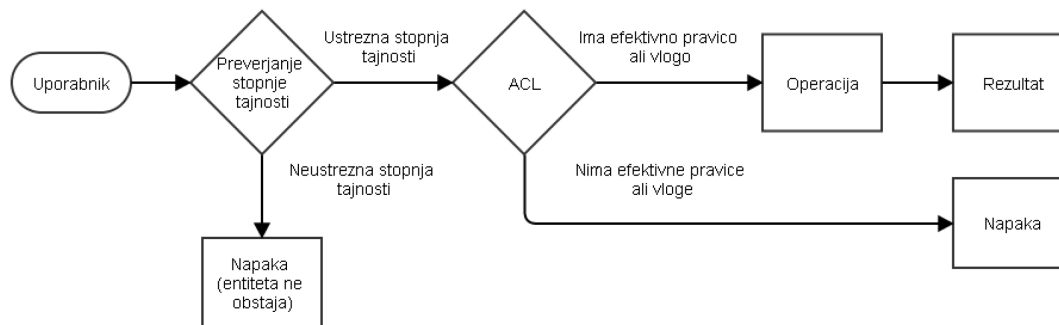
Stopnja tajnosti je predpogoj, da lahko uporabnik vidi obstoj entitet in izvaja dejanja nad entitetami. Administrator za vsakega uporabnika ali skupino določi do katerega nivoja tajnosti je avtoriziran.

Uporabnik mora imeti enako ali višjo stopnjo tajnosti, kot jo imajo entitete, ki so bodisi eksplicitno določene ali podedovane od nadrejene entitete. Če stopnja tajnosti uporabniku omogoča videti obstoj entitet, se nadalje preverja dostop do entitet.

Za preverjanje dostopov do entitet, uporablja strežnik IMiS®/ARChive Server koncept liste dostopnih pravic (angl. Access Control Lists - ACL). Za vsako operacijo na strežniku, ki jo izvaja uporabnik s pravicami preveri, ali jo ima pravico izvajati.

V primeru, da uporabnik nima pravice izvajati operacije, se operacija ne izvrši in strežnik vrne napako. Delovanje dostopa predstavlja naslednja slika.





Slika 3: Delovanje ACL

### 3.3.5.1 Stopnje tajnosti

Stopnja tajnosti je dodaten nivo varnosti dostopa do arhiviranega gradiva zaradi nevarnosti razkritja dokumentov nepooblaščenim osebam. Na nivoju vrste dokumentov administrator nastavi stopnjo tajnosti in za vsakega uporabnika (ali skupino) določi do katerega nivoja tajnosti je avtoriziran. V osnovnih nastavitvah so vse vrste dokumentov dostopne vsem uporabnikom (stopnja tajnosti je 0).

Podobno kot pri dostopnih pravicah, se tudi stopnja tajnosti deduje po hierarhiji navzdol. V primeru, da ima entiteta v hierarhiji eksplicitno nastavljeno stopnjo tajnosti, le-ta prevlada nad podedovano vrednostjo.

Pri nastavljanju stopnje tajnosti obstajajo naslednja pravila:

- Največja stopnja tajnosti, ki jo lahko uporabnik nastavi za entiteto je enaka izračunani efektivni stopnji tajnosti.
- Uporabnik lahko nastavi samo večjo ali enako stopnjo tajnosti na entiteti, kot jo ima nadrejena entiteta v hierarhiji. Če nadrejena entiteta nima nastavljene stopnje tajnosti, potem lahko nastavi poljubno vrednost stopnje tajnosti, ki je manjša ali enaka uporabnikovi efektivni stopnji tajnosti.
- Pri dvigovanju se stopnja tajnosti zviša vsem podrejenim entitetam, ki imajo stopnjo tajnosti nižjo ali enako kot entiteta, ki ji dvigujemo stopnjo tajnosti (velja tako za eksplicitno nastavljene stopnje tajnosti kot podedovane).
- Pri spuščanju, se stopnja tajnosti spusti vsem podrejenim entitetam, ki imajo podedovano stopnjo tajnosti.

Primer 1:

Za primer vzemimo hierarhijo, ki jo predstavlja slika v poglavju [Efektivne pravice](#).

Predpostavimo, da nobena od entitet nima eksplicitno nastavljene stopnje. Razredu nastavimo stopnjo tajnosti na »Restricted«. Zaradi dedovanja se vsem vsebovanim entitetam nastavi stopnja tajnosti na »Restricted«.

Primer 2:

Zadevi iz prejšnjega primera hočemo spustiti stopnjo tajnosti na »Unclassified«. Ker ima nadrejeni razred stopnjo tajnosti »Restricted«, spuščanje stopnje tajnosti ni mogoče.

Primer 3:

Zadevi nastavimo eksplicitno stopnjo tajnosti na »Restricted«, nakar nadrejenemu razredu odvzamemo stopnjo tajnosti. Zadeva in podrejeni dokumenti imajo nastavljeno stopnjo tajnosti na »Restricted«.

Primer 4:

Razredu dvignemo stopnjo tajnosti na »Confidential«. Zadevi in podrejenim dokumentom se stopnja tajnosti dvigne na »Confidential«, saj imajo podrejene entitete nižjo stopnjo tajnosti kot entiteta, kateri zvišujemo stopnjo tajnosti.

Primer 5:

Zadevi dvignemo stopnjo tajnosti na »Secret«. Posledično se tudi stopnja tajnosti dokumentov dvigne na »Secret«. Nato razredu spustimo stopnjo tajnosti na »Unclassified«. Stopnja tajnosti zadeve in podrejenih dokumentov se ohrani, saj ima zadeva eksplicitno nastavljeno višjo stopnjo tajnosti kot razred, kateremu spuščamo stopnjo tajnosti.

Kot že omenjeno, ima uporabnik možnost nastavljanja največje stopnje tajnosti glede na njegovo izračunano efektivno stopnjo tajnosti. Podobno kot računanje efektivnih pravic, se računa tudi efektivna stopnja tajnosti za posameznega uporabnika, saj je le-ta odvisna od skupin, ki jim uporabnik pripada.

Efektivna stopnja tajnosti se izračuna na naslednji način:

- Če ima uporabnik eksplicitno nastavljeno stopnjo tajnosti, potem ta vrednost prevlada.
- Če uporabnik nima eksplicitno nastavljenih stopnje tajnosti, potem se efektivna stopnja tajnosti računa na podlagi skupin, ki jim uporabnik pripada. Efektivna stopnja tajnosti je največja stopnja tajnosti vseh skupin, ki jim uporabnik pripada (ne glede na njihovo postavitev v hierarhiji entitet).

***Primer 1:***

Uporabnik ima eksplicitno nastavljeno stopnjo tajnosti na 1 (Unclassified). Hkrati pa je vsebovan v dveh skupinah, ki imata stopnjo tajnosti nastavljeno na 2 (Restricted) in 3 (Confidential). Efektivna stopnja tajnosti za tega uporabnika je tako 1, saj eksplicitno nastavljena stopnja tajnosti prevlada nad stopnjami tajnosti skupin.

Tak uporabnik lahko dostopa do entitet, ki so dostopne vsem uporabnikom (stopnja tajnosti 0) in entitet, ki imajo stopnjo tajnosti nastavljeno na 1 (Restricted).

***Primer 2:***

Vzemimo uporabnika iz prejšnjega primera in mu pobrišemo eksplicitno nastavljeno stopnjo tajnosti. Tako pridobi efektivno stopnjo tajnosti 3 (Confidential), saj prevlada največja stopnja tajnosti vseh skupin, ki jim pripada. Tako ima uporabnik dostop do entitet z največjo stopnjo tajnosti 3 ali manj.

**3.3.5.2 Lista dostopnih pravic (ACL)**

Uporabnik s pravico določanja dostopnih pravic na entiteti (angl. Change permissions) lahko dodeli listo dostopnih pravic uporabniku, uporabniški skupini ali pa atributu, ki mora biti tipa »DirectoryEntity«. Dostopne pravice razdelimo v dve skupini:

- Dostopne pravice za entitete.
- Specializirane dostopne pravice za attribute.

Vsaki skupini pravic lahko uporabnik s pravico določi eksplicitno dovoljenje (angl. Allow) ali prepoved (angl. Deny), Eksplicitna dovoljenja skupaj s podedovanimi pravicami določajo efektivne pravice (angl. Effective rights), oziroma pravice uporabnika do zahtevane operacije na strežniku.

Vsakemu eksplicitnemu dovoljenju ali prepovedi se lahko določi naslednje lastnosti:

- Dovoljenje ali prepoved velja za dotičnega uporabnika ali za pooblaščen osebo.  
Za več informacij glej poglavje [Komponente](#).
- Dovoljenje ali prepoved velja za entitete v poddrevesu.
- Dovoljenje ali prepoved velja za entiteto, na kateri je določena.
- Dovoljenje ali prepoved lahko časovno omejimo.  
Za več informacij glej poglavje [Eksplicitna dovoljenja ali prepovedi](#).

S kombinacijo teh lastnosti lahko natančno določimo listo dostopnih pravic za posamezne uporabnike in skupine uporabnikov ter s tem učinkovito omejimo dostop do entitet.

Primeri uporabe so podrobno opisani v poglavju [Efektivne pravice](#).

### 3.3.5.2.1 Dostopne pravice za entiteto

Za dostop do razredov, zadev in dokumentov se uporabljajo naslednje dostopne pravice:

- »Branje entitete« (angl. Read): pravica branja entitete.  
Uporabnik mora imeti to pravico, če hoče entiteto odpirati v načinu samo za branje (angl. Read-only mode).
- »Urejanje entitete« (angl. Write): pravica pisanja na entiteti.  
Za urejanje entitete mora imeti uporabnik poleg pravice pisanja tudi pravico branja (angl. Read-write mode).
- »Premik entitete« (angl. Move): pravica premika entitete v načrtu razvrščanja gradiva.  
Uporabniku je omogočeno premikanje entitete in njej podrejenih entitet v načrtu razvrščanja gradiva.
- »Brisanje entitete« (angl. Delete): pravica brisanja entitete.  
Uporabniku je omogočeno brisanje entitete in njenih komponent.
- »Ustvarjanje entitet« (angl. Create entities): pravica ustvarjanja novih vsebovanih entitet.  
Uporabnikom pravica omogoča ustvarjanje novih vsebovanih entitet.
- »Spreminjanje dovoljenj« (angl. Change permissions): pravica spreminjanja liste dostopnih pravic (ACL).  
Uporabniku je dovoljeno spreminjati dostopne pravice za entitete in metapodatke.  
Spreminjanje dostopnih pravic je mogoče samo, ko je entiteta odprta v načinu za urejanje.
- »Spreminjanje stopnje tajnosti« (angl. Change security class): pravica spreminjanja stopnje tajnosti. Uporabnikom, katerim je pravica dodeljena, lahko entiteti določajo inicialno stopnjo tajnosti, ko entiteta še ni shranjena, oziroma spreminjajo stopnjo tajnosti obstoječim entitetam. V kolikor uporabnik te pravice nima, entiteti ne more določati inicialne stopnje tajnosti (jo implicitno podeduje od nadrejene entitete) ali jo kasneje spreminjati.
- »Spreminjanje statusa« (angl. Change status): pravica spreminjanja statusa.  
Uporabnikom, katerim je pravica dodeljena, lahko spreminjajo status entitete.  
Privzeta vrednost je podedovana iz nadrejene entitete. Preostali eksplicitni vrednosti sta lahko »Odprto« (angl. Opened) ali »Zaprto« (angl. Closed).  
V primeru, da uporabnik zapre entiteto, hkrati zapre tudi vse podrejene entitete.  
V postopku odpiranja že zaprte entitete se status spremeni le neposredni entiteti, podrejene entitete ohranijo njihov status.

- »Spreminjanje hrambe« (angl. Change retention): pravica spremembe veljavnosti rokov hrambe entitete. Uporabniki, katerim je pravica dodeljena, lahko spreminjajo veljavnost rokov hrambe za entiteto. Privzete vrednosti so podedovane iz nadrejenih entitet.
- »Ustvarjanje referenc« (angl. Create reference): pravica ustvarjanja referenc med entitetami. Uporabnikom, katerim je pravica dodeljena je omogočeno ustvarjanje referenc, s katerimi lahko med seboj povežejo različne tipe entitet.

Naslednja tabela prikazuje operacije nad entitetami in zahtevane dostopne pravice za izvajanje le-teh.

Operacija	Pravica									
	Read	Write	Delete	Move	Change permissions	Create-entities	Change security class	Change status	Change retention	Create reference
Odpiranje entitete v načinu za branje	✓									
Urejanje entitete	✓	✓								
Brisanje entitete	✓		✓							
Urejanje ACL	✓	✓			✓					
Re-klasifikacija (izvorna entiteta)	✓			✓						
Re-klasifikacija (tarčna entiteta)						✓				
Ustvarjanje entitet (nadrejena entiteta)						✓				
Spreminjanje stopnje tajnosti	✓						✓			
Spreminjanje statusa	✓							✓		
Spreminjanje rokov hrambe									✓	
Ustvarjanje referenc	✓									✓

Ustvarjanje osnutka	✓					✓				
Vložitev osnutka	✓	✓								
Zavrženje osnutka			✓							

Tabela 4: Tabela operacij in pravic

Pri vložitvi osnutka se poleg dostopnih pravic preverja tudi ali je uporabnik, ki izvaja operacijo lastnik osnutka (je prisoten v atributu »sys:Owner«), oziroma ali ima uporabnik vlogo »DraftManagement«. Za več informacij glej poglavje [Vloge](#).

### 3.3.5.2.2 Dostopne pravice za metapodatke

Za dostop do metapodatkov entitete se uporabljajo naslednje dostopne pravice:

- »Branje« (angl. Read): pravica branja metapodatkov.
- »Urejanje« (angl. Write): pravica spreminjanja vrednosti metapodatkov.
- »Brisanje« (angl. Delete): pravica brisanja metapodatkov.
- »Ustvarjanje« (angl. Create): pravica dodeljevanja vrednosti metapodatkov na predhodno praznih metapodatkih.

Z dostopnimi pravicami za metapodatke strežnik dodatno omeji dostop in urejanje metapodatkov, ki niso javni. Tako lahko uporabniku s pravico branja na določeni entiteti prepreči branje posameznih metapodatkov z uporabo prepovedi »Read« pravice.

Če dostopne pravice za metapodatke niso določene, jih metapodatki prevzamejo iz dostopnih pravic pripadajoče entitete. Prepoved »Delete« pravice za brisanje metapodatkov ne zadrži brisanja entitete in njenih metapodatkov. Če ima uporabnik pravico brisanja entitete in hkrati nima pravice brisanja metapodatkov, potem ima pravica brisanja entitete prednost pred prepovedjo brisanja metapodatkov. Nastavljanje dostopnih pravic na attribute, ki so označeni kot »Searchable« ni dovoljeno, saj so taki atributi lahko del indeksiranja v zunanjih iskalnikih, ki nimajo povezave z dostopnimi pravicami na strežniku IMiS®/ARChive Server.

Za več informacij glej poglavje [Iskanje](#).

### 3.3.5.2.3 Izjeme

Pri izračunu efektivnih pravic (glej poglavje [Efektivne pravice](#)) obstaja nekaj izjem, ki jih lahko ločimo na:

- Izjeme pri izračunu efektivnih pravic iz pravic atributa.
- Izjeme pri izračunu efektivnih pravic na metapodatkih.
- Izjeme pri izračunu efektivnih pravic v primeru delegirane seje.

#### Izjeme pri izračunu efektivnih pravic iz pravic atributa:

Listo dostopnih pravic lahko nastavimo na posamezne attribute tipa »DirectoryEntity«.

Tako nastavljena lista pravic velja za vse uporabnike ali skupine, ki se v tem atributu nahajajo, z izjemo sistemskih uporabnikov in skupin. Izjeme so:

- Sistemska skupina »sys:Everyone«.  
Skupini pripadajo vsi registrirani uporabniki in se upošteva pri izračunu efektivnih pravic.
- Dedovanje pravic, ki so nastavljene na atributu.  
Vsa dovoljenja in vse prepovedi se seštevajo glede na hierarhijo. Seštevek pravic se uporabi pri računu efektivnih pravic na entiteti, na kateri se v dotičnem atributu nahaja uporabnik ali skupina, kateri uporabnik pripada. Seštevek pravic se upošteva kot seštevek podedovanih dovoljenj in prepovedi, ki učinkujejo na dedovane pravice, ki so posledica nastavitve dovoljenj in prepovedi za uporabnika ali skupino, v kateri se uporabnik nahaja.

#### Izjeme pri izračunu efektivnih pravic na metapodatkih:

Izjeme pri izračunu efektivnih pravic na metapodatkih so odvisne od nastavitve posamezne predloge. Glede na nastavitve predloge veljajo naslednje izjeme:

- Če je atribut na predlogi določen kot javni, ima vsak uporabnik pravico branja metapodatkov.
- Če je atribut na predlogi določen kot obvezen, ima vsak uporabnik pravico ustvarjanja metapodatkov, hkrati pa nima pravice brisanja.

- Glede na »read-only« nastavitve atributa veljajo naslednje omejitve:
  - Če je atribut določen kot »ReadOnlyDisabled«, zanj ne veljajo nobene izjeme.
  - Če je atribut določen kot »ReadOnlyAfterCreate« in ne gre za novo entiteto, uporabnik nima pravice pisanja in brisanja.
  - Če je atribut določen kot »ReadOnlyAfterCheckin« in entiteta ni delovna kopija, uporabnik nima pravice pisanja in brisanja.
  - Če je atribut določen kot »ReadOnlyAlways«, uporabnik nima pravice pisanja in brisanja.

Javne metapodatke lahko uporabnik bere tudi, če nima pravice branja na entiteti, ki jih vsebuje. To mora uporabniku omogočati globalna varnostna nastavitve na strežniku IMiS®/ARChive Server.

Naslednja tabela prikazuje omejitev pravic vpogleda v javne metapodatke uporabnikov, glede na kombinacijo »Read« pravice na entiteti in globalne varnostne nastavitve.

Omejitev vpogleda javnih metapodatkov	»Read« pravica na entiteti	Globalna varnostna nastavitve
Uporabniku se ne prikaže nobena informacija, tako ni mogoče ugotoviti obstoja entitete (tudi če ima uporabnik zadostno stopnjo tajnosti).		
Uporabniku se prikažejo javni metapodatki. Uporabnik lahko potrdi obstoj entitete, ne more pa videti metapodatkov, ki niso javni.		✓
Če ima uporabnik pravico branja na entiteti, potem ima ne glede na globalno varnostno nastavitve tudi pravico branja javnih metapodatkov.	✓	N/A

Tabela 5: Omejitev pravic vpogleda v javne metapodatke

Poleg prej naštetih izjem, se posebej obravnavajo še naslednji sistemski metapodatki: sys:ExternalIds, sys:Opened, sys:Closed, sys:Creator.

Tem metapodatkom je prepovedano nastavljanje kakršnih koli dovoljenj ali prepovedi.



### Izjeme pri izračunu efektivnih pravic v primeru delegirane seje

Pri izračunu efektivnih pravic uporabnikov, ki so se prijavili preko delegirane seje, se upoštevajo eksplicitna dovoljenja in prepovedi uporabnikov in njihovih delegatov, če so le-te prisotne. Ker so dovoljenja in prepovedi uporabnikov in delegatov enakovredne, se na posameznem nivoju njihove vrednosti seštevajo.

#### **3.3.5.2.4 Vloge**

Vloga je skupek pravic, ki uporabniku omogočajo izvajanje določene operacije na strežniku.

Vnaprej so določene naslednje vloge, ki omogočajo:

- AuditLogQuery: pridobivanje revizijske sledi.
- ImportExport: uvoz in izvoz gradiva.
- ContentManagement: izvajanje zahtev za indeksiranje in avtomatično pretvorbo vsebine.
- Reports:
  - prikaz in tiskanje sistemskih poročil o zadevah, dokumentih, vsebini dokumentov, hrambi, pregledih, dostopih, entitetah, razredih (in zadevah) načrta razvrščanja gradiva, brisanih entitetah in entitetah za izbris.
- ManageDraft: vloga omogoča vpogled in vložitev/zavrženje osnutka dokumenta drugih uporabnikov (v kombinaciji z dostopnimi pravicami za entiteto).
- AdminCodeListaRead: vloga omogoča pregled šifrantov.
- AdminCodeListUpdate: vloga omogoča dodajanje, brisanje ali spreminjanje šifranta.
- AdminCountersRead: vloga omogoča pregled določitev števcov.
- AdminCounterUpdate: vloga omogoča dodajanje, brisanje ali spreminjanje določitev števca.
- AdminDirectoryEntitiesRead: vloga omogoča pregled imeniških entitet.
- AdminDirectoryEntityUpdate: vloga omogoča dodajanje, brisanje ali spreminjanje imeniške entitete.
- AdminDirectoryGroupRead: vloga omogoča pregled članov imeniške skupine.
- AdminDirectoryGroupUpdate: vloga omogoča dodajanje ali brisanje članov imeniške skupine.
- AdminAttributesRead: vloga omogoča pregled atributov.
- AdminAttributeUpdate: vloga omogoča dodajanje, brisanje ali spreminjanje atributa.
- AdminTemplatesRead: vloga omogoča branje predlog entitet.

- AdminTemplateUpdate: vloga omogoča dodajanje, brisanje ali spreminjanje predlog entitete.
- AdminStorageProfilesRead: vloga omogoča branje strežniških profilov.
- AdminStorageProfileUpdate: vloga omogoča dodajanje, brisanje ali spreminjanje strežniškega profila.
- AdminStorageVolumesRead: vloga omogoča branje strežniških volumnov.
- AdminStorageVolumeUpdate: vloga omogoča dodajanje, brisanje ali spreminjanje strežniškega volumna.
- AdminACLRead: vloga omogoča branje dostopnih pravic.
- AdminACLUpdate: vloga omogoča dodajanje, brisanje ali spreminjanje dostopnih pravic.
- AdminLegacyArchiveRead: vloga omogoča branje strežniške konfiguracije za starejše odjemalce.
- AdminLegacyArchiveUpdate: vloga omogoča spreminjanje strežniške konfiguracije za starejše odjemalce.
- AdminArchiveSettingsRead: vloga omogoča branje splošnih nastavitev arhiva.
- AdminArchiveSettingsUpdate: vloga omogoča dodajanje, brisanje ali spreminjanje splošnih nastavitev arhiva.
- AdminAuditLogSettingsRead: vloga omogoča branje nastavitev revizijske sledi.
- AdminAuditLogSettingsUpdate: vloga omogoča dodajanje, brisanje ali spreminjanje nastavitev revizijske sledi.
- AdminRetentionRead: vloga omogoča branje politik hrambe.
- AdminRetentionUpdate: vloga omogoča dodajanje, brisanje ali spreminjanje politik hrambe.
- AdminContentSettingsRead: vloga omogoča branje strežniške konfiguracije za upravljanje z vsebino.
- AdminContentSettingsUpdate: vloga omogoča spreminjanje strežniške konfiguracije za upravljanje z vsebino.
- AdminLTANSSettingsRead: vloga omogoča branje strežniške konfiguracije za dolgoročno arhiviranje vsebin.
- AdminLTANSSettingsUpdate: vloga omogoča spreminjanje strežniške konfiguracije za dolgoročno arhiviranje vsebin.

- AdminAAASettingsRead: vloga omogoča branje strežniške konfiguracije za zunanjo avtentikacijo in sinhronizacijo uporabnikov.
- AdminAAASettingsUpdate: vloga omogoča spreminjanje strežniške konfiguracije za zunanjo avtentikacijo in sinhronizacijo uporabnikov.
- AdminSecuritySettingsRead: vloga omogoča branje shrambe digitalnih potrdil.
- AdminSecuritySettingsUpdate: vloga omogoča spreminjanje shrambe digitalnih potrdil.

### 3.3.5.2.5 Eksplicitna dovoljenja ali prepovedi

Z nastavljanjem eksplicitnih dovoljenj ali prepovedi upravljamo učinkovite pravice uporabnika.

Vsaka sprememba dovoljenj in prepovedi se zabeleži v revizijsko sled.

Časovne omejitve dovoljenj ali prepovedi lahko ločimo na:

- Dovoljenja ali prepovedi brez časovne omejitve.
- Dovoljenja ali prepovedi z začetkom časovne omejitve.
- Dovoljenja ali prepovedi s koncem časovne omejitve.
- Dovoljenja ali prepovedi z začetkom in koncem časovne omejitve.

#### Dovoljenja ali prepovedi brez časovne omejitve

Standardni način uporabe dovoljenj ali prepovedi. Takšna dovoljenja in prepovedi veljajo vedno, ne glede na to, kdaj se uporabljajo pri izračunu učinkovitenh pravic.

#### Dovoljenja ali prepovedi z začetkom časovne omejitve

Dovoljenja ali prepovedi imajo določen začetek veljavnosti, nimajo pa določenega konca. Takšna dovoljenja in prepovedi se upoštevajo pri izračunu učinkovitenh pravic v primeru, da je trenutni datum večji ali enak datumu začetka veljavnosti dovoljenja ali prepovedi.

#### Dovoljenja ali prepovedi s koncem časovne omejitve

Dovoljenja ali prepovedi imajo določen konec veljavnosti, nimajo pa določenega začetka. Takšna dovoljenja ali prepovedi se upoštevajo pri izračunu učinkovitenh pravic v primeru, da je trenutni datum manjši ali enak datumu konca veljavnosti dovoljenja ali prepovedi.

### Dovoljenja ali prepovedi z začetkom in koncem časovne omejitve

Dovoljenja ali prepovedi imajo določen začetek in konec veljavnosti.

Takšna dovoljenja ali prepovedi se upoštevajo pri izračunu efektivnih pravic v primeru, da je trenutni datum večji ali enak začetku veljavnosti, in manjši ali enak koncu veljavnosti dovoljenja ali prepovedi.

Dedovanje eksplicitnih dovoljenj ali prepovedi je odvisno od nastavitve posameznega dovoljenja ali prepovedi. Za več informacij glej poglavje [Lista dostopnih pravic \(ACL\)](#).

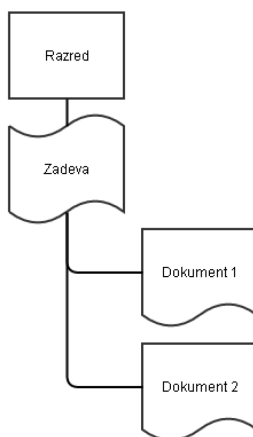
#### **3.3.5.2.6 Efektivne pravice**

Efektivne pravice so skupek podedovanih in eksplicitnih dovoljenj ali prepovedi, ki nam povedo, ali ima uporabnik pravico izvajati operacijo na strežniku IMiS®/ARChive Server.

Vrstni red upoštevanja dovoljenj ali prepovedi pri izračunu efektivnih pravic je naslednji:

1. Eksplicitno dovoljenje (angl. Explicit allow rights).
2. Eksplicitna prepoved (angl. Explicit deny rights).
3. Podedovano dovoljenje (angl. Inherited allow rights).
4. Podedovana prepoved (angl. Inherited deny rights).

Na izračun efektivnih pravic ne vpliva število skupin ali atributov kjer je uporabnik naveden, pač pa samo hierarhija le-teh v listah dostopnih pravic (ACL). Izračun efektivnih pravic za entitete predstavlja primer hierarhije, ki jo predstavlja slika v nadaljevanju.



Slika 4: Hierarhija z razredom, zadevo in dvema dokumentoma

*Primer 1:* Za uporabnika želimo nastaviti pravice branja za celotno hierarhijo entitet, ki jo predstavlja zgornja slika. V listi dostopnih pravic razreda za uporabnika nastavimo eksplicitno dovoljenje branja entitete (»Read« pravica). Dodatno v nastavitvah dovoljenj (angl. Allow) nastavimo, da dovoljenje velja za izbrano entiteto in vse entitete v vsebovanem drevesu entitet.

Dedovanje po hierarhiji (dovoljenje velja za entitete v vsebovanem drevesu entitet) uporabniku omogoča, da ima učinkovite pravice branja na vseh vsebovanih entitetah razreda. Tako lahko uporabnik v našem primeru odpira razred, zadevo in oba dokumenta v načinu samo za branje.

*Primer 2:* Uporabniku iz primera 1 želimo dodati pravice urejanja zadeve in obeh dokumentov v zadevi. Za urejanje entitet sta potrebni pravici branja in pisanja (»Read« in »Write«). Pravico branja ima uporabnik že podedovano od razreda. Zato lahko v listi dostopnih pravic (ACL) zadeve nastavimo samo eksplicitno dovoljenje pisanja za tega uporabnika (dovoljenje velja za izbrano entiteto in vse vsebovane entitete v drevesu). Tako uporabniku nastavimo učinkovite pravice branja in pisanja na zadevi ter na obeh dokumentih znotraj zadeve.

*Primer 3:* Iz primerov 1 in 2 izhaja, da ima uporabnik pravice branja vseh entitet iz hierarhije ter urejanja zadeve in obeh dokumentov v zadevi. Uporabniku želimo prepovedati urejanje dokumenta »Dokument 1«. V listi dostopnih pravic (ACL) dokumenta nastavimo eksplicitno prepoved pisanja (dovoljenje velja za izbrano entiteto). Tako uporabniku na tem dokumentu prepovemo urejanje, saj ima vrstni red upoštevanja prepovedi pri izračunu učinkovnih pravic prednost pred podedovanimi dovoljenji. Uporabnik ima tako še vedno pravico urejanja zadeve in dokumenta »Dokument 2«, nima pa pravice urejati dokumenta »Dokument 1«.

*Primer 4:* V primeru 3 smo uporabniku onemogočili urejanje dokumenta »Dokument 1«. V listi dostopnih pravic (ACL) dokumenta dodamo eksplicitno dovoljenje pisanja. Ker se glede na vrstni red upoštevanja dovoljenj eksplicitna dovoljenja upoštevajo pred eksplicitnimi prepovedmi, uporabnik pridobi učinkovito pravico pisanja ter posledično lahko spreminja dokument.

*Primer 5:* Uporabniku v listi dostopnih pravic (ACL) zadeve dodamo eksplicitno dovoljenje za spreminjanje ACL (pravica »ChangeRights«). Uporabnik tako dobi učinkovito pravico urejanja ACL na zadevi ter na obeh dokumentih.

*Primer 6:* Uporabniku iz primera 5 odvzamemo pravico spreminjanja liste dostopnih pravic (ACL). Hkrati mu želimo onemogočiti urejanje določenega metapodatka, ki se nahaja na zadevi in obeh dokumentih, ker ni javnega značaja. V ACL zadeve nastavimo eksplicitno prepoved pisanja metapodatka za uporabnika (dovoljenje velja za izbrano entiteto in vse vsebovane entitete v drevesu). S tem uporabniku preprečimo urejanje metapodatka kljub temu, da ima pravico urejanja zadeve in obeh dokumentov.

*Primer 7:* Iz liste dostopnih pravic (ACL) razreda uporabniku odstranimo eksplicitno dovoljenje branja. Tako onemogočimo uporabniku odpiranje ter urejanje vseh entitet v hierarhiji.

*Primer 8:* Iz liste dostopnih pravic (ACL) vseh entitet v hierarhiji za uporabnika odstranimo vsa eksplicitna dovoljenja in prepovedi. V ACL razreda dodamo eksplicitna dovoljenja branja, pisanja in brisanja za entiteto ter eksplicitno prepoved brisanja za vse metapodatke v hierarhiji (za vsa dovoljenja in prepovedi velja, da veljajo za izbrano entiteto in vse vsebovane entitete v drevesu).

S tem uporabniku omogočamo urejanje vseh entitet in metapodatkov v hierarhiji, onemogočamo pa brisanje le-teh. Kljub onemogočenem brisanju metapodatkov, pa lahko uporabnik izbriše celotno entiteto z metapodatki, saj ima pravica brisanja entitete prednost pred prepovedjo brisanja metapodatkov.

*Primer 9:* Eksplicitnim prepovedim brisanja metapodatkov iz »primera 8« nastavimo začetek časovne omejitve na datum 1.4.2015 (brez konca). Uporabnik tako izgubi učinkovite pravice brisanja metapodatkov z dnem 1.4.2015, pred tem datum pa uporabnik lahko normalno briše metapodatke.

Če nastavimo konec časovne omejitve na 1.4.2015 (brez začetka), potem uporabnik do 1.4.2015 nima učinkovite pravice brisanja metapodatkov, po 1.4.2015 pa jo pridobi, saj se prepoved ne upošteva več pri računanju učinkovnih pravic, pravica brisanja pa se prenese iz entitete.

*Primer 10:* Iz list dostopnih pravic (ACL) vseh entitet v hierarhiji odstranimo vse eksplicitne prepovedi in dovoljenja, ter nastavimo naslednje ACL vrednosti za uporabnika:

- V ACL razreda nastavimo eksplicitno dovoljenje branja entitete, ki je časovno omejeno od 1.4.2015 do 15.4.2015 (dovoljenje velja za izbrano entiteto in vse vsebovane entitete v drevesu).
- V ACL zadeve nastavimo eksplicitno dovoljenje pisanja in ustvarjanja podrejenih entitet, ki je časovno omejeno od 6.4.2015 do 12.4.2015 (dovoljenje velja za izbrano entiteto in vse vsebovane entitete v drevesu).
- V ACL dokumenta »Dokument 1« nastavimo eksplicitno prepoved pisanja, ki je časovno omejeno od 8.4.2015 do 12.4.2015 (dovoljenje velja za izbrano entiteto).

Glede na nastavljene vrednosti ACL ima uporabnik naslednje časovno omejene pravice:

- Med 1.4.2015 in 15.4.2015 ima uporabnik pravico odpiranja vseh entitet v hierarhiji.
- Med 6.4.2015 in 12.4.2015 ima uporabnik pravico urejanja zadeve in dokumenta »Dokument 2« ter ustvarjanja podrejenih entitet v zadevi.
- Urejanje dokumenta »Dokument 1« je dovoljeno uporabniku med 6.4.2015 in 8.4.2015, saj z 8.4.2015 začne veljati eksplicitna prepoved pisanja dokumenta, ki ima prednost pri računanju učinkovnih pravic in posledično izniči učinkovito pravico pisanja.

- *Pred 1.4.2015 in po 15.4.2015 uporabnik nima pravice odpiranja in urejanja entitet v hierarhiji. Še vedno pa ima pravico branja javnih metapodatkov, če mu globalna varnostna nastavitev to dopušča.*

*Primer 11: Iz list dostopnih pravic (ACL) vseh entitet v hierarhiji odstranimo vse eksplicitne prepovedi in dovoljenja. Predpostavimo, da vse entitete v hierarhiji vsebujejo atributa »Readers« in »Editors«, ki so tipa »DirectoryEntity«. V listo dostopnih pravic razreda dodamo naslednja dovoljenja in prepovedi:*

- *Za atribut »Readers« dodamo dovoljenje branja entitete ter prepoved vseh ostalih pravic (dovoljenje in prepoved velja za izbrano entiteto in vse vsebovane entitete v drevesu).*
- *Za atribut »Editors« dodamo dovoljenje branja in pisanja na entiteti ter prepoved vseh ostalih pravic (dovoljenje in prepoved velja za izbrano entiteto in vse vsebovane entitete v drevesu).*

*Uporabnika dodamo v atribut »Editors« na razredu. Tak uporabnik na razredu prevzame pravice atributa, tako ima sedaj pravice branja in pisanja na vseh entitetah v hierarhiji.*

*Primer 12: Uporabnika iz prejšnjega primera dodamo v atribut »Readers« na entiteti »Dokument 1«. Uporabnik zaradi dedovane hierarhije pridobi pravice branja in pisanja na entiteti »Dokument 1«, vendar pridobi še podedovana dovoljenja in prepovedi iz atributa »Readers« na razredu in jih aplicira na ostale podedovane vrednosti. Za več informacij glej poglavje [Izjeme](#). Ker je ta nastavitev nastavljena tako, da omogoča samo pravico branja, ima uporabnik na entiteti »Dokument 1« samo pravico branja, na vseh ostalih entitetah pa pravico branja in pisanja.*

*Primer 13: Za osnovo vzamemo prejšnji primer. Na zadevo naknadno dodamo dovoljenje brisanja entitete za atribut »Editors«. Dovoljenje označimo, da velja samo za entitete v vsebovanem drevesu entitet. Uporabnika nato dodamo v atribut »Editors« na zadevo. Uporabnik ima tako možnost branja in urejanja razreda in zadeve, obenem pa ima tudi možnost izbrisa entitete »Dokument 2«, saj se dedovane pravice atributa seštevajo. Do entitete »Dokument 1« ohrani samo pravice branja.*

*Primer 14: V listo dostopnih pravic (ACL) iz prejšnjega primera dodamo na entiteto »Dokument 1« za uporabnika eksplicitno dovoljenje brisanja entitete. Uporabnik tako dobi možnost brisanja entitete, saj eksplicitno nastavljene pravice prevladajo nad podedovanimi.*

***Primer 15:** Iz list dostopnih pravic (ACL) vseh entitet v hierarhiji odstranimo vse eksplicitne prepovedi in dovoljenja. Predpostavimo, da imamo navadnega uporabnika »Uporabnik\_1« in pooblaščen osebo »Uporabnik\_2«. Na razred dodamo naslednje kombinacije dovoljenj in prepovedi:*

- *Za uporabnika »Uporabnik\_1« dodamo pravice branja entitete, ki velja za to entiteto ter entitete v vsebovanem drevesu entitet.*
- *Za uporabnika »Uporabnik\_2« dodamo pravice branja in pisanja na entiteti, ki velja za to entiteto in entitete v vsebovanem drevesu entitet, obenem pa dovoljenje velja samo v primeru, ko je »Uporabnik\_2« delegat.*

*Glede na nastavitve dovoljenj in prepovedi imamo naslednje situacije:*

- *Če se »Uporabnik\_1« prijavi v sistem preko normalne seje, ima pravico branja na vseh entitetah v hierarhiji.*
- *Če se »Uporabnik\_2« prijavi v sistem preko normalne seje, nima nobenih pravic nad entitetami v hierarhiji.*
- *Če se »Uporabnik\_2« prijavi v sistem kot delegat »Uporabnika\_1«, ima »Uporabnik\_1« pravice branja in pisanja na vseh entitetah, saj se pravice uporabnikov in delegatov seštevajo. Za več informacij glej poglavje [Lzjeme](#).*

***Primer 16:** Za osnovo vzamemo prejšnji primer, kjer na razred dodamo pravice branja entitete za atribut »Readers« (glej Primer 11). Pravica velja za razred in podrejene entitete v hierarhiji. Naknadno dodamo še uporabnika »Uporabnik\_2« v atribut »Readers« na zadevo. Glede na nastavitve dovoljenj in prepovedi imamo naslednje situacije:*

- *Če se »Uporabnik\_1« prijavi v sistem preko normalne seje, ima pravico branja na vseh entitetah v hierarhiji.*
- *Če se »Uporabnik\_2« prijavi v sistem preko normalne seje, nima pravic na razredu, ima pa možnost branja zadeve in dokumentov.*
- *Če se »Uporabnik\_2« v sistem prijavi kot delegat »Uporabnika\_1«, ima »Uporabnik\_1« pravice branja in pisanja na vseh entitetah, saj se pravice uporabnikov in delegatov seštevajo.*

***Primer 17:** Za osnovo vzamemo prejšnji primer in predpostavimo, da imajo vse entitete še dodaten »DirectoryEntity« atribut, imenovan »DelegatedReaders«. Na razredu za ta atribut nastavimo dovoljenja za branje entitete, vsa ostala dovoljenja pa prepovemo. V dodatnih nastavitvah dovoljenj in prepovedi označimo, da dovoljenja in prepovedi veljajo za izbrano entiteto ter entitete v vsebovanem drevesu entitet. Obenem označimo, da se dovoljenja upoštevajo samo, če je uporabnik, ki se v atributu nahaja delegat.*



Na atribut v zadevi zapišemo uporabnika »Uporabnik\_2«. Glede na nastavitve dovoljenj in prepovedi imamo naslednje situacije:

- Če se »Uporabnik\_1« prijavi v sistem preko normalne seje, ima pravico branja na vseh entitetah v hierarhiji.
- Če se »Uporabnik\_2« prijavi v sistem preko normalne seje, nima pravic na razredu, ima pa možnost branja zadeve in dokumentov.
- Če se »Uporabnik\_2« v sistem prijavi kot delegat »Uporabnika\_1«, ima »Uporabnik\_1« pravice branja in pisanja na vseh entitetah razen na zadevi, saj se upoštevajo tudi pravice delegata.

### 3.3.6 Identifikatorji

Strežnik IMiS®/ARChive Server pozna tri načine identificiranja posameznih entitet.

V vseh načinih identificiranja identifikator določa natančno eno entiteto, oziroma nobene entitete v primeru arhivu neznanega identifikatorja. Identifikator nikoli ne more določati več entitet.

#### 3.3.6.1 Notranji identifikatorji

Notranji identifikator entitete je samodejno generiran niz dolžine 24 ali 32 bajtov (dolžina je odvisna od zahteve odjemalca). Vsebina niza je odvisna tudi od identifikatorja arhiva, ki naj bi bil unikatni za vse arhive. S tem je notranji identifikator posameznih entitet tudi globalno unikatni. Pri generiranju niza strežnik IMiS®/ARChive Server uporablja šifriranje po standardu AES-256, kar zagotavlja zanemarljivo majhno verjetnost zadetka pravilnega identifikatorja v primeru naključnega ugibanja identifikatorjev.

Pri arhivu, ki vsebuje na primer 100.000.000 entitet, je verjetnost, da bo naključno generiran identifikator pravilen, samo  $1 : 1,593 \times 10^{50}$  pri identifikatorju dolžine 24 bajtov in  $1 : 8,636 \times 10^{70}$  pri identifikatorjih dolžine 32 bajtov.

Za shranjevanje identifikatorjev, kjer binarni način shranjevanja ni mogoč, strežnik omogoča tri načine kodiranja notranjih identifikatorjev:

- Šestnajstiško kodiranje, kjer je identifikator predstavljen z nizom znakov iz nabora 0-9, 'a'-'f'. Tak niz je dolg 48 znakov za identifikator velikosti 24 bajtov in 64 znakov za identifikator velikosti 32 bajtov.

- Base64 kodiranje, kjer je identifikator predstavljen z nizom znakov iz nabora velikih in malih črk angleške abecede (52 znakov), števil (0-9) in znakov '-' ter '\_'.  
Tak niz je dolg 32 znakov za identifikatorje velikosti 24 bajtov in 43 znakov za identifikator velikosti 32 bajtov.
- Base85 kodiranje, kjer je identifikator predstavljen z nizom znakov iz nabora base64 in dodatnih 21 znakov: !#\$%&()\*+;<=>?@^`{|}~.

Tako predstavljen notranji identifikator ima dolžino 30 znakov za identifikatorje velikosti 24 bajtov in dolžino 40 znakov za identifikatorje velikosti 32 bajtov.

Način kodiranja notranjih identifikatorjev v svojih zahtevkih določa odjemalec glede na njegove zahteve podatkovnega modela baze, kamor jih bo shranjeval.

### 3.3.6.2 Zunanji identifikatorji

Zunanji identifikatorji so nizi poljubnih znakov dolžine največ 100 znakov, ki nastajajo neodvisno od strežniškega okolja IMiS®/ARChive Server. Strežnik omogoča asociacijo katerekoli entitete s poljubnim številom zunanjih identifikatorjev, pod pogojem, da v istem arhivu še nobena entiteta ni asociirana z enakim identifikatorjem. Asociacija entitete z zunanjimi identifikatorju ni obvezna.

### 3.3.6.3 Klasifikacijska oznaka

Zaradi možnosti hitrejšega upravljanja z entitetami v načrtu razvrščanja gradiva in večje preglednosti, označujemo entitete (razredi, zadeve, dokumenti) v načrtu razvrščanja gradiv. Strežnik IMiS®/ARChive Server samodejno dodeljuje klasifikacijske oznake entitetam v načrtu razvrščanja gradiva glede na položaj razredov in zadev v hierarhiji. Klasifikacijske oznake so enolično določene in se dodeljujejo ob namestitvi ali kasneje pri upravljanju z načrtom razvrščanja gradiva.

V primeru spremembe položaja razreda v načrtu razvrščanja gradiva se vsem entitetam uvrščenim pod ta razred določi nova klasifikacijska oznaka, ki odraža nov položaj v hierarhiji. Nova klasifikacijska oznaka postane nemudoma veljavna za vse entitete uvrščene v ta razred.

Kadar novo-nastali entiteti strežnik zaradi pomanjkljive ali namerno določene konfiguracije ne more samodejno dodeliti klasifikacijske oznake, mora klasifikacijsko oznako ob nastajanju nove entitete določiti uporabnik. Ročno dodeljena klasifikacijska oznaka mora ustrezati naslednjim kriterijem:

- Biti mora enolično določena znotraj nadrejene entitete.
- Če je na števcu nastavljen izraz za preverjanje (angl. Regular expression), potem se mora ročno nastavljena klasifikacijska koda ujemati z nastavljenim izrazom.
- Klasifikacijska koda ne sme vsebovati rezerviranega znaka »^«.

V primeru premeščanja gradiva znotraj arhiva (reklasifikacija), se vsem premaknjenim entitetam spremeni klasifikacijska oznaka glede na naslednje nastavitve nadrejene entitete:

- Če ima nadrejena entiteta nastavitve za ročno dodeljevanje klasifikacijske oznake za vsebovane entitete, se klasifikacijska oznaka premikajočih entitet ohrani.
- Če ima nadrejena entiteta nastavitve za samodejno dodeljevanje klasifikacijske oznake za vsebovane entitete, se vsebovanim entitetam spremeni klasifikacijska oznaka.

Premikajoči entiteti je mogoče tudi ročno določiti novo klasifikacijsko oznako. Nadrejena entiteta, kamor uvrščamo premikajočo entiteto, mora imeti nastavljeno ročno dodeljevanje klasifikacijske oznake oz. kombinacijo samodejnega dodeljevanja z možnostjo ročnega prepisa (angl. override).

Za entitete v premikajočem vsebovanem drevesu entitet to ne velja, saj se vedno upošteva konfiguracija nadrejene entitete. V primeru, da dodeljevanje unikatne klasifikacijske oznake (ročno ali samodejno) ni mogoče, tudi premeščanje gradiva ni mogoče. Strežnik zavrne zahtevo za premik in sporoči napako.

Klasifikacijsko oznako je mogoče ročno spremeniti v primeru, da ima uporabnik pravico urejanja entitete (angl. Write), ter da nastavitve nadrejene entitete dovoljujejo nastavljanje ročne klasifikacijske kode. Pri tej operaciji veljajo vsa prej opisana pravila in omejitve.

V primeru, da je nastavljanje nove klasifikacijske kode uspešno, se v revizijsko sled zapiše dogodek o spremembi klasifikacijske oznake ter stara in nova klasifikacijska oznaka.

### 3.3.6.3.1 Kanonična oblika (angl. Fully Qualified Classification Code – FQCC)

*Primer: C=01^C=02^F=2020-01^D=0001*

Kanonična oblika polne klasifikacijske oznake se uporablja predvsem pri komunikaciji med strežnikom IMiS®/ARChive Server in odjemalci, uporabniki pa take oblike ne vidijo pogosto.

Kanonična oblika polne klasifikacijske oznake je sestavljena iz komponent, kjer posamezna komponenta predstavlja lastno/delno klasifikacijsko oznako entitete iz hierarhije, ki ji izbrana entiteta pripada.

Komponente so med seboj vedno ločene z znakom »^«. Posamezna komponenta je sestavljena iz dveh delov. Prvi del je enoznakovna oznaka za tip entitete: C za razred, F za zadevo in D za dokument. Drugi del komponente je dejanska vrednost klasifikacijske oznake, dela pa sta ločena z znakom '='.

### 3.3.6.3.2 Javna klasifikacijska oznaka (angl. Public Classification Code – PCC)

*Primer: 01.02-2020-01/0001 (ekvivalent primeru kanonične oblike zgoraj)*

Javna klasifikacijska oznaka je oblika, ki uporabnikom predstavlja polno klasifikacijsko oznako. Sestavljena je iz prav toliko komponent kot kanonična oblika, posamezna komponenta pa vsebuje le dejansko vrednost klasifikacijske oznake. Med komponentami so nizi znakov, ki jih administrator pri nastavitvi produkta določi za ločilne znake klasifikacijskih oznak in sicer za vsak tip entitet posebej.

V tem primeru je pred komponentami, ki predstavljajo razrede, znak pika (.), pred komponentami, ki predstavljajo zadeve znak minus (-) in pred zadnjo komponento, ki predstavlja dokument pa je znak poševnica (/).

### 3.3.7 Življenjski cikel

Ločimo dva različna življenjska cikla entitet. Prvi opisuje spremembo statusa, drugi pa zgolj življenjski cikel instance entitete znotraj uporabniške seje. Vse navedeno v nadaljevanju velja za tipe entitet: razred, zadeva in dokument, razen kjer je posebej naveden tip entitete.

#### 3.3.7.1 Status entitete

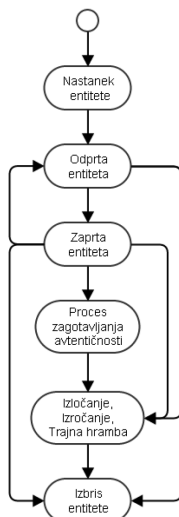
Ob nastanku dobi entiteta podedovano vrednost »Odprto« (angl. Opened). Za več informacij glej poglavje [Hierarhija](#). Uporabnik lahko poljubno nastavlja status s spreminjanjem vrednosti atributa. Po prvem shranjevanju entitete je spreminjanje vrednosti atributa onemogočeno. Uporabnik lahko spremeni status z izvajanjem akcije za spremembo statusa.

V statusu »Odprto« (angl. Opened) uporabnik izvaja operacije nad entitetami, ki omogočajo spreminjanje njenih atributov in dodajanje podrejenih entitet (npr. vlaganje novih dokumentov v zadevo).

Uporabnik spremeni status v »Zaprto« (angl. Closed) šele, ko je povsem prepričan, da entitete ne bo več potrebno spreminjati in pod njo uvrščati novih entitet. Vsebine zaprtih entitet uporabnik ne more spreminjati. Na zaprti entiteti in podrejenih entitetah (glej poglavje [StatusClosed](#)) lahko uporabnik sproži postopek zagotavljanja avtentičnosti (glej poglavje [Predpogoji](#)).

Ta omogoča izdelavo in vzdrževanje dokaznih elementov avtentičnosti, ki bi v primeru kasnejših sprememb entitete v hrambi postali neveljavni.

Izbris entitete je mogoč v katerikoli fazi življenjskega cikla. Brisanje pred postopkom izločanja je izreden dogodek in naj ne bi bil del rednega delovnega procesa v organizaciji. Uporabljen naj bi bil zgolj v primeru zmotnega vnosa entitete in je namenjen popravljanju napak.



Slika 5: Življenjski cikel entitete

### 3.3.7.1.1 Status »Opened«

Status »Opened« povzroči, da je entiteto mogoče odpreti v načinu za pisanje, ter da je dovoljeno dodajanje novih podrejenih entitet (npr. vlaganje novih dokumentov v zadevo). Uporabnik odpre zaprto entiteto tako, da spremeni status samo dotični entiteti, status vseh podrejenih entitet pa ostane zaprt.

Odpiranje zaprte entitete je možno v primeru da:

- je entiteta, ki jo želi odpreti zaprta;
- ima nadrejene entitete odprte.

### 3.3.7.1.2 Status Closed

V statusu »Closed« je mogoče entiteto odpreti zgolj v načinu za branje. Spreminjanje atributov in dodajanje podrejenih entitet je onemogočeno. V kolikor je strežnik IMiS®/ARChive Server nastavljen za zagotavljanje avtentičnosti gradiva, strežnik v seznam entitet, primernih za generiranje dokaznih elementov avtentičnosti, takšne entitete vključi. Zapiranje odprte entitete povzroči zapiranje vseh odprtih podrejenih entitet s statusom.

V primeru, da so zaprte entitete (ter njihove vsebovane entitete) vključene v postopek zagotavljanja avtentičnosti, se za vse spremenjene entitete ponovno generira arhivski informacijski paket (AIP) ter sproži postopek zagotavljanja avtentičnosti. Za več informacij glej poglavje [Predpogoji](#).

### 3.3.7.2 Instanca entitete

Instanca entitete je njena reprezentacija v delovnem spominu strežnika IMiS®/ARChive Server. Pri odpiranju entitete je potrebno najprej preveriti ali je entiteta že v predpomnilniku.

V predpomnilniku je vselej, kadar je uporabljena v drugi seji.

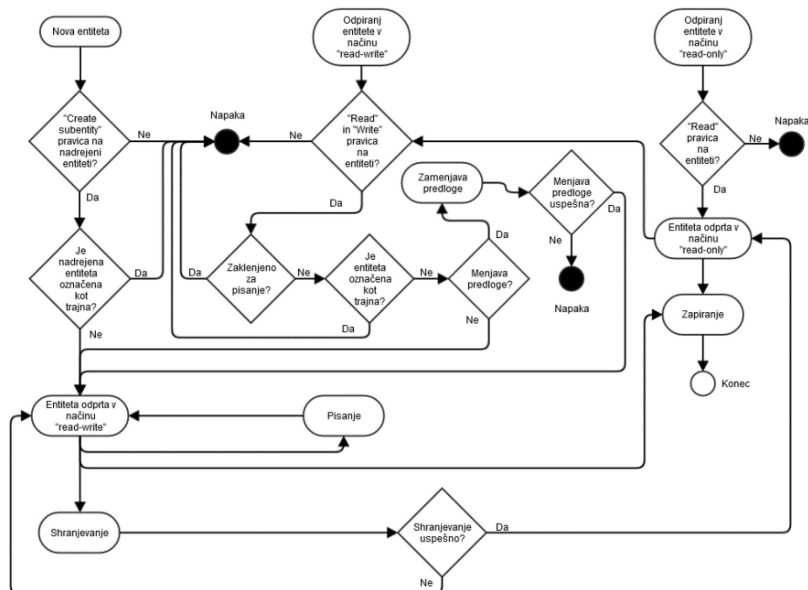
Če entitete še ni v predpomnilniku, se naloži iz podatkovne baze, drugače se uporabi že obstoječa instanca, ki je skupna vsem sejam. Ta model omogoča učinkovito izrabo virov strežnika in hitrejše odzive na zahteve po odpiranju entitet, saj je uporaba že naloženih instanc neprimerno hitrejša od prenašanja iz podatkovne baze.

V primeru dostopa »za pisanje« se v pomnilniku naredi nova kopija entitete, ki ni dostopna nobeni drugi seji. Če ima katera druga seja že odprto svojo kopijo entitete (entiteta je odprta v načinu za pisanje v drugi seji), se dostop zavrne. Prav tako se dostop zavrne, če je entiteta označena kot trajna.

Ostale seje dostopajo do instance, iz katere je bila kopija za pisanje ustvarjena; ta za ostale seje ostane živa in nespremenljiva. Istočasno je dovoljena zgolj ena kopija »za pisanje«.

Posledično, nobena sprememba entitete ni vidna v drugih sejah, dokler se ne izvede postopek shranitve instance, odprte za pisanje. Slednji preveri konsistentnost vnesenih metapodatkov, shrani spremembe v podatkovno bazo in zamenja instanco v predpomnilniku.

Po shranitvi, vse nove operacije odpiranja entitete vračajo spremenjeno instanco. Seje, ki imajo entiteto odprto pred shranitvijo nove instance, novega stanja v obstoječi instanci ne vidijo (model deluje po principu nespremenljivega stanja v časovni točki odpiranja).



Slika 6: Življenjski cikel instance entitete v delovnem spominu strežnika

### 3.3.7.3 Nova entiteta

Ne-shranjena instance entitete nastane kot posledica zahtevka odjemalca, ki mora obvezno vsebovati:

- Veljavni enolični identifikator nadrejene entitete.
- Veljavni enolični identifikator predloge, ki ne sme biti sistemska ali interna.

Nadalje se preveri, če so izpolnjeni naslednji pogoji:

- Pravica dostopa do nadrejene entitete iz naslova stopnje tajnosti.
- Uporabnik ima pravico ustvarjanja novih podrejenih entitet na nadrejeni entiteti.
- Status nadrejene entitete ne sme biti »Closed«.
- Nadrejena entiteta ne sme biti označena za trajno hrambo.

Za več informacij glej poglavje [Odbiranje in izločanje](#).

- Enolični identifikator predloge mora biti vsebovan v spisku dovoljenih entitet na tem delu načrtu razvrščanja gradiva.

Če katerikoli od zgornjih pogojev ni izpolnjen, strežnik IMiS®/ARChive Server vrne odgovor z napako. Sicer se v delovnem pomnilniku naredi nova instance entitete, ki pa se v tej fazi še ne zapiše v podatkovno bazo. Instance je dostopna samo v seji uporabnika, ki je objekt ustvaril.

Če naredimo poizvedbo po novi entiteti iz druge seje, le-ta ni vidna.



Tip entitete določa uporabljena predloga, ki je ni mogoče spreminjati, razen v primeru zamenjave predloge. Za več informacij glej poglavje [Odpiranje entitete za »branje in pisanje« ali »samo za branje«](#).

Pri ustvarjanju entitet iz predlog elektronske pošte se ob ustvarjanju entitete izvede samodejno razčlenjevanje in zapisovanje atributov elektronske pošte (glej poglavje [Atributi dokumentov elektronske pošte](#)). Strežnik podpira samodejno razčlenjevanje za naslednje vrste elektronskih sporočil:

- EML (RFC822).
- Microsoft Outlook MSG (MS-OXMSG).

V tej fazi klasifikacijska oznaka nove entitete ni določena. Entiteta se fizično shrani na strežniku po klicu metode za shranjevanje. Po uspešnem klicu postane entiteta dosegljiva drugim sejam.

#### **3.3.7.4 Odpiranje entitete za »branje in pisanje« ali »samo za branje«**

Zahtevek za odpiranje entitete pri strežniku IMiS®/ARChive Server izvede odjemalec.

Ta določi ali entiteto odpira v načinu samo za branje (»RO«) ali pa v načinu za branje in pisanje – spreminjanje (»RW«).

Strežnik odpre zahtevano instanco entitete (glej poglavje [Instanca entitete](#)) in preveri dostopne pravice. Če stopnja tajnosti entitete dovoljuje dostop in ima uporabnik potrebne dostopne pravice, se dejanje lahko izvede. V primeru odpiranja entitete v načinu »za branje in pisanje«, je možno zamenjati predlogo entitete. Nova predloga mora biti enakega tipa, kar pomeni, da predloge razreda ni mogoče zamenjati s predlogo zadeve ali dokumenta. Poleg tega mora biti predloga v naboru dovoljenih predlog in entiteta ne sme imeti verzij. Strežnik vrne odjemalcu naslednje podatke:

- Referenco na odprto instanco entitete.
- Identifikator njene nadrejene entitete (starša).
- Predlogo, s katero je bila ustvarjena.
- Več sistemskih metapodatkov o entiteti (datum ustvarjanja, zadnje spremembe, efektivne pravice uporabnika nad entiteto, ...).
- Seznam predlog, s katerimi je možno ustvariti podrejene entitete.

Vsi naknadni klici se morajo sklicevati na dano referenco.

Dogodek odpiranja entitete povzroči zapis dogodka v revizijski sledi.

### 3.3.7.5 Branje vsebine entitete

Zahtevek za branje podatkov iz entitete je zahteva strežniku IMiS®/ARChive Server za branje komponent entitete. Entiteta mora biti odprta ali v načinu »samo za branje« ali pa v načinu »za branje in pisanje«.

Zahteva mora vsebovati vsaj:

- Referenco na instanco entitete.
- Obseg branja podatkov.

Obseg branja podatkov vsebuje navodila strežniku, kaj naj v svojem odgovoru na zahtevo vrne.

Zahteva lahko obsega zahtevo za:

- Metapodatke (vsi, javni, navedeni).
- Dostopne pravice (zapisi dostopnih pravic entitete, zapisi dostopnih pravic atributov ali oboji).
- Dokazila o avtentičnosti in celovitosti entitete (AIP in ERS).

V odgovoru odjemalcu strežnik vrne vse vrednosti zahtevanih atributov, z izjemo vrednosti do katerih uporabnik nima pravice dostopa.

V primeru, da uporabnik nima dostopnih pravic, IMiS®/ARChive Server ne javi napake vendar mu vrednosti takih metapodatkov ne vrne.

Dogodek branja vsebine entitete ne povzroči zapisa v revizijsko sled.

### 3.3.7.6 Spreminjanje vsebine entitete

Zahtevek za zapis sprememb komponent instance entitete je zahteva strežniku IMiS®/ARChive Server, da si v svojo instanco entitete v spominu začasno shrani spremembe metapodatkov iz zahtevka. Odjemalec lahko pošlje več zahtevkov za spreminjanje na entiteti, ki je odprta za pisanje. Spremembe se ne shranijo v podatkovno bazo dokler strežnik ne prejme zahtevka za shranjevanje entitete.

Zahtevek vsebuje:

- Referenco na instanco entitete (obvezno).
- Seznam specializiranih sistemskih atributov in njihovih vrednosti.
- Seznam atributov in njihovih vrednosti (vse attribute entitete razen specializiranih sistemskih atributov).
- Seznam spremenjenih dostopnih pravic (dodanih, spremenjenih, izbrisanih).

V kolikor uporabnik spreminja atribut, ki vsebuje več vrednosti, je potrebno zapisati vse vrednosti, tako spremenjene kot tiste, ki ostajajo iste. Pri zapisovanju teh vrednosti se delno preveri tudi veljavnost vrednosti atributov. Za več informacij glej poglavje [Parametri atributov](#). Na strežniku se lahko pošlje več zaporednih zahtevkov za spreminjanje na entiteti odprti za pisanje.

V odgovoru na zahtevek za spreminjanje strežnik odjemalcu odgovori pritrdilno ali vrne napako, da spremembe ni mogoče izvesti. Entiteta se fizično shrani na strežniku po klicu metode za shranjevanje. Po uspešnem klicu postanejo spremembe entitete dosegljive drugim sejam.

Dogodek spreminjanja entitete ne povzroči zapisa v revizijsko sled, morebitne spremembe se zabeležijo v času shranitve, saj se pri spreminjanju spreminja le instanca entitete v delovnem spominu in te spremembe niso trajne.

### 3.3.7.7 Shranitev entitete

Zahtevek za shranitev je zahteva strežniku IMiS®/ARChive Server za shranjevanje entitete.

Entiteta, ki je odprta za pisanje, se fizično zapiše v podatkovno bazo,

kopija zaščiten za pisanje pa se naloži v predpomnilnik. Za več informacij glej poglavje [Instanca entitete](#).

Zahtevek mora vsebovati vsaj:

- referenco na instanco entitete.

Obenem se preveri drugi del veljavnost vrednosti atributov. Za več informacij glej poglavje [Parametri atributov](#). Razlog za dvofazno preverjanje je, da veljavnost vseh atributov ni mogoče preverjati pri shranjevanju. Tipični primer je preverjanje prisotnosti obveznih atributov, ki v posamičnem klicu za spreminjanje instance ni mogoč.

V postopku shranjevanja se preverijo tudi učinkovni roki hrambe na entiteti, če entiteta predstavlja razred, zadevo ali dokument pod razredom.

V primeru, da entiteta nima učinkovnega roka hrambe, shranjevanje ni uspešno.

Če je pri urejanju entitete prišlo do zamenjave predloge, se vrednosti starih atributov, ki jih nova predloga nima, izbrišejo.

Po shranitvi instance entitete ostane entiteta odprta v načinu »samo za branje«, odjemalcu pa se vrne tudi unikatni notranji identifikator entitete, katerega si lahko odjemalec oziroma aplikacija, ki ga uporablja, shrani v podatkovne zbirke tretjih aplikacij za kasnejši neposredni priklic entitete. Po uspešni shranitvi so spremembe entitete vidne na vsaki instanci, ki je bila odprta po shranjevanju. Instance odprte pred shranitvijo, ostanejo nespremenjene v njihovem celotnem življenjskem ciklu.

Shranitev povzroči zapis naslednjih dogodkov v revizijsko sled:

- »Sprememba vrednosti atributa«: v kolikor pride do spremembe enega ali več sistemskih ali specializiranih atributov.
- »Sprememba liste dostopnih pravic«: v kolikor pride do spremembe enega ali več zapisov dostopnih pravic.
- »Sprememba atributa fizičnega gradiva«: v kolikor pride do spremembe enega ali več atributov upravljanja s fizičnim gradivom.
- »Sprememba predloge«: v kolikor pride do spremembe predloge.
- »Entiteta shranjena«.

### **3.3.7.8 Zapiranje entitete**

Zahtevek za zapiranje instance entitete je zahteva strežniku IMiS®/ARChive Server, da zniža število referenc na instanco entitete za 1 in v kolikor je števec referenc padel na 0, zavrže instanco iz predpomnilnika.

Klic za zapiranje se izvede tudi za vse instance entitet neke seje ob njenem zapiranju na katerih ni bil eksplicitno klican zahtevek za zapiranje instance entitete.

Zahtevek mora vsebovati vsaj:

- referenco na instanco entitete.

Po zaprtju entitete postane referenca na instanco entitete neveljavna.

Če je bila zaprta ne-shranjena instanca entitete, odprta »za pisanje«, so spremembe nepovratno izgubljene. Zapiranje ne povzroči zapisa v revizijsko sled.

### 3.3.7.9 Premik entitete

Premik entitete se sproži z zahtevkom za premik. Gre za uvrstitev entitete v drug del načrta razvrščanja gradiva, govorimo lahko tudi o reklasifikaciji.

Zahtevek mora vsebovati vsaj:

- Enolično oznako entitete, ki jo želimo premakniti.
- Enolično oznako entitete pod katero želimo entiteto iz prejšnje točke uvrstiti.
- Razlog za premik.
- Novo delno klasifikacijsko kodo (opsijsko).

Pri premiku strežnik IMiS®/ARChive Server preverja naslednje predpogoje:

- Pravica dostopa do entitete iz naslova stopnje tajnosti.
- Pravica spreminjanja entitete, ki jo premikamo (dodajanje vrednosti sistemskih atributov).
- Pravica premika entitete, ki jo premikamo.
- Pravica dodajanja novih podrejenih entitet pod entiteto, kamor jo uvrščamo (nova lokacija).
- Tarčna entiteta, kamor uvrščamo entiteto, ki se premika, mora dovoljevati ustvarjanje podrejenih entitet s predlogo, s katero je bila izdelana entiteta, ki se premika.
- Tarčna entiteta, kamor uvrščamo entiteto, ne sme biti zaprta.
- Če je delna klasifikacijska koda prisotna v zahtevku, je potrebno preveriti, ali je na tarčni entiteti možno nastaviti ročno/samodejno ustvarjanje klasifikacijske oznake, ki je bila poslana v zahtevku.

Če katerikoli od zgornjih predpogojev ni izpolnjen, je operacija premika zavrnjena.

Skupaj z označeno entiteto se premaknejo tudi vse njene podrejene entitete.

Vsi zgoraj omenjeni predpogoji se preverjajo tudi na podrejenih entitetah.

Klasifikacijske oznake premaknjenih entitet se izračunajo na novo glede na pravila, ki veljajo na novi lokaciji (glej poglavje [Klasifikacijske oznake](#)) in nimajo povezave s starimi oznakami. Uporabnik, ki je sprožil premik, mora obvezno navesti tudi razlog.

Dogodek premika se zabeleži v revizijski sledi premaknjene entitete, hkrati pa pride do zapisa dogodka premika na vseh podrejenih entitetah, ki se z njo premikajo.

Obseg podatkov v vsebini sporočila v revizijski sledi je različna za entiteto, ki se premika in njej podrejene entitete.

### **3.3.7.10 Sprememba stopnje tajnosti entitete**

Spremembo stopnje tajnosti odjemalec sproži z zahtevkom za spremembo stopnje tajnosti.

Zahtevek mora vsebovati vsaj:

- enolično oznako entitete
- novo stopnjo tajnosti
- razlog za spremembo.

Pred spremembo stopnje tajnosti strežnik IMiS®/ARChive Server preverja naslednje predpogoje:

- Pravica dostopa do entitete iz naslova stopnje tajnosti.
- Pravica uporabnika do spremembe stopnje tajnosti na dotični entiteti.
- Pravica do uporabe stopnje tajnosti, ki ustreza uporabnikovi, torej je manjša ali enaka uporabnikovi.

Strežnik najprej preveri ali je operacije spremembe stopnje tajnosti izvedljiva. Stopnja tajnosti ne more biti višja od podedovane s strani nadrejene entitete. V primeru dviga stopnje tajnosti, dvigne stopnjo tajnosti entiteti in njej podrejenim entitetam z enako stopnjo tajnosti, v kolikor imajo podrejene entitete nižjo stopnjo tajnosti, jih pusti nedotaknjene.

V primeru nižanja stopnje tajnosti spremeni stopnjo tajnosti vsem podrejenim entitetam, ki eksplicitno določajo stopnjo tajnosti, na novo raven.

Strežnik ob spremembi stopnje tajnosti samodejno dopolni attribute sprememb stopenj tajnosti na entiteti, kateri neposredno določamo novo stopnjo tajnosti:

- »sys:SecurityClassChangeReason«: razlog za spremembo stopnje tajnosti posreduje uporabnik kot obvezen podatek ob dejanju spremembe stopnje tajnosti.
- »sys:SecurityClassChangeAgent«: uporabnik, ki je spremembo stopnje tajnosti izvedel.
- »sys:SecurityClassChangeDateTime«: datum in čas spremembe stopnje tajnosti.
- »sys:SecurityClassChangeFrom«: vrednost efektivne stopnje tajnosti entitete pred spremembo, lahko je eksplicitna ali podedovana.
- »sys:SecurityClassChangeTo«: vrednost efektivne stopnje tajnosti entitete po spremembi, lahko je eksplicitna ali podedovana.

Vsaka sprememba stopnje tajnosti iz naslova neposredne spremembe ali spremembe kot posledice podrejenosti entiteti, ki se ji stopnja tajnosti spreminja, se zabeleži v revizijsko sled vsakokratne entitete kot dogodek spremembe stopnje tajnosti s prejšnjo vrednostjo, novo vrednostjo in razlogom za spremembo.

### 3.3.7.11 Brisanje entitete

Izbris entitete se odjemalec sproži z zahtevkom za izbris entitete. Zahtevk mora vsebovati vsaj:

- Enolično oznako entitete.
- V kolikor sistemski atribut »sys:Description« entitete nima vrednosti, mu je vrednost možno dodeliti ob izbrisu, saj je opis entitete ob izbrisu obvezen podatek.
- Razlog za izbris.

Pred izbrisom strežnik IMiS®/ARChive Server preverja naslednje predpogoje:

- Pravica uporabnika do izbrisa entitete.
- Prisotnost vseh obveznih metapodatkov: preveri tudi sistemski atribut »sys:Description«, ki v primeru izbrisa postane obvezen.
- Preveri se sistemski atribut »sys:Significance«, če je vrednost atributa nastavljena na 1 («Vital») ali 2 («Permanent»), potem je brisanje entitete onemogočeno.

Način izbrisa je na strežniku mogoče nastaviti tako, da izbris:

- Ohrani celovitost entitete, torej ne pride do izbrisa katere koli komponente entitete (specifikacija Moreq2 9.3.1).
- Povzroči izbris vseh metapodatkov in vsebin razen tistih, ki so obvezni za ohranitev konsistentnosti izbrisane entitete (specifikacija Moreq2 9.3.2).

V obeh primerih se entiteta premakne v sistemski razred izbrisov s klasifikacijsko oznako »C=sys ^C=Trash^C=Deleted«, kjer se zbirajo vsi izbrisi.

Posledično se entiteta vsem uporabnikom »skrije«.

Vsaka izbrisana entiteta ne glede na nastavitev obsega izbrisa ohrani naslednje sistemske attribute:

- »sys:Title«: Naslov entitete.
- »sys:Description«: Opis entitete (prej neobvezen postane v izbrisanih entitetah obvezen). V primeru, da uporabnik poda opis entitete pred izbrisom, se entiteta odpre v načinu za spreminjanje, izvede se popravek atributa in shrani entiteta. Vse spremembe se zabeležijo v revizijski sledi.

Dodatno strežnik samodejno doda naslednje sistemske attribute izbrisane entitete:

- »int:Template«: izvirna predloga s katero je bila entiteta ustvarjena (uporabniku je skrita).
  - »int:ParentId«: notranji identifikator nadrejene entitete, kamor je bila izbrisana entiteta uvrščena (uporabniku skrita).
  - »sys:del:Reason«: razlog za izbris posreduje uporabnik kot obvezen podatek ob izbrisu.
  - »sys:del:Agent«: uporabnik, ki je izbris izvedel.
  - »sys:del:DateTime«: datum in čas izbrisa.
  - »sys:del:ClassificationCode«: klasifikacijska oznaka entitete pred izbrisom.
  - »sys:del:Reference«: referenca na preneseno entiteto – atribut je v primeru brisane entitete prazen, uporablja se samo za prenesene entitete v okviru odbiranja in izločanja.
- Za več informacij glej poglavje [Odbiranje in izločanje](#).

*Opozorilo: Operacija izbrisa je nepovratna.*



V primeru, da se opis entitete posreduje v času izbrisa, pride pred izbrisom do beleženja naslednjih dogodkov v revizijski sledi:

- Odpiranje entitete v načinu za spreminjanje.
- Sprememba systemskega atributa »sys:Description«.
- Shranitev entitete.

Dogodek izbrisa se zabeleži v revizijski sledi izbrisane entitete.

### **3.3.7.12 Sprememba statusa entitete**

Spremembo statusa odjemalec sproži z zahtevkom za spremembo statusa.

Zahtevek mora vsebovati:

- Enolično oznako entitete.
- Novo vrednost statusa.
- Razlog za spremembo (neobvezno).

Pred spremembo stopnje tajnosti strežnik IMiS®/ARChive Server preverja naslednje predpogoje:

- Pravica uporabnika do spremembe statusa na dotični entiteti in vsebovanih entitetah.
- Entiteta, kateri se spreminja status mora imeti nadrejene entitete odprte.

Spremembo statusa lahko delimo v naslednje akcije:

- Odpiranje zaprte entitete.
- Zapiranje odprte entitete.
- Nastavljanje podedovane vrednosti na odprti entiteti.

Odpiranje zaprte entitete: odpiranje zaprte entitete povzroči, da se odpre samo dotična entiteta, njene podrejene entitete pa ostanejo zaprte. V sistemski atribut »sys:Status« se zapiše nov status, v »sys:Opened« se zapiše trenutni datum in čas odprtja, vrednost »sys:Closed« pa se izbriše. Dogodek odprtja se zapiše v revizijsko sled odprte entitete.

Zapiranje odprte entitete: zapiranje odprte entitete povzroči, da se zapre dotična in vse podrejene odprte entitete. Vsem zaprtim entitetam se nastavi »sys:Closed« na trenutni datum in čas ter v »sys:Status« zapiše nova vrednost statusa (samo na dotični entiteti, ker podrejene entitete to vrednost podedujejo). V revizijsko sled vsake zaprte entitete se zapiše dogodek o spremembi statusa.

Nastavljanje podedovane vrednosti: v primeru, da ima odprta entiteta eksplicitno nastavljeno vrednost za status, potem ji s to akcijo nastavimo podedovano vrednost nadrejene entitete. Ker se vsebinsko vrednost statusa za dotično entiteto ni spremenila se tudi akcija ne zapiše v revizijsko sled.

### **3.3.7.13 Prenos neklasificiranih vsebin iz obstoječih arhivov v arhivsko entiteto**

Neklasificirano vsebino predstavljajo dokumenti, ki so bili ustvarjeni s starejšimi odjemalci. Ker slednji ne poznajo koncepta klasifikacije in metapodatkov, ustvarijo vse dokumente v naprej predpisane kontejnerje in z metapodatki, ki so določeni s strežniško konfiguracijo za starejše odjemalce.

S prenosom neklasificiranih vsebin na katerokoli obstoječo arhivsko entiteto se ohrani:

- Revizijska sled, ki pripada neklasificirani vsebini.
- Arhivski informacijski paket in sintaksa evidenčnih podatkov (če so prisotni).

Entiteta, ki je predstavljala kontejner neklasificirane vsebine ni več dostopna, starejši odjemalci pa lahko do vsebine dostopajo preko identifikatorja vsebine.

Prenos neklasificirane vsebine se izvede pod naslednjimi pogoji:

- Entiteta, ki je predmet prenosa, mora predstavljati veljaven kontejner neklasificirane vsebine.
- Entiteta, ki je predmet prenosa ne sme vsebovati verzij ali imeti referenc.
- Če ima arhivska entiteta, v katero se prenaša neklasificirano vsebino verzije, potem se bo vsebina prenesla na trenutno aktualno verzijo.

### 3.3.8 Revizijska sled

Revizijska sled je nespremenljiv kronološki zapis dostopov, poizvedb in sprememb na strežniku IMiS®/ARChive Server. Revizijska sled vsebuje vsaj informacijo o uporabniku, času in dejanju v zvezi s katerim koli dokumentom, zbirko ali razredom načrta razvrščanja gradiva.

Hkrati je dokumentiran zapis o izvajanju določenih postopkov.

Revizijska sled je popolnoma nespremenljiva v svojem celotnem življenjskem ciklu in iz tega vidika zaščitena pred dovoljenimi in nedovoljenimi posegi.

Omogoča beleženje sprememb in pregled nad izvajanjem postopkov.

Namenjena je ugotavljanju izvajanja aktivnosti nad arhiviranimi objekti.

Podatki revizijske sledi se shranjujejo skupaj z arhiviranim gradivom v strežniku.

Za vsako uporabnikovo sejo se v revizijski sledi zabeleži tudi začetek in konec »Revizijske seje« (angl. Audit Session). Vsi dogodki vsebujejo referenco na to sejo.

Podatki, ki se beležijo v revizijski sledi, sledijo določbam Zakona o varstvu osebnih podatkov.

Namen zakona je preprečevati nezakonite in neupravičene posege v zasebnost posameznika pri obdelavi osebnih podatkov, njihovem varovanju in uporabi.

#### 3.3.8.1 Seje

Z odprtjem seje na strežniku IMiS®/ARChive Server se obenem odpre tudi seja revizijske sledi.

Pri odprtju slednje se v podatkovno bazo zapišejo naslednji podatki:

- Uporabniški račun uporabnika, ki se je prijavil.
- Ime (angl. Hostname) računalnika iz katerega je bila seja vzpostavljena.
- Datum in čas začetka seje.
- Interni omrežni naslov (notranji IP naslov mrežnega vmesnika iz katerega je bila seja vzpostavljena, posreduje odjemalec v avtentikacijskih podatkih).
- Javni omrežni naslov (omrežni naslov odjemalca kot ga vidi strežnik).
- Datum ter čas zaključka seje.

- Razlog zaključka seje:
  - seja ni bila zaprta (0)
  - normalen zaključek seje (1)
  - nepričakovan zaključek seje s strani odjemalca (2)
  - iztek dovoljene neaktivnosti (angl. Time-out) (3)
  - nepravilna avtorizacija (4)
  - nepravilni zahtevek (5).
- Uporabniško ime delegata (če gre za delegirano sejo).

Po zapisu teh podatkov seji strežnik dodeli enolični identifikator, ki se ne spreminja v času veljavnosti seje in se uporablja za zapis vsakega dogodka, ki je bil zaznan in sprožen v okviru te seje; postane povezovalni podatek med podatki o seji in vseh dogodkov te seje.

### 3.3.8.2 Dogodki

Vsak dostop do strežnika se zabeleži kot dogodek revizijske sledi.

V vsak zapis dogodka v revizijsko sled se zabeležijo vsaj naslednji parametri:

- Enolični identifikator seje.
- Vrsta dogodka.
- Datum in čas dogodka.

Revizijska sled dovoljuje shranitev naslednjih neobveznih parametrov, ki jih posreduje odjemalec ob dejanju:

- Razlog za dejanje: lahko je parametriziran s »printf« oblikovanim sporočilom ([http://en.wikipedia.org/wiki/Printf\\_format\\_string](http://en.wikipedia.org/wiki/Printf_format_string)).
- Parametri razloga za dejanje: v kolikor je razlog parametriziran, se vsebina parametrov pri izpisu dejanja združi z razlogom za dejanje v enotno sporočilo.

V revizijski sledi se samodejno beležijo naslednji dogodki:

### Nova entiteta [1]

Dogodek se zapiše v revizijsko sled vsakokrat, ko uporabnik ustvari novo entiteto.

Za več informacij glej poglavje [Nova entiteta](#). Ker potrebujemo enolično oznako entitete, ki pa v tej fazi še ni na voljo (dodeli se ob shranjevanju), se dogodek fizično zapiše v podatkovno bazo šele ob shranjevanju s časom shranitve, istočasno kot dogodek »Entiteta shranjena«.

Razlog za tak model beleženja tega dogodka je tudi v tem, da entiteta pred shranitvijo dejansko ne obstaja in na strežniku fizično nastane ob prvi shranitvi.

V poročilo revizijske sledi se zabeleži:

- Enolična oznaka entitete.
- Razlog/sporočilo uporabnika ob ustvaritvi entitete (neobvezno).
- Parametri razloga/sporočila (neobvezno, oziroma obvezno, če je prisoten parametriziran razlog/sporočilo).

### Odpiranje entitete v načinu za branje [2]

Dogodek se zapiše v revizijsko sled vsakokrat, ko uporabnik odpre entiteto v načinu za branje.

Za več informacij glej poglavje [Odpiranje entitete za »branje in pisanje« ali »samo za branje](#).

V poročilo revizijske sledi se zabeleži:

- Enolična oznaka entitete.
- Razlog/sporočilo uporabnika za odpiranje entitete (neobvezno).
- Parametri razloga/sporočila (neobvezno, oziroma obvezno, če je prisoten parametriziran razlog/sporočilo).

### Odpiranje entitete v načinu za branje in pisanje [3]

Dogodek se zapiše v revizijsko sled vsakokrat, ko uporabnik odpre entiteto v načinu za pisanje.

Za več informacij glej poglavje [Odpiranje entitete za »branje in pisanje« ali »samo za branje](#).

V poročilo revizijske sledi se zabeleži:

- Enolična oznaka entitete.
- Razlog/sporočilo uporabnika za odpiranje entitete (neobvezno).
- Parametri razloga/sporočila (neobvezno, oziroma obvezno, če je prisoten parametriziran razlog/sporočilo).

### Entiteta shranjena [4]

Dogodek se zapiše v revizijsko sled, ko se entiteta shrani. Za več informacij glej poglavje

[Shranitev entitete](#).

V poročilo revizijske sledi se zabeleži:

- Enolična oznaka entitete.
- Razlog/sporočilo uporabnika za shranitev entitete (neobvezno).
- Parametri razloga/sporočila (neobvezno, oziroma obvezno, če je prisoten parametriziran razlog/sporočilo).

### Premik entitete [5]

Dogodek se zapiše v revizijsko sled pri premiku.

Za vsako premaknjeno entiteto (pri premiku veje entitet jih je lahko več) se dogodek zabeleži v njeno revizijsko sled. Za več informacij glej poglavje [Premik entitete](#).

V poročilo revizijske sledi se zabeleži:

- Status entitete.
- Stara polna klasifikacijska oznaka.
- Nova polna klasifikacijska oznaka.
- Vrednosti vseh vsebovanih atributov.
- Razlog/sporočilo uporabnika za premik entitete (neobvezno).

### Brisanje entitete [6]

Dogodek se zapiše v revizijsko sled pri izbrisu entitete.

Obvezni podatek o razlogu za izbris se poleg zabeleženja v za to namenjeni atribut zabeleži tudi v revizijski sledi. Za več informacij glej poglavje [Brisanje entitete](#).

V poročilo revizijske sledi se zabeleži:

- Enolična oznaka entitete.
- Razlog/sporočilo uporabnika za izbris entitete (neobvezno)
- Parametri razloga/sporočila (neobvezno, oziroma obvezno, če je prisoten parametriziran razlog/sporočilo).

### Poizvedba revizijske sledi [7]

Dogodek se zapiše v revizijsko sled ob vsakokratni poizvedbi v revizijsko sled.

V poročilo revizijske sledi se zabeleži:

- Iskalni niz, ki ga strežnik oblikuje na podlagi uporabnikove poizvedbe.

### Sprememba nastavitvev revizijske sledi [8]

Dogodek se zapiše v revizijsko sled ob zaznavi strežnika, da je prišlo do spremembe nastavitvev profila revizijske sledi. Ker se nastavitvev spremembe profila revizijske sledi lahko izvede tudi ob zaustavljeni storitvi, se to preverjanje istovetnosti prejšnjih in novih nastavitvev profila revizijske sledi zgodi ob zagonu.

V poročilo revizijske sledi je zabeležena sprememba profila in njegovih nastavitvev.

Spremenjene nastavitve so označene s »\*«.

*Primer:* V sporočilu revizijske sledi se zabeleži:

- *»Audit log profile 'c148d24c-d8c0-4837-b930-cee05cbf1629' enabled state changed to on\*«;*
- *»Audit log profile 'c148d24c-d8c0-4837-b930-cee05cbf1629' required parameters settings changed. UserName: on\* ComputerName: on, PrivateAddress: on, Reason: on\*«;*
- *»Audit log profile 'c148d24c-d8c0-4837-b930-cee05cbf1629' events settings changed. AuditLog.Query: on\*, Entity.Create: on\*, Entity.OpenReadOnly: on\*, Entity.OpenReadWrite: on\*, Entity.Update: on\*, Entity.Move: on\*, Entity.Delete: on\*, Entity.ACLChange: on\*, Entity.PropertiesChange: on\*, Entity.PhysicalRecordsManagementChange: on\*, Entity.SecurityClassChange: on\*, Entity.StatusChange: on\*, Entity.RetentionChange: on\*, Entity.Disposed: on\*, Entity.Permanent: on\*, Entity.Transferred: on\*, Entity.Reviewed: on\*, Content.Move: off, Content.OpenReadOnly: off, Content.OpenReadWrite: off, Content.Create: off, Content.Delete: off, Content.Update: off, Content.MetadataChange: off, Entity.CheckOut: on\*, Entity.CheckIn: on\*, Entity.DiscardPWC: on\*, Entity.TemplateSwitch on\*, Entity.ClassificationCodeChange on\*«.*

Z beleženjem dogodka preprečujemo zlorabe, kjer bi administrator z dostopom do konfiguracije strežnika lahko začasno konfiguracijo strežnika spremenil.

*Primer:* izključitev revizijske sledi za čas ene poizvedbe.

### Sprememba vrednosti atributa [9]

Dogodek se zapiše v revizijsko sled ob shranjevanju entitete in sicer ob spremembi vrednosti enega ali več atributov. Atributi upravljanja s fizičnim gradivom so zavedeni v svojem dogodku in ta dogodek ne beleži. Za več informacij glej poglavje [Spreminjanje vsebine entitete](#) in [Shranitev entitete](#).

V poročilo revizijske sledi se zabeleži:

- Enolična oznaka entitete.
- Seznam vseh spremenjenih atributov.

### Sprememba liste dostopnih pravic [10]

Dogodek se zapiše v revizijsko sled ob shranjevanje entitete in sicer ob spremembi liste dostopnih pravic. Takrat strežnik preveri in primerja obstoječo in novo listo dostopnih pravic ter ugotovi razlike. Za več informacij glej poglavje [Spreminjanje vsebine entitete](#) in [Shranitev entitete](#).

V kolikor je prišlo do spremembe, se v revizijsko sled zabeležita obe listi: stara in nova.

Če je bil dodan kakšen nov vpis v listi se zapiše samo ta, saj stare vrednosti ni.

V primeru izbrisa zapisa iz liste dostopnih pravic se zapiše zgolj stara, saj nove vrednosti ni.

Enolična oznaka atributa se zapiše kadar se spremeni lista dostopnih pravic za atribut.

V poročilo revizijske sledi se zabeleži:

- Enolična oznaka entitete imenika – uporabnik ali skupina.
- Staro stanje zapisa v listi dostopnih pravic.
- Nova stanje zapisa v listi dostopnih pravic.
- Enolična oznaka atributa – v kolikor gre za zapis v listi dostopnih pravic za atribut.



### Sprememba atributov upravljanja s fizičnim gradivom [11]

Dogodek se zapiše v revizijsko sled ob shranjevanju entitete. Zapiše se samo v primeru, ko je bil spremenjen vsaj en atribut upravljanja s fizičnim gradivom. Za več informacij glej poglavje [Spreminjanje vsebine entitete](#) in [Shranitev entitete](#).

V poročilo revizijske sledi se zabeleži:

- Enolična oznaka entitete.
- Vsi spremenjeni in nespremenjeni atributi upravljanja s fizičnim gradivom in njihove vrednosti pred in po spremembi.

### Sprememba stopnje tajnosti [12]

Dogodek se zapiše v revizijsko sled ob spremembi stopnje tajnosti. Za več informacij glej poglavje [Stopnje tajnosti](#).

V poročilo revizijske sledi se zabeleži:

- Stara stopnja tajnosti.
- Nova stopnja tajnosti.
- Komentar.

### Sprememba statusa entitete [13]

Dogodek se zapiše v revizijsko sled ob spremembi statusa entitete.

V poročilo revizijske sledi se zabeleži:

- Nova vrednost statusa.
- Razlog (neobvezno).

### Sprememba politik hrambe in zadržanj v postopku odbiranja in izločanja [14]

Dogodek se zapiše v revizijsko sled ob spremembi učinkovitih politik hrambe ter dodanih ali odvzetih zadržanj entitet v postopku odbiranja in izločanja.

V poročilo revizijske sledi se zapišejo nazivi:

- Dodanih politik hrambe.
- Odvzetih politik hrambe.
- Dodanih zadržanj.
- Odvzetih zadržanj.

### Zamenjava predloge [15]

Dogodek se zapiše v revizijsko sled ob spremembi predloge. V poročilo revizijske sledi se zabeleži:

- Staro in novo ime predloge.
- Razlog (neobvezno).

### Premik vsebine [16]

Dogodek se zapiše v revizijsko sled ob premiku vsebine. Če se premik vsebine izvede znotraj iste entitete, se v revizijsko sled zabeleži:

- Enolični identifikator in opis premikajoče vsebine.
- Izvorno in ponorno ime atributa, kamor se vsebina premika.
- Razlog (neobvezno).

Če gre za premik vsebine med različnimi entitetami, se v revizijsko sled zabeleži:

- Na izvorni entiteti se zabeleži: enolični identifikator in opis premikajoče vsebine, ime atributa (kjer se je premikajoča vsebina nahajala) ter klasifikacijska oznaka ponorne entitete, v katero se je premaknila vsebina.
- Na ponorni entiteti se zabeleži: enolični identifikator in opis premikajoče vsebine, ime atributa (kjer se premikajoča vsebina nahaja) ter klasifikacijska oznaka izvorne entitete, iz katere se je vsebina premaknila.
- Razlog (neobvezno).

### Odpiranje vsebin v načinu za branje [17]

Dogodek se zapiše v revizijsko sled ob odpiranju vsebine v načinu za branje. Za več informacij glej poglavje [Sistemski atributi / sys:Content](#).

V poročilo revizijske sledi se zabeleži:

- Identifikator vsebine.
- Opis vsebine (če je prisoten).
- Razlog (neobvezno).

### Odpiranje vsebin v načinu za urejanje [18]

Dogodek se zapiše v revizijsko sled ob odpiranju vsebine v načinu za urejanje.

V poročilo revizijske sledi se zabeleži:

- Identifikator vsebine.
- Opis vsebine (če je prisoten).
- Razlog (neobvezno).

### Ustvarjanje vsebine [19]

Dogodek se zapiše v revizijsko sled ob ustvarjanju vsebine.

V poročilo revizijske sledi se zabeleži:

- Identifikator vsebine.
- Opis vsebine (če je prisoten).
- Razlog (neobvezno).

### Brisanje vsebine [20]

Dogodek se zapiše v revizijsko sled ob brisanju vsebine.

V poročilo revizijske sledi se beleži:

- Identifikator vsebine.
- Opis vsebine (če je prisoten ob izbrisu).
- Razlog (neobvezno).

### Shranjevanje vsebine [21]

Dogodek se zapiše v revizijsko sled ob shranjevanju spremenjene vsebine.

V poročilo revizijske sledi se zabeleži:

- Identifikator vsebine.
- Opis vsebine (če je prisoten).
- Razlog (neobvezno).

### Sprememba metapodatkov vsebine [22]

Dogodek se zapiše v revizijsko sled ob spremembi metapodatkov vsebine (sprememba opisa).

V poročilo revizijske sledi se zabeleži:

- Identifikator vsebine.
- Nov opis vsebine (če je prisoten).
- Razlog (neobvezno).

### Izločanje entitete [23]

Dogodek se zapiše v revizijsko sled ob izločanju entitete v postopku odbiranja in izločanja.

V poročilo revizijske sledi se zabeleži:

- Razlog izločanja.
- Komentar (neobvezno).

### Trajna hramba entitete [24]

Dogodek se zapiše v revizijsko sled ob označevanju entitete za trajno v postopku odbiranja in izločanja.

V poročilo revizijske sledi se zabeleži:

- Razlog za trajno hrambo.
- Komentar (neobvezno).

### Izročanje entitete [25]

Dogodek se zapiše v revizijsko sled ob izročanju entitete v postopku odbiranja in izločanja.

V poročilo revizijske sledi se zabeleži:

- Razlog izročanja.
- Komentar (neobvezno).

### Izpuščeno za naslednji pregled [26]

Dogodek se zapiše v revizijsko sled ob izpuščanju entitete v postopku odbiranja in izločanja.

V poročilo revizijske sledi se zabeleži:

- Razlog izpustitve.
- Komentar (neobvezno).

### Ustvarjanje osnutka [27]

Dogodek se zapiše v revizijsko sled entitete, iz katere se je izdelal osnutek.

V poročilo revizijske sledi se zabeleži:

- Razlog (neobvezno).
- Verzija, iz katere je bil osnutek narejen.

### Vložitev osnutka [28]

Dogodek se zabeleži v revizijsko sled entitete, v katero se vlaga osnutek.

V poročilo revizijske sledi se zabeleži:

- Razlog (neobvezno).
- Verzija vložene osnutka.

### Zavrženje osnutka [29]

Dogodek se zabeleži v revizijsko sled entitete, iz katere se je osnutek izdelal.

V poročilo revizijske sledi se zabeleži:

- Razlog (neobvezno).

### Sprememba klasifikacijske oznake [30]

Dogodek se zabeleži v revizijsko sled entitete, kateri se spreminja klasifikacijska oznaka.

V poročilo revizijske sledi se zabeleži:

- Razlog (neobvezno).
- Stara in nova klasifikacijska oznaka.

#### **3.3.8.3 Pravica vpogleda v revizijsko sled**

Uporabnik lahko izvaja poizvedbe revizijske sledi v kolikor ima pravico vpogleda v revizijsko sled. Uporabnik ima lahko vpogled v celotno revizijsko sled ali pa ga nima. Pravico pridobi z dodelitvijo vloge »RevizijskaSled« (angl. AuditLogQuery). Rezultat vpogleda je poročilo v XML datoteki, ki je opisano v poglavju [Format poročila](#). Kljub temu, da ima uporabnik pravico vpogleda v revizijsko sled, so lahko v rezultatu poizvedbe tudi dogodki, ki pripadajo entitetam, do katerih uporabnik nima dostopa. Taki dogodki se iz rezultata poizvedbe odstranijo. Rezultat vpogleda je seznam dogodkov, ki ustrezajo iskalnim parametrom, hkrati pa pripadajo entitetam, do katerih ima uporabnik dostop.

#### 3.3.8.4 Poizvedba

Uporabnik lahko pri poizvedbi uporabi naslednje iskalne parametre in tako omeji število rezultatov na dogodke, ki ga dejansko zanimajo:

- Razpon datumov dogodkov.
- Razpon omrežnih (IP) naslovov (npr. od 192.168.1.1 do 192.168.1.99).
- Spisek omrežnih (IP) naslovov.
- Spisek uporabniških imen.
- Spisek imen računalnikov, ki so bili uporabljeni za dostop do sistema.
- Seznam šifriranih enoličnih identifikatorjev entitete.

V primeru, da so iskalni parametri premalo selektivni in bi bilo prikazanih preveč rezultatov, strežnik v odgovoru vrne napako. V tem primeru je priporočljivo ponoviti poizvedbo z bolj natančno določenimi parametri iskanja. Uporabnik najlažje omeji razpon rezultatov s čim manjšim časovnim obdobjem dogodkov.

Iskalne parametre lahko med seboj tudi kombinira, vendar obstajajo omejitve.

Ne glede na ostale parametre lahko vedno išče po datumu poizvedbe in po seznamu šifriranih enoličnih identifikatorjev entitete.

Dodatno lahko izbere en parameter iz naslednjega seznama:

- Razpon omrežnih (IP) naslovov.
- Seznam omrežnih (IP) naslovov.
- Seznam uporabniških imen.
- Spisek imen računalnikov, iz katerih se je izvajal dostop do sistema.

Rezultat poizvedbe je poročilo v XML datoteki, ki je opisano v poglavju [Format poročila](#) v nadaljevanju.

### 3.3.8.5 Format poročila

Poročilo, izdelano na podlagi podatkov iz revizijske sledi, je ključno pri rekonstrukciji dogodkov, ki spremljajo neko arhivirano gradivo v celotnem življenjskem ciklu – od nastanka do izvedbe revizijskega pregleda. Izostanek revizijske sledi praktično onemogoči verodostojen revizijski pregled pooblaščen osebe, ki lahko temelji na podlagi subjektivnih ocen okoliščin in dogodkov.

Kot rezultat vpogleda v revizijsko sled posreduje odjemalcu, ki je vpogled opravil, XML datoteko. Ta je sestavljena po določilih XSD sheme priložene strežniku IMiS®/ARChive Server. XSD shema je dostopna tudi na spletnem naslovu:

<http://www.imis.si/imisarc/auditlog.xsd>.

*Primer:* XML zapis vsebuje rezultat vpogleda v revizijsko sled

```
<?xmlversion="1.0" encoding="UTF-8"?>
<auditlog.query.resultsetxsi:schemaLocation="http://www.imis.si/imisarc
http://www.imis.si/imisarc/auditlog.xsd" xmlns="http://www.imis.si/imisarc"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<sessions>
<!--Audit query sessions.-->
<session id="86055" isAuditQuery="true" closureReason="1" address="192.168.50.15"
internal_address="192.168.80.71" dateTimeOpened="2019-09-30T14:38:53Z" dateTimeClosed="2019-
09-30T14:40:22Z" username="jnovak" computerName="novak-pc"/>
<session id="86057" closureReason="1" address="192.168.50.15" internal_address="192.168.80.71"
dateTimeOpened="2019-09-30T14:40:33Z" dateTimeClosed="2019-09-30T14:40:49Z"
username="fkovac" delegate="jnovak" computerName="Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:69.0) Gecko/20100101 Firefox/69.0"/>
</sessions>
<events>
<!--Sort compare function is QuerySorter::CompareSESS_TS-->
<event sessionId="86055" type="7" seq="0" dateTime="2019-09-30T14:40:07Z" message="Requested
all audit events from '2019-09-30T14:30:00Z' to '2019-09-30T14:40:00Z' "/>
<event sessionId="86057" type="2" seq="1" dateTime="2019-09-30T14:40:38Z"
classificationCode="C=86^F=2019-000001^F=00000001^D=000018"
context="_IDi7wiQzbL1LtR0kxNqzWu3zzm8s5v-"/>
<event sessionId="86057" type="17" seq="2" dateTime="2019-09-30T14:40:43Z"
classificationCode="C=86^F=2019-000001^F=00000001^D=000018"
context="_IDi7wiQzbL1LtR0kxNqzWu3zzm8s5v-" message="Invoice 14-390-0799192.xml
[6n8k2rDOMqwlHmPmyOBXPnO-DNMC5SDg]"/>
</events>
</auditlog.query.resultset>
```

XML datoteko sestavljata dva (2) sklopa:

- »sessions«
- »events«.

#### **3.3.8.5.1 Podatki o sejah: sklop »Sessions«**

Skop »sessions« vsebuje seznam vseh sej, znotraj katerih so bili sproženi iskani dogodki.

Seznam podatkov seje:

- Enolični identifikator seje (Id).
- Razlog zaključka seje (closureReason), seznam možnih razlogov zaključka sej je na voljo v pripadajoči shemi na spletnem naslovu: <http://www.imis.si/imisarc/auditlog.xsd>.
- Javni omrežni (IP) naslov (address).
- Privatni omrežni (IP) naslov (internal\_address).
- Ime računalnika (computerName).
- Čas vzpostavitve seje (dateTimeOpened).
- Čas zaključka seje (dateTimeClosed).
- Enolični identifikator uporabniškega računa - uporabnik (username).
- Enolični identifikator uporabniškega računa v primeru delegirane seje (delegate).

V primeru, da seja še ni zaključena, je vrednost razloga zaključka seje enaka nič, čas zaključka seje pa je nedoločen. To se zgodi v primeru, če je seja še aktivna, ali pa (teoretičen primer), če je med sejo prišlo do nenadzorovane zaustavitve strežnika.

#### **3.3.8.5.2 Podatki o dogodkih: sklop »Events«**

Skop »events« vsebuje seznam iskanih dogodkov in njihovih podatkov.

Seznam podatkov dogodka:

- Sekvenca dogodka v seznamu (seq).
- Identifikator seje (sessionId): referenca na sejo, v okviru katere se je dogodek sprožil.
- Vrsta dogodka (type).
- Čas dogodka (dateTime).
- Klasifikacijska oznaka pripadajočega objekta (classificationCode).
- Šifrirani enolični identifikator entitete (context).
- Poročilo/razlog za dejanje (message).



### 3.3.9 Roki hrambe

Roki hrambe predstavljajo časovni okvir v katerem mora arhivski sistem hraniti entitete. Po pretečenem časovnem okviru se v postopku odbiranja in izločanja odloča, kaj se bo s hranjenimi entitetami zgodilo.

Vsak rok hrambe vsebuje poleg ostalih obveznih atributov tudi naslednja atributa, ki sta ključna za njeno delovanje v pripravi postopka odbiranja in izločanja:

- Atribut »sys:ret:pol:Trigger«: predstavlja iskalni niz s katerim določimo časovni okvir roka hrambe. Za več informacij glej poglavje [Pravila iskalnega niza](#).
- Atribut »sys:ret:pol:Action«: predstavlja privzeto akcijo za entitete, ki bodo postale predmet odbiranja in izločanja po preteku roka hrambe.

Vsaka entiteta v načrtu razvrščanja gradiva (razen dokumenta v zadevi) mora imeti določen vsaj en rok hrambe. Z vzpostavitvijo povezav med entitetami in politikami hrambe nadziramo učinkovite roke hrambe ter s tem posredno postopek priprave za odbiranje in izločanje. Posebno vlogo pri postopu priprave in izvedbe odbiranja in izločanja ima t.i. zadržanje. Zadržanje omogoča, da se iz postopka priprave za odbiranje in izločanje izločijo vse entitete, ki imajo povezavo na vsaj eno zadržanje. Pri postopku izvedbe se za takšne entitete izbrana akcija ne izvede. Zadržanja se tako kot politike hrambe upravlja preko povezav, opisanih v nadaljevanju.

#### 3.3.9.1 Upravljanje s povezavami zadržanj

Zadržanje povežemo na entitete kadar jih želimo zadržati iz postopka odbiranja in izločanja. Zadržanje lahko povežemo na vse vrste entitet, na katere lahko povežemo tudi politike hrambe. Zadržanje velja za entiteto na katero je povezano in za vse vsebovane entitete, ne glede na učinkovite roke hrambe. Zadržanje velja do preklica, oziroma dokler povezava ni odstranjena.

*Primer:* Za primer vzemimo zadevo z vsebovano zadevo »F=2015-00011^F=00001«, ki je v postopku odločanja. Zaradi izjemnega dogodka (npr. tožbe na sodišču) je zadeva »F=2015-00011« ključen material, ki se v času trajanja postopka ne sme uničiti. V tem primeru vežemo zadržanje na zadevo »F=2015-00011«. S tem poskrbimo, da bo zadeva z vsebovano zadevo izločena iz postopka izvedbe odbiranja in izločanja. Prav tako zadeva z vsebovano zadevo ne bo predmet postopka priprave za odbiranje in izločanje, dokler bo povezava na zadržanje obstajala.

### 3.3.9.2 Upravljanje s povezavami politik hrambe

Pri povezavah politik hrambe na entitete lahko določimo naslednje parametre:

- ali je politika omogočena ali onemogočena;
- na katere vrste entitet vpliva politika hrambe (razred, zadeva, dokument uvrščen neposredno pod razred).

S temi parametri nadziramo učinkovitost politik hrambe za posamezne entitete.

Učinkovne politike hrambe so skupek eksplicitnih in podedovanih politik hrambe, ki nam povedo, katere politike imajo učinkoviten vpliv na postopek odbiranja in izločanja posameznih entitet.

Vrstni red upoštevanja povezav politik hrambe pri izračunu učinkovitosti je naslednji:

1. Eksplicitne povezave.
2. Podedovane povezave.

Učinkovni roki hrambe za določeno entiteto se izračunajo na naslednji način:

- Iz celotne veje entitet (vseh nadrejenih entitet) se pregledajo povezave na politike hrambe. Ob upoštevanju hierarhije se preveri, katere politike hrambe vplivajo na trenutno vrsto entitete, za katero se izračunavajo. Rezultat so podedovani roki hrambe.
- Za dotično entiteto se pregledajo eksplicitne povezave na politike hrambe, ki se združijo s podedovanimi politikami hrambe. Rezultat so učinkovni roki hrambe, ki veljajo za to entiteto.

#### *Primeri:*

*Za primer vzemimo konfiguracijo politik hrambe, ki jo prikazuje spodnja tabela.*

Politika hrambe	Časovni okvir
5 let	5 let od datuma ustvarjanja entitete
10 let	10 let od datuma ustvarjanja entitete

Tabela 6: Primer konfiguracije politik hrambe

Imamo naslednje drevo entitet v načrtu razvrščanja gradiva:

$C=3300$

$C=3300^{\wedge}C=3301$

$C=3300^{\wedge}C=3301^{\wedge}F=2015-00100$

$C=3300^{\wedge}C=3301^{\wedge}F=2015-00101$

$C=3300^{\wedge}C=3301^{\wedge}F=2015-00102$

$C=3300^{\wedge}C=3302$

$C=3300^{\wedge}C=3302^{\wedge}D=1000$

$C=3300^{\wedge}C=3302^{\wedge}D=1001$

Glavni razred »C=3300« vsebuje razreda »C=3301« in »C=3302«. Vsebovani razred »C=3301« vsebuje zadeve »F=2015-00100«, »F=2015-00101« in »F=2015-00102«. V vsebovanem razredu »C=3302« se nahajata dokumenta »D=1000« in »D=1001«.

Primer 1: Na glavnem razredu »C=3300« imamo vezano politiko hrambe »5 let«, ki je omogočena za razrede, zadeve in dokumente uvrščene neposredno pod razrede. S to konfiguracijo pokrijemo vse entitete v drevesu, saj se politika hrambe deduje na vse vrste entitet v drevesu.

Primer 2: Konfiguracijo iz prejšnjega primera spremenimo tako, da politiko hrambe »5 let« omogočimo za razrede in zadeve. Taka konfiguracija je neveljavna, saj se politika hrambe deduje na vse vrste entitet v drevesu razen za dokumente pod razredom, ki pa nimajo eksplicitnih povezav na politike hrambe.

Primer 3: Na vsebovani razred »C=3302« dodamo eksplicitno povezavo za politiko hrambe »10 let«, in jo omogočimo za dokumente, hkrati pa na razredu »C=3300« omogočimo politiko hrambe »5 let« za razrede in zadeve. Taka konfiguracija je ustrezna, saj velja politika hrambe »5 let« za vse razrede in zadeve, politika hrambe »10 let« pa velja samo za dokumente v vsebovanem razredu »C=3302«.

Primer 4: Na razred »C=3300« povežemo politiko hrambe »10 let« ter jo omogočimo za razrede in dokumente. Na vsebovan razred »C=3301« povežemo politiko hrambe »5 let«, in jo omogočimo za zadeve. Takšna konfiguracija določa, da se bodo zadeve odbirale po politiki hrambe »5 let«, razredi in vsebovani razredi z dokumenti pa po politiki hrambe »10 let«.

Primer 5: Na razred »C=3300« povežemo politiko »10 let« in jo omogočimo za razrede in dokumente. Na isti razred povežemo še politiko »5 let« in jo omogočimo za zadeve. Taka konfiguracija nam omogoča odbiranje vseh zadev znotraj razreda po politiki hrambe »5 let«, odbiranje razredov in dokumentov pod njimi pa po politiki hrambe »10 let«.

Primer 6: Na razred »C=3300« povežemo politiko hrambe »10 let«, in jo omogočimo za razrede, zadeve in dokumente. Na vsebovani razred »C=3301« povežemo politiko hrambe »10 let« in jo onemogočimo za razrede in zadeve, hkrati pa povežemo politiko hrambe »5 let« in jo omogočimo za razrede in zadeve. S takšno konfiguracijo lahko odbiramo razrede, zadeve in dokumente pod razredi s politiko hrambe »10 let« razen vsebovanega razreda »C=3301«, ki ima politiko hrambe »10 let« onemogočeno, ima pa omogočeno politiko hrambe »5 let«, ki je omogočena za razrede in zadeve.

Primer 7: Na razred »C=3300« vežemo politiko hrambe »10 let« in jo omogočimo za razrede, zadeve in dokumente. Nato na vsebovani razred »C=3301« vežemo politiko hrambe »5 let« in jo omogočimo za zadeve. Konfiguracija je sicer veljavna, saj imajo vse vrste entitet v drevesu učinkovito politiko hrambe. Vendar pa so zadeve v vsebovanem razredu »C=3301« v konfliktu, saj imajo podedovani obe politiki hrambe (politika »10 let« se deduje od glavnega razreda »C=3300«, politika »5 let« pa se deduje od vsebovanega razreda »C=3301«). V primeru, da se bo pripravljalo odbiranje in izločanje po eni ali obeh politikah hrambe, bodo zadeve zmeraj prisotne zaradi konflikta.

Primer 8: Na razred »C=3300« vežemo politiko hrambe »10 let«, in jo omogočimo za razrede, zadeve in dokumente. Na zadevo »F=2015-00100« povežemo politiko »10 let« in jo onemogočimo za zadeve, hkrati pa na isto zadevo povežemo politiko hrambe »5 let« in jo omogočimo za zadeve. Enako naredimo še za zadevi »F=2015-00101« in »F=2015-00102«. S tako konfiguracijo lahko odbiramo zadeve po politiki hrambe »5 let«, razrede in dokumente pod razredi pa po politiki hrambe »10 let«.

Primer 9: Na razred »C=3300« vežemo politiko hrambe »10 let« in jo omogočimo za razrede, zadeve in dokumente. Na vsebovani razred »C=3302« vežemo politiko hrambe »10 let« in jo onemogočimo za dokumente. Konfiguracija je neveljavna, saj dokumenti v vsebovanem razredu nimajo učinkovitih politik hrambe. Če pa na oba dokumenta v vsebovanem razredu vežemo recimo politiko hrambe »5 let« in jo omogočimo za dokumente, potem lahko na vsebovanem razredu »C=3302« onemogočimo politiko hrambe »10 let« za dokumente, saj imajo vsi dokumenti v vsebovanem razredu vsaj eno učinkovito politiko hrambe.

Primer 10: V drevesu entitet imamo naslednjo konfiguracijo: na razred »C=3300« je vezana politika »10 let«, ki je omogočena za razrede. Na vsebovani razred »C=3301« je vezana politika »5 let«, ki velja za zadeve, na vsebovani razred »C=3302« je tudi vezana politika »5 let«, ki pa velja za dokumente. Želeli bi, da bi politika »10 let« veljala za vse entitete v drevesu entitet. Najlažji način je, da najprej omogočimo na razredu »C=3300« politiko »10 let« za razrede, zadeve in dokumente. S to potezo sicer naredimo konflikt za zadeve in dokumente, vendar pa, če odstranimo povezavi na politike na vsebovanih razredih »C=3301« in »C=3302«, rešimo nastali konflikt, hkrati pa nam konfiguracija politike na razredu »C=3300« pokrije celotno drevo entitet s politiko hrambe »10 let«.

### 3.3.10 Upravljanje z vsebinami

Vsebina je poleg metapodatkov pomemben del celote entitete. Poleg ustvarjanja, spreminjanja in brisanja vsebine lahko z vsebino upravljamo tudi na naslednje načine:

- Samodejna pretvorba vsebine.
- Izvajanje drugih akcij nad vsebino.

#### 3.3.10.1 Samodejno pretvarjanje vsebin

Samodejna pretvorba vsebin je postopek, kjer se za določen tip vsebine ustvari več reprezentacij iste vsebine, v različnih formatih. Tako lahko pretvarjamo BMP slike v TIFF format, MS Word dokumente v PDF/A, ... ipd.. Vse samodejno ustvarjene vsebine so odvisne od originalne vsebine, zato za njih velja nekaj omejitev:

- Brisanje vsebine, ki ima odvisne vsebine ni dovoljeno, razen če se eksplicitno izbrišejo tudi vse odvisne vsebine.
- Premikanje in urejanje odvisne vsebine ni dovoljeno, razen če se vsebine ne odklopi (angl. Detach) ter jo naredi samostojno.

Samodejno pretvarjanje vsebin se izvaja s pomočjo vtičnikov, ki jih s konfiguracijo povežemo v verige. Verige se nato izvajajo na strežniku ter ustvarjajo odvisne vsebine.

*Primer konfiguracijske verige:*

```
<ns1:Converter xsi:type="ns1:ConverterSettings">
  <ns1:Id xsi:type="xsd:string">c6d25a2e-f1ea-40ba-9267-39e4c6b72ef1</ns1:Id>
  <ns1:SourceOperation xsi:type="ns1:ContentSourceOperation">None</ns1:SourceOperation>
  <ns1:Filter xsi:type="ns1:ContentTypeFilter" disposition="Include">
    <ns1:ContentType xsi:type="xsd:string">image/bmp</ns1:ContentType>
  </ns1:Filter>
  <ns1:Output queueForFTI="true" nextConverterId="c3287e71-068a-4ec5-9277-985303f810de"
descriptionExpression="%DESC_BASE%-
%NOW_HOUR%:%NOW_MINUTE%:%NOW_SECOND%.jpg">image/jpeg</ns1:Output>
  <ns1:Provider xsi:type="ns1:ServiceProvider" id="ImageMagic-BMP" type="Plugin"
driver="libiaconvim.so.1">
    <ns1:Arguments
xsi:type="xsd:string">&lt;/WorkDirectory>/iarc/work/conversion&lt;/WorkDirectory><ConversionReason>Conversion to JPEG</ConversionReason></ns1:Arguments>
  </ns1:Provider>
  <ns1:Name xsi:type="xsd:string">ImageMagick</ns1:Name>
  <ns1:Description xsi:type="xsd:string">Conversion with ImageMagick</ns1:Description>
</ns1:Converter>
```

```

<ns1:Converter xsi:type="ns1:ConverterSettings">
  <ns1:Id xsi:type="xsd:string">c3287e71-068a-4ec5-9277-985303f810de</ns1:Id>
  <ns1:SourceOperation xsi:type="ns1:ContentSourceOperation">None</ns1:SourceOperation>
  <ns1:Filter xsi:type="ns1:ContentTypeFilter" disposition="Include"/>
  <ns1:Scope xsi:type="ns1:EntityId" type="ClassificationCode">C=61</ns1:Scope>
  <ns1:Output queueForFTI="true" descriptionExpression="picture.tiff">image/tiff</ns1:Output>
  <ns1:Provider xsi:type="ns1:ServiceProvider" id="ImageMagic-TIFF" type="Plugin"
driver="libiaconvim.so.1">
  <ns1:Arguments
xsi:type="xsd:string">&lt;WorkDirectory>/iarc/work/conversion&lt;/WorkDirectory><ConversionReason>Conversion to TIFF</ConversionReason></ns1:Arguments>
  </ns1:Provider>
  <ns1:Name xsi:type="xsd:string">ImageMagick2</ns1:Name>
  <ns1:Description xsi:type="xsd:string">Conversion with ImageMagick2</ns1:Description>
</ns1:Converter>

```

Veriga je sestavljena iz dveh vtičnikov. Prvi vtičnik (id: c6d25a2e-f1ea-40ba-9267-39e4c6b72ef1) najprej pretvori BMP v JPEG, nato pa drugi vtičnik pretvori JPEG v TIFF. Rezultat so tri med seboj odvisne datoteke (JPEG je reprezentacija BMP, TIFF je reprezentacija JPEG). Za vsako pretvorbo se izdelava tudi dnevnik pretvorbe (angl. Conversion log) z naslednjimi informacijami:

- Datum pretvorbe.
- Informacije o pretvorbi.
- Informacije o programski opremi, ki je pretvorbo izvedla.
- Razlog za pretvorbo.
- Id objekta, ki je rezultat pretvorbe.
- Opis objekta, ki je rezultat pretvorbe.

Primer dnevnikov pretvorbe, ki so rezultat konfiguracijske verige:

```
<iarc:convertlog xmlns:iarc="http://www.imis.si/imisarc/commitlog.xsd">
  <iarc:object>
    <iarc:conversionDateTime>2020-09-04T13:11:29Z</iarc:conversionDateTime>
    <iarc:conversionProcessInfo>Processed output resolution: 100 x
100</iarc:conversionProcessInfo>
    <iarc:conversionSoftwareInfo>ImageMagick 6.7.2-7 2016-06-16 Q16
http://www.imagemagick.org</iarc:conversionSoftwareInfo>
    <iarc:conversionReason>Conversion to JPEG</iarc:conversionReason>
    <iarc:id
iarc:valuetype="3">0b6db3842fd0e08daa6abcb99840a1e6fa57ea966677796c3fbb6c4077b4641c</i
arc:id>
    <iarc:description>picture-04-13-11.jpg</iarc:description>
  </iarc:object>
</iarc:convertlog>

<iarc:convertlog xmlns:iarc="http://www.imis.si/imisarc/commitlog.xsd">
  <iarc:object>
    <iarc:conversionDateTime>2020-09-04T13:11:29Z</iarc:conversionDateTime>
    <iarc:conversionProcessInfo>Processed output resolution: 100 x
100</iarc:conversionProcessInfo>
    <iarc:conversionSoftwareInfo>ImageMagick 6.7.2-7 2016-06-16 Q16
http://www.imagemagick.org</iarc:conversionSoftwareInfo>
    <iarc:conversionReason>Conversion to TIFF</iarc:conversionReason>
    <iarc:id
iarc:valuetype="3">0a1a0d2f930d09b47ee1bee0cadf3c45e6e4805583cbe936c2c9f298bc368cab</i
arc:id>
    <iarc:description>picture.tiff</iarc:description>
  </iarc:object>
</iarc:convertlog>
```

V nadaljevanju sledi podroben opis posameznih etiket in atributov konfiguracijskega XML.

**Etiketa »Id«:** Etiketa vsebuje unikatni identifikator vtičnika.

**Etiketa »SourceOperation«:** Vrednost etikete predstavlja operacijo, ki se bo izvedla po uspešni pretvorbi na izvorni vsebini. Naslednja tabela prikazuje veljavne vrednosti z njihovimi opisi.

Vrednost	Opis
NONE	Izvorna vsebina ostane nedotaknjena.
DELETE	Izvorna vsebina se izbriše.
REPLACE	Izvorna vsebina se nadomesti z vsebino, ki je bila na novo ustvarjena.

Tabela 7: Vrednosti etikete »SourceOperation«

**Etiketa »Filter«:** Vrednost etikete predstavlja vhodni seznam MIME tipov, katere lahko vtičnik pretvori (vrednost atributa »disposition« je »Include«) oziroma za katere vtičnik nima podpore (vrednost atributa »disposition« je »Exclude«). Če je vrednost »disposition« atributa »Include« in je seznam prazen, potem tak vtičnik ni konfiguriran kot vhodni vtičnik v verigi.

**Etiketa »Output«:** Vrednost etikete predstavlja MIME tip pretvorjene vsebine. Naslednja tabela prikazuje attribute etikete ter njihove opise.

Atribut	Opis
queueForFTI	Vrednost »True« pomeni, da se bo novo ustvarjena vsebina indeksirala za kasnejše iskanje po vsebini. Vrednost »False« pomeni, da se vsebina ne bo indeksirala.
nextConverterId	Vrednost je unikatni identifikator vtičnika, ki bo naslednji izvajal pretvarjanje vsebine. Če atribut ni prisoten se pretvorbena veriga konča.



Atribut	Opis
descriptionExpression	<p>Vrednost predstavlja opis vsebine, ki jo bo vtičnik ustvaril.</p> <p>Če atribut ni prisoten je opis enak opisu izvorne vsebine.</p> <p>Rezervirane besede za opis so naslednje:</p> <ul style="list-style-type: none"> <li>• %PAGE_COUNT% - beseda se nadomesti s številom strani pretvorjene vsebine;</li> <li>• %DESC_BASE% - beseda se nadomesti z opisom izvorne vsebine brez končnice (za končnico se šteje zapis za zadnjo piko v izvornem opisu);</li> <li>• %DESC_EXT% - beseda se nadomesti s končnico (pika je vključena) iz izvornega opisa;</li> <li>• %DESC% - beseda se nadomesti z izvornim opisom vsebine;</li> <li>• %NOW_YEAR% - beseda se nadomesti z letom trenutnega datuma pretvorbe;</li> <li>• %NOW_MONTH% - beseda se nadomesti z mesecem trenutnega datuma pretvorbe;</li> <li>• %NOW_DAY% - beseda se nadomesti z dnevom trenutnega datuma pretvorbe;</li> <li>• %NOW_HOUR% - beseda se nadomesti z uro trenutnega časa pretvorbe;</li> <li>• %NOW_MINUTE% - beseda se nadomesti z minuto trenutnega časa pretvorbe;</li> <li>• %NOW_SECOND% - beseda se nadomesti s sekundo trenutnega časa pretvorbe.</li> </ul>

Tabela 8: Atributi etikete »Output«

**Etiketa »Provider«:** Vrednost etikete so argumenti, ki jih posamezen vtičnik potrebuje za pretvarjanje vsebine. Naslednja tabela prikazuje attribute etikete ter njihove opise.

Atributi	Opis
id	Identifikator vtičnika
type	Tip vtičnika – vrednost mora biti »Plugin«
driver	Ime datoteke, kjer se vtičnik nahaja

Tabela 9: Atributi etikete »Provider«

**Etiketa »Name«:** Etiketa je opsijska, vrednost etikete predstavlja ime vtičnika.

**Etiketa »Description«:** Etiketa je opsijska, vrednost etikete pa predstavlja kratek opis vtičnika.

### 3.3.10.2 Izvajanje drugih operacij

Poleg prej opisanih operacij lahko nad vsebino entitete izvajamo še:

- Premikanje vsebine (angl. Move).
- Odklapanje odvisne vsebine (angl. Detach).
- Kloniranje vsebine (angl. Clone).
- Izvajanje zahtev za indeksiranje (angl. Index) in samodejno pretvorbo vsebin (angl. Convert).

**Premikanje vsebine:** Vsebino lahko premikamo med entitetami. Pogoji so, da je vsebina neodvisna, ter da se premik izvaja med atributi istega tipa. Izvorna entiteta mora biti odprta v načinu za urejanje. Uporabnik mora imeti na tarčnih entitetah pravico urejanja, saj se tarčne entitete ob premiku vsebine implicitno odprejo v načinu za urejanje. Premik vsebine se dejansko izvede ob shranitvi izvorne entitete.

**Odklapanje odvisne vsebine:** Odvisno vsebino, ki je rezultat avtomatične pretvorbe lahko odklopimo. S tem dobimo neodvisno vsebino, za katero veljajo vse lastnosti kot za druge neodvisne vsebine.

**Kloniranje vsebine:** Vsebino lahko kloniramo med entitetami.

Izpolnjeni morajo biti naslednji pogoji:

- vsebina se klonira med atributi istega tipa;
- izvorna entiteta je odprta v načinu za branje;
- tarčna entiteta je odprta v načinu za urejanje.

Kloniranje vsebine se dejansko izvede ob shranitvi tarčne entitete.

**Izvajanje zahtev za indeksiranje vsebine:** Za vsako vsebino (tako odvisno kot neodvisno) se lahko izvaja zahteva za indeksiranje. Entiteta, ki vsebino vsebuje mora biti odprta v načinu za branje. Uporabnik pa mora imeti »ContentManagement« vlogo, drugače je zahteva za indeksiranje vsebine zavrnjena.

**Izvajanje zahtev za samodejno pretvorbo vsebin:** Zahtevo za samodejno pretvorbo vsebin lahko izvaja uporabnik z vlogo »ContentManagement«, vsebina mora biti neodvisna, entiteta pa mora biti odprta v načinu samo za branje. V nasprotnem primeru se zahteva za avtomatsko pretvorbo vsebine zavrne.

### 3.3.11 Reference

Reference predstavljajo simbolične povezave med entitetami. Z referencami lahko povezujemo različne entitete med seboj. Osnovni pogoj za vzpostavitev povezave je, da ima uporabnik na vseh entitetah, ki jih hoče povezati med seboj efektivno pravico branja in ustvarjanja reference. Za več informacij glej poglavje [Dostopne pravice za entiteto](#). Z referencami lahko povezujemo med seboj entitete, ki so razvrščene pod različnimi zadevami, vendar so si podobne po vsebini ali drugih karakteristikah in tako predstavljajo vsebinsko celoto. Povezave med entitetami lahko dodajamo in odzemamo, pogoj za obstoj reference pa je, da sta med seboj povezani najmanj dve entiteti. Če povezane entitete izbrišemo, samodejno izbrišejo tudi reference.

### 3.3.12 Kategorije

Kategorije omogočajo dodatno razvrščanje entitet, ki se nahajajo v pregledih (rezultat iskanja, seznam vsebovanih entitet, ...). Ob ustvarjanju pregleda lahko uporabnik določi, kateri atributi bodo uporabljeni za kategorizacijo. Njihove vrednosti se nato uporabijo kot kategorije.

Poseben atribut, ki je namenjen kategorizaciji je »sys:Category«, lahko pa se uporabijo tudi drugi tipi atributov, ki niso tipa »File«, »StringMax« ali »Binary«. Za več informacij glej poglavje [Vrste](#).

Kategorije so lahko tudi gnezdene, ločitveni znak za gnezdenje kategorij je »\«.

Entitete, ki v procesu kategorizacije ne ustrezajo posamezni kategoriji, se uvrstijo pod posebno kategorijo, imenovano »Nekategorizirano«. Tako se lahko ena entiteta nahaja v različnih kategorijah in je hkrati uvrščena v kategorijo »Nekategorizirano«. Razlogov za to je lahko več, najpogostejši pa je ta, da entiteta nima kategorizacijskih atributov, oziroma so kategorizacijski atributi prazni. V nadaljevanju so različni primeri kategorizacije entitet.

**Primer 1:** Imamo 4 dokumente, ki imajo vrednosti ključnih besed »K01« in »K01\01«, kot prikazuje naslednja tabela. Kategorizacija se izvede glede na vrednost ključnih besed. Dokument 1 in 2 se kategorizirata pod kategorijo »K01«, dokument 3 in 4 pa se kategorizirata v podkategorijo »K01\01«.

Naziv entitete	Vrednosti ključnih besed
Dokument 1	K01
Dokument 2	K01
Dokument 3	K01\01
Dokument 4	K01\01

Tabela 10: Kategorizacija (primer 1)

**Primer 2:** Imamo 4 dokumente, ki imajo vrednosti ključnih besed »K01«, »K02« in »K01\01«, kot je prikazano v naslednji tabeli. Kategorizacija se izvede glede na vrednost ključnih besed.

Rezultat kategorizacije so 3 kategorije:

- Kategorija »K01«: v tej kategoriji sta dokument 1 in dokument 2.
- Kategorija »K02«: v tej kategoriji se nahaja dokument 1.
- Podkategorija »K01\01«: v tej podkategoriji se nahajata dokument 3 in dokument 4.

Naziv entitete	Vrednosti ključnih besed, ločene z »,«
Dokument 1	K01, K02
Dokument 2	K01
Dokument 3	K01\01
Dokument 4	K01\01

Tabela 11: Kategorizacija (primer 2)

**Primer 3:** Imamo 4 dokumente, ki imajo vrednosti ključnih besed »K01«, »K01\01« in »K02«, kot je prikazano v naslednji tabeli. Rezultat kategorizacije je glede na ključne besede naslednji:

- Kategorija »K01«: v kategoriji se nahajajo vsi dokumenti. Pri vseh dokumentih je prisotna v ključnih besedah.
- Kategorija »K02«: v kategoriji se nahaja dokument 1.
- Podkategorija »K01\01«: v podkategoriji se nahajata dokumenta 3 in 4.

Naziv entitete	Vrednosti ključnih besed, ločene z »,«
Dokument 1	K01, K02
Dokument 2	K01
Dokument 3	K01, K01\01
Dokument 4	K01, K01\01

Tabela 12: Kategorizacija (primer 3)

**Primer 4:** Imamo 4 dokumente iz prejšnjega primera, kjer za dokument 1 izbrišemo ključne besede, kot je prikazano v naslednji tabeli. Rezultat kategorizacije po ključnih besedah je naslednji:

- Kategorija »K01«: v kategoriji so dokumenti 2, 3 in 4.
- Podkategorija »K01\01«: v podkategoriji sta dokumenta 3 in 4.
- Kategorija »Nekategorizirano«: v kategoriji se nahaja dokument 1.

Naziv entitete	Vrednosti ključnih besed, ločene z »,«
Dokument 1	/
Dokument 2	K01
Dokument 3	K01, K01\01
Dokument 4	K01, K01\01

Tabela 13: Kategorizacija (primer 4)

**Primer 5:** Dokumente iz prejšnjega primera kategoriziramo po ključnih besedah ter po atributu »sys:Category«, katerega imajo vsi dokumenti in nima vrednosti. Rezultat kategorizacije je naslednji:

- Kategorija »K01«: v kategoriji so dokumenti 2, 3 in 4.
- Podkategorija »K01\01«: v podkategoriji sta dokumenta 3 in 4.
- Kategorija »Nekategorizirano«: v kategoriji se nahajajo vsi dokumenti, saj nimajo nastavljenih vrednosti za atribut »sys:Category«.

**Primer 6:** Imamo 4 dokumente iz prejšnjega primera z vrednostmi atributov, ki so prikazane v naslednji tabeli. Rezultat kategorizacije po atributih je naslednji:

- Kategorija »K01«: v kategoriji so dokumenti 2, 3 in 4.
- Podkategorija »K01\01«: v podkategoriji sta dokumenta 3 in 4.
- Kategorija »CAT01«: v kategoriji se nahaja dokument 1.
- Kategorija »Nekategorizirano«: v kategoriji se nahajajo vsi dokumenti. Vzrok je ta, da se dokument 1 ne more kategorizirati po ključnih besedah, dokumenti 2, 3 in 4 pa se ne morejo po atributu »sys:Category«.

Naziv entitete	Vrednosti ključnih besed (ločene z »,«)	Vrednosti atributa »sys:Category«
Dokument 1	/	CAT01
Dokument 2	K01	/
Dokument 3	K01, K01\01	/
Dokument 4	K01, K01\01	/

Tabela 14: Kategorizacija (primer 6)

### 3.4 Razvrščanje

Razvrščanje (klasifikacija) dokumentacije je bil nepogrešljiv pripomoček že pri klasičnem upravljanju, oziroma hrambi dokumentacije v papirni obliki.

Enako velja tudi za elektronsko upravljanje in elektronsko hrambo. Za potrebe razvrščanja je potrebno v strežniku IMiS®/ARChive Server predhodno vzpostaviti načrt razvrščanja dokumentarnega gradiva (klasifikacijski načrt), ki omogoča:

- Strukturiranje, razčlenjevanje in razvrščanje dokumentacije po vsebini, pristojnostih, dejavnostih ter poslovnih in strokovnih funkcijah.
- Določanje rokov hrambe dokumentarnega gradiva.
- Določanje arhivskega gradiva, oblike dokumentacije in strukture metapodatkov, ki so dodani zadevam in dokumentom, vključno z vodenjem evidence o fizičnem gradivu.

Strežnik omogoča vzpostavitev načrta razvrščanja gradiva poljubnih, praktično neomejenih dimenzij. Pri tem ne omejuje števila nivojev razredov, kakor tudi ne števila podrazredov posameznega razreda. Število nivojev razredov v posameznih delih arhiva je lahko različno. Načrt razvrščanja gradiva predstavlja osnovo za nadzor dostopa do posameznih delov arhiva in je v arhivu predstavljen s hierarhijo entitet vrsta razred.

### 3.4.1 Klasifikacijske oznake

Vsaka entiteta v arhivu ima svojo polno klasifikacijsko oznako, ki je unikatna za celoten arhiv. Dodeljena je ob nastanku entitete in je nespremenljiva, razen v primeru premika entitete v arhivu (reklasifikacija).

Polna klasifikacijska oznaka razreda je sestavljena iz polne klasifikacijske oznake nadrejenega razreda. Tej je dodan del oznake, ki je entiteti lasten in unikaten med vsemi entitetami, ki imajo isto nadrejeno entiteto. Opcijsko je lahko dodano tudi poljubno ločilo, ki je enotno za cel arhiv in ga določi administrator arhiva v nastavitvah strežnika (primer: ».«).

Polna klasifikacijska oznaka zadeve je sestavljena iz polne klasifikacijske oznake razreda kamor je uvrščena. Tej je dodana tudi unikatna oznaka zadeve znotraj tega razreda. Med obema komponentama lahko opcijsko nastopi ločilo, ki ga določi administrator arhiva in je lahko različno od ločila, ki nastopa med oznakami nivojev razreda. Tega določi administrator arhiva v nastavitvah strežnika (primer: »—«).

Polna klasifikacijska oznaka dokumenta je sestavljena iz polne klasifikacijske oznake zadeve ali razreda, ki ji/mu dokument pripada. Tej je dodana unikatna oznaka samega dokumenta znotraj nadrejene entitete. Pred to oznako lahko opcijsko nastopi tudi ločilo, ki ga določi administrator arhiva in je namenjeno ločevanju komponente dokumenta v polnih klasifikacijski oznakah. Tega določi administrator arhiva v nastavitvah strežnika (primer: »/«).

Strežnik IMiS®/ARChive Server samodejno določa klasifikacijske oznake ob dodajanju novih entitet vseh vrst. Za več informacij glej poglavje [Klasifikacijska oznaka](#).

Če samodejno določanje klasifikacijskih oznak za novo entiteto ni določeno (nastavitev posamične entitete za njene podrejene entitete), strežnik zavrne zahtevo za nastanek nove entitete. To stori v primeru, če zahtevku ni dodana vrednost klasifikacijske oznake, ali če podana klasifikacijska oznaka ni unikatna znotraj novi entiteti nadrejene entitete.

### 3.4.2 Nastavitve načrta razvrščanja gradiva

Podroben in praktično dokončen načrt razvrščanja gradiva mora biti praviloma določen ob uvodni konfiguraciji strežnika IMiS®/ARChive Server, oziroma pred začetkom njegove uporabe. Administrator v hierarhijo načrta razvrščanja gradiva doda vse potrebne razrede.

Za dodajanje razredov je potrebno predhodno:

- Ustvariti predloge za nove razrede. Za več informacij glej poglavje [Predloge](#).
- Nastaviti samodejno generiranje klasifikacijskih oznak (po potrebi).

Pred nastankom zadev in dokumentov je potrebno pripraviti:

- Predloge za zadeve v končnih razredih (razredi, ki nimajo vsebovanih razredov).
- Predloge za dokumente, ki bodo nastajali v zadevah ali neposredno v razredih.

S predlogami določimo:

- Metapodatke, ki so za posamezne entitete obvezni.
- Metapodatke, ki so dovoljeni za vnos.
- Metapodatke, kjer je za isto entiteto možno vnesti več vrednosti.
- Druge lastnosti entitet.

Vsaka predloga lahko določa, katere predloge je mogoče uporabiti za nastanek podrejenih entitet v entiteti, ki je nastala z uporabo te predloge. Dovoljene predloge za nastanek podrejenih entitet je mogoče določiti tudi neposredno na že obstoječih entitetah arhiva. Tako razredi, ki so na zadnjem nivoju razredov v arhivu navadno vsebujejo zadeve, izjemoma pa lahko vsebujejo tudi samostojne dokumente.

Kljub temu, da strežnik IMiS®/ARChive Server omogoča zamenjavo predloge enakega tipa in naknadno dodajanje atributov na obstoječe predloge, je natančna priprava načrta razvrščanja gradiva pred uporabo strežnika zelo pomembna.

Za več informacij o omejitvi dodajanja atributov na obstoječe predloge glej poglavje [Povezava s predlogami](#).

Po začetku uporabe strežnika, ko se v njem že nahajajo zadeve in/ali dokumenti pa so možne naslednje operacije, ki vplivajo na načrt razvrščanja gradiva:

- Nove razrede na kateri koli nivo je v arhiv mogoče dodajati kadarkoli.  
Novim razredom bodo klasifikacijske oznake dodeljene samodejno ali ročno, odvisno od nastavitvev samodejnega dodeljevanja klasifikacijskih oznak.
- Brisanje razredov je mogoče, ko razred ne vsebuje nobene entitete, torej v primeru, ko je popolnoma prazen.



- Dodajanje predlog, ki določajo metapodatke podrejenih entitet. Mogoče jih je dodajati na določeno mesto v hierarhiji.
- Premikanje entitet je mogoče skupaj s celotnim drevesom entitet, ki ga premikajoča se entiteta vsebuje. Za več informacij glej poglavje [Premikanje gradiva v načrtu razvrščanja \(reklasifikacije\)](#).

*Opozorilo:* Vse naštetje operacije so mogoče le, če uporabniku to dovoljujejo dostopne pravice. Tako je administratorjem dovoljeno upravljanje z dostopnimi pravicami kadarkoli po nastanku hierarhije razvrščanja.

Uporabnikom, ki jim dostopne pravice to omogočajo, je kadarkoli po nastanku razredov omogočeno tudi:

- Spreminjanje metapodatkov razredov.
- Zapiranje razredov, kar onemogoči:
  - dodajanje novih entitet v zaprt razred ali v hierarhijo pod njim;
  - spreminjanje vsebine arhiva kjerkoli v hierarhiji pod zaprtim razredom, vključno z metapodatki razreda samega.

### **3.4.3 Premikanje gradiva v načrtu razvrščanja (reklasifikacija)**

Kljub skrbnemu načrtovanju razvrščanja gradiva, prihaja v življenjski dobi elektronskega arhiva do potrebe po spremembah načrta razvrščanja gradiva.

Vse večkrat pa prihaja do potreb po spremembi klasifikacijske oznake določene zadeve ali dokumenta. V ta namen strežnik IMiS®/ARChive Server ponuja možnost premikanja entitete katerega koli tipa na drugo mesto znotraj arhiva.

Premikanje entitete, ki vsebuje hierarhijo drugih entitet, povzroči premik celotne hierarhije na drugo mesto.

Za uspešno premikanje entitete v arhivu morajo biti izpolnjeni naslednji pogoji:

- Uporabnik mora imeti pravico branja entitete, ki se premika.  
Za več informacij glej poglavje [Dostopne pravice za entiteto](#).
- Uporabnik mora imeti pravico premika entitete, ki se premika.  
Za več informacij glej poglavje [Dostopne pravice za entiteto](#).

- Uporabnik mora imeti pravico ustvarjanja novih entitet na mestu, kamor premika izbrano entiteto. Za več informacij glej poglavje [Dostopne pravice za entiteto](#).
- Predloga premikajoče se entitete mora ustrezati predlogam, ki so določene kot dovoljene na mestu, kamor uporabnik entiteto premika.
- Premikajoči se entiteti nadrejena entiteta ne sme biti zaprta.
- Hierarhija kamor premika entiteto ne sme biti zaprta.
- Omogočeno mora biti samodejno dodeljevanje klasifikacijskih oznak za vse entitete v hierarhiji pod premikajočo se entiteto.
- Stopnja tajnosti (angl. Security class) premikajoče se entitete mora biti manjša ali enaka stopnji tajnosti entitete, kamor uporabnik entiteto premika.

Ob uspešnem premeščanju entitete ali drevesa entitet, se na vseh premaknjenih entitetah izvede reklasifikacija glede na pravila opisana v poglavju [Klasifikacijska oznaka](#).

Krovni entiteti premaknjenih entitet so poleg tega dodani metapodatki:

- »sys:MoveReason«: razlog za premik entitete, ki ga obvezno posreduje uporabnik ob premiku.
- »sys:MoveAgent«: uporabnik, ki je premik izvedel.
- »sys:MoveDateTime«: datum in čas premika (konca).
- »sys:MoveClassificationCode«: polna klasifikacijska oznaka entitete pred premikom.

Za podrobnejši pomen naštetih metapodatkov glej poglavje [Sistemske atributi](#).

Za vse premaknjene entitete se v revizijsko sled zabeleži dogodek opisan v poglavju [Premik entitete](#).

V revizijsko sled se ob dogodku premika entitete in njej podrejenih entitet vnese še sporočilo ob premiku, ki vsebuje naslednje informacije:

- Trenutni status entitete.
- Stara in nova vrednost polne klasifikacijske oznake entitete.
- Razlog za premik, ki ga je ob premiku navedel uporabnik, ki je izvedel premik.
- Vrednosti vseh metapodatkov, ki jih je ob premiku entiteta vsebovala.

## 3.5 Iskanje

Ena najpomembnejših funkcionalnosti strežnika IMiS®/ARChive Server je zmožnost iskanja arhiviranega gradiva ter prikaz zadev in dokumentov glede na pravice dostopov.

Uporabnik lahko izvaja iskanje po naslednjih kriterijih:

- Iskanje po vrednostih posameznih atributov.
- Iskanje po polnem besedilu tako v atributih kot tudi shranjenih dokumentih.

Iskanje in indeksiranje po celotnem besedilu se izvaja v okviru ločenih iskalnikov (npr. Elasticsearch, Solr...), medtem ko se iskanje po vrednostih atributov lahko izvaja v ločenih iskalnikih, ali pa neposredno v bazi strežnika z vgrajenim IMiS®/ARChive Server iskalnikom.

Trenutno podprt ločen iskalnik na strežniku je Elasticsearch.

Iskanja lahko omejimo na naslednje načine:

- Omejitev glede na število entitet: če je v rezultatu iskanja 500 entitet in je omejitev nastavljena na 200, bo končni rezultat iskanja prvih 200 entitet.
- Omejitev iskanja entitet glede na nivo: z omejitvijo nivoja omejimo iskanje entitet, ki se nahajajo globlje v poddrevesu, kot pa ga predstavlja nivo. Za primer vzemimo iskanje po celotnem arhivu, z omejitvijo na nivo »1«. V rezultatu iskanja bodo samo entitete, ki se nahajajo neposredno pod arhivom. Če bi omejili nivo na »2«, potem bi v rezultatu iskanja nahajale entitete neposredno pod arhivom ter njihove podrejene entitete na prvem nivoju.

### 3.5.1 Varnost in zaščita podatkov pri iskanju

Rezultati iskanja so lahko samo razredi, zadeve ali dokumenti do katerih ima uporabnik pravico dostopa, bodisi iz naslova stopnje tajnosti, bodisi kot seznamov dostopnih pravic (ACL). Entitete, do katerih uporabnik nima pravice dostopov, ostanejo uporabniku zakrite, čeprav ustrezajo iskalnim pogojem.

Ostale pravice za operacije nad entitetami, ki so rezultat iskanja, so enake pravicam pri običajnem pregledovanju arhiva.

*Primer:* Če uporabnik nima pravice za odpiranje entitete v bralskem načinu, bo v rezultatih iskanja videl samo njen obstoj in njene javne metapodatke.

### 3.5.2 Pravila iskalnega niza

Enostaven pogoj je osnovni del iskalnih nizov. Strežnik IMiS®/ARChive Server pozna dve vrsti enostavnih pogojev:

- Pogoji za iskanje po metapodatkih.
- Pogoji za iskanje po celotnem besedilu dokumentov.

Iskalni niz je sestavljen iz najmanj enega enostavnega pogoja.

Zahtevnejši iskalni nizi so sestavljeni iz več enostavnih pogojev, ki so v nizu združeni z logičnimi operacijami (IN, ALI, izključujoči ALI in negacija).

Zaporedje računanja logičnih operacij lahko dodatno določimo z uporabo oklepajev.

Osnova za iskanje bodisi z vgrajenim iskalnikom ali ločenim iskalnikom je sintaksa strežnika IMiS®/ARChive Server. Ta se nato neposredno izvede v vgrajenem iskalniku, če se ga uporablja kot osnovo za iskanje. V primeru, da se uporablja ločeni iskalnik Elasticsearch, se sintaksa najprej pretvori v ekvivalentno Elasticsearch sintakso, ki se pošlje v izvajanje ločenem iskalniku.

#### 3.5.2.1 Enostavni pogoji za iskanje po metapodatkih

Strežnik IMiS®/ARChive Server omogoča iskanje po vseh metapodatkih, za katere je glede na nastavitve sistema omogočeno iskanje. Iskanje je na voljo za metapodatke vseh tipov.

Enostaven pogoj za iskanje po metapodatkih sestavljajo tri komponente:

- Ime metapodatka za katerega velja pogoj. V pogoju je ime metapodatka vedno navedeno v oglatih oklepajih. Primer: {Znesek}.
- Operacija primerjanja. Poznane operacije za primerjanje v enostavnih pogojih so: manjše (<), manjše ali enako (<=), enako (= ali ==), različno (<> ali !=), večje ali enako (>=) in večje (>).
- Vrednost za katero velja operacija primerjanja. Vse vrednosti so lahko navedene v dvojnih narekovajih. Če vrednost vsebuje preslednice, je uporaba dvojnih narekovajev obvezna (npr. »Spodnja Kungota«).

Znak za ločevanje celega dela od decimalk v decimalnih vrednostih je pika. Datumske in časovne vrednosti morajo biti navedene v XML notaciji. Pri datumskih in časovnih vrednostih lahko uporabimo štiri posebne izraze, ki nadomestijo celotno vrednost ali enega od njenih delov.

*@NOW@* cela vrednost bo sestavljena iz trenutnega datuma in časa

*Primer: [ZacetekSeje] < @NOW@*

*@TODAY@* datum v vrednosti bo enak današnjemu datumu

*Primer: [CasPrejema] < @TODAY@T08:00+02:00*

*@YEAR@* leto v vrednosti bo enako trenutnemu letu

*@MONTH@* mesec v vrednosti bo enak trenutnemu mesecu

*Primer: [CasFotografije] < @YEAR@@MONTH@-15T20:00+02:00*

Posebna vrednost za pogoje iskanja je izraz NULL. To vrednost je mogoče uporabiti za pogojevanje obstoja vrednosti določenega metapodatka.

Pri uporabi vrednosti NULL in pri metapodatkih logičnega tipa je možna samo uporaba primerjalnih operatorjev enako (== ali =) in različno (<> ali !=).

- Opcijsko lahko za imenom metapodatka navedemo aritmetično operacijo seštevanja ali odštevanja (+ ali -), katere drugi operand je konstantna vrednost.

Pri znakovnih in logičnih metapodatkih ta opcija ni na voljo.

Za datumske metapodatke je predpisana posebna oblika konstantne vrednosti, sestavljena iz najmanj ene ali vseh treh komponent, ki predstavljajo leta, mesece in dneve. Posamezne komponente so sestavljene iz celega števila in črke, ki predstavlja datumsko enoto kot izhaja iz naslednjih primerov:

- za leta uporabimo črko y ali Y (npr. 15y)
- za mesece m ali M (npr. 3m)
- za dneve d ali D (npr. 60d).

*Primeri: enostavni pogoji za iskanje po metapodatkih:*

*[Znesek] - 40.5 >= 250*

*[Avtor]="Janez Novak"*

*[ZacetekSeje] + 1y3m <= 2014-05-07T11:05+02:00*

*[KonecSeje] + 7d <= @NOW@*

*[Avtor]!=NULL*

### 3.5.2.2 Enostavni pogoji za iskanje po polnem besedilu dokumentov

Strežnik IMiS®/ARChive Server omogoča iskanje po celotnem besedilu dokumentov, za katere je glede na nastavitve strežnika omogočeno iskanje. Možnost iskanja je na voljo za datoteke vseh razširjenih tipov, katerih vsebina je lahko besedilo.

Enostavni pogoji za iskanje po celotnem besedilu dokumentov so v iskalnih nizih navedeni v zavutih oklepajih: {"Janez Novak"}.

Znotraj zavutih oklepajev sledi sintaksa za iskanje po celotnem besedilu, in je odvisna od uporabe zunanega iskalnika. V primeru Elasticsearcha gre za t.i »Simple query string query« sintakso, ki je podrobneje razložena na spletni strani produkta (<https://www.elastic.co/guide/en/elasticsearch/reference/8.0/query-dsl-simple-query-string-query.html>).

V osnovi gre za sestavljanje enostavnih iskalnih pogojev s pomočjo logičnih operacij. Dodatno omogoča tudi naprednejše iskanje z iskanjem približnih rezultatov, v kolikor nastavitve Elasticsearch iskalnika to dovoljujejo.

V nadaljevanju so prikazani primeri iskanja po celotnem besedilu z uporabo Elasticsearch sintakse.

*Primer: {log4j + report}*

*Rezultat so vsa besedila, ki vsebujejo besedi »log4j« in »report«.*

*Primer: {(log4j + report) + -customer}*

*Rezultat so vsa besedila, ki vsebujejo besedi »log4j« in »report«, vendar ne vsebuje besede »customer«.*

*Primer: {google~2}*

*Rezultat so vsa besedila, ki ustrezajo besedi »google« in vsa besedila, ki vsebujejo besedo, ki se od besede »google« razlikuje v dveh črkah, kot na primer »gppgle« ali »toople«.*

### 3.5.2.3 Logične operacije v iskalnih nizih

Enostavni pogoji so v kompleksnejše iskalne nize povezani z logičnimi operacijami.

Strežnik IMiS®/ARChive Server podpira naslednje logične operacije, ki so navedene po vrstnem redu izračunavanja:

- negacija: NOT ali !
- in: AND ali &
- izključujoči ali: XOR ali ^
- ali: OR ali |.

*Primer:* Izraz:  $[A]>3 \text{ OR } [A]=3 \text{ AND } [B]!=\text{NULL}$

je enakovreden izrazu:  $\text{NOT } [B]==\text{NULL} \ \& \ [A]==3 \ | \ [A]>3$

V obeh primerih se najprej izračuna operacija »in«, nato pa še operacija »ali«.

V drugem primeru se pred »IN« izračuna še negacija »NOT«.

Z uporabo navadnih oklepajev je mogoče spremeniti privzeti vrstni red izračuna logičnih operacij. Zgornji iskalni izraz lahko z uporabo oklepajev postane povsem nekaj drugega in posledično bo rezultat iskanja popolnoma drugačen.

*Primer:* Uporaba oklepajev povzroči, da se operacija »AL« izračuna pred operacijo »IN«:  $[A]>3 \text{ OR } [A]=3 \text{ AND } [B]!=\text{NULL}$

V istem iskalnem nizu je možna hkratna uporaba obeh tipov enostavnih pogojev.

*Primer:* Izraz:  $[Povrsina] \geq 12 \text{ AND } \{ "Janez \text{ AND } Novak" \}$

je povsem pravilen.

Priporočljivo je, da se pogoji za iskanje po polnem besedilu združijo v en izraz znotraj zavitih oklepajev, če je to le mogoče.

*Primer:* Izraz:  $[Povrsina] \geq 12 \text{ AND } \{ "Janez" \} \text{ AND } \{ "Novak" \}$

bo na primer vrnil enake rezultate kot izraz:

$[Povrsina] \geq 12 \text{ and } \{ "Janez" \} \text{ AND } \{ "Novak" \}$

Drugi izraz bo iskanje izvedel nekoliko hitreje kot prvi.

## 3.6 Avtentičnost

### 3.6.1 Predpogoji

Skrozi življenjski cikel entitet se lahko spreminjajo njeni metapodatki in vsebina.

Predpogoj za zagotavljanje avtentičnosti entitet je njihova nespremenljivost.

Strežnik IMiS®/ARChive Server za matematično preverjanje nespremenljivosti uporablja priporočila delovne skupine LTANS (angl. Long-Term Archive and Notary Services), ki predpisujejo »de-facto« standarde postopkov dolgoročnega arhiviranja vsebin.

V postopek se vključujejo entitete po pravilih, ki so opisana v nadaljevanju.

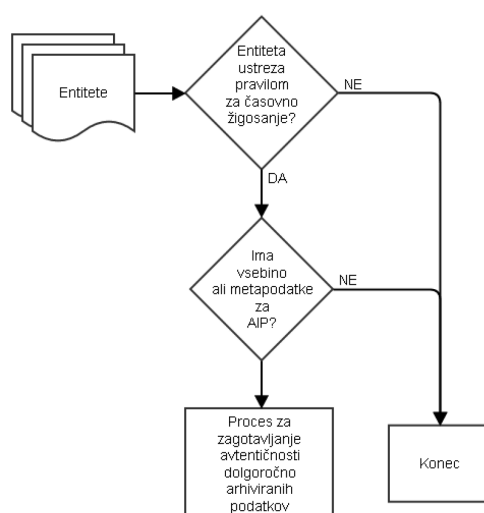
Za več informacij glej poglavje [Pravila](#). Priporočljivo je, da so pravila napisana tako, da se v postopek avtentičnosti vključujejo samo entitete, ki so nespremenljive (npr. zaprte entitete). Ker se lahko vsebina entitet tudi kasneje spreminja, se vedno znova ustvarjajo tudi dokazila za tako entiteto.

Kot dodatno mora imeti entiteta vsaj en metapodatek, ki označuje, da je predmet arhivskega informacijskega paketa (angl. Archival Information Package – AIP).

AIP je XML reprezentacija vsebine entitete in njenih metapodatkov in je podrobneje opisan v nadaljevanju.

Avtentičnost AIP in posledično entitete dokazuje pripadajoča sintaksa evidenčnih podatkov (ERS), ki se ustvari v postopku zagotavljanja avtentičnosti dolgoročno arhiviranih podatkov.

Spodnja slika prikazuje postopek umeščanja entitet, ki ustrezajo predpogojem v postopku za zagotavljanje avtentičnosti dolgoročno arhiviranih podatkov.



Slika 7: Umeščanje entitete v postopku za zagotavljanje avtentičnosti dolgoročno arhiviranih podatkov



### 3.6.2 Koncept

Eden izmed ključnih konceptov zagotavljanja varnega elektronskega arhiva je zagotavljanje avtentičnosti arhiviranega gradiva skozi ves čas njegove hrambe.

To pomeni, da je potrebno ohraniti izvirne lastnosti dokumenta glede na kontekst, strukturo in njegovo vsebino. Bistveno je, da se od trenutka arhiviranja dokumenta vsi njegovi deli (struktura, vsebina, metapodatki, ...) potrebni za zagotovitev avtentičnosti, ne spremenijo več.

Avtentičnost elektronsko arhiviranega gradiva lahko zagotovimo z uporabo naslednjih funkcionalnosti:

- Prstni odtis (angl. Hash - #).
- Elektronski podpis z digitalnim potrdilom (angl. Digital signature).
- Časovni žig (angl. Timestamp).

#### 3.6.2.1 Prstni odtis

Prstni odtis je rezultat enosmerne zgoščevalne funkcije, ki za vhodni podatek vzame blok podatkov (npr. niz zlogov binarne vsebine dokumenta, izvorno besedilo dokumenta) in izračuna prstni odtis fiksne dolžine. Minimalna sprememba vhodnih podatkov se odraža v veliki spremembi vrednosti prstnega odtisa.

Lastnosti idealne zgoščevalne funkcije so naslednje:

- Za vsak vhodni blok podatkov je preprosto izračunati prstni odtis.
- Iz prstnega odtisa je nemogoče ugotoviti vhodni blok podatkov (zgoščevalna funkcija je enosmerna).
- Nemogoče je spremeniti vhodni blok podatkov na tak način, da bo prstni odtis nespremenjen.
- Teoretično je nemogoče, da bi prišlo do sovpadanja zgoščenih vrednosti različnih vhodnih blokov (angl. Collision).

Z razvojem tehnologije in večanjem računalniške moči, se veča tudi možnost sovpadanja zgoščenih vrednosti različnih vhodnih blokov, kar oslabi varnost zgoščevalne funkcije.

Tako danes velja MD5 zgoščevalna funkcija za zlomljivo in ni več varna za uporabo.



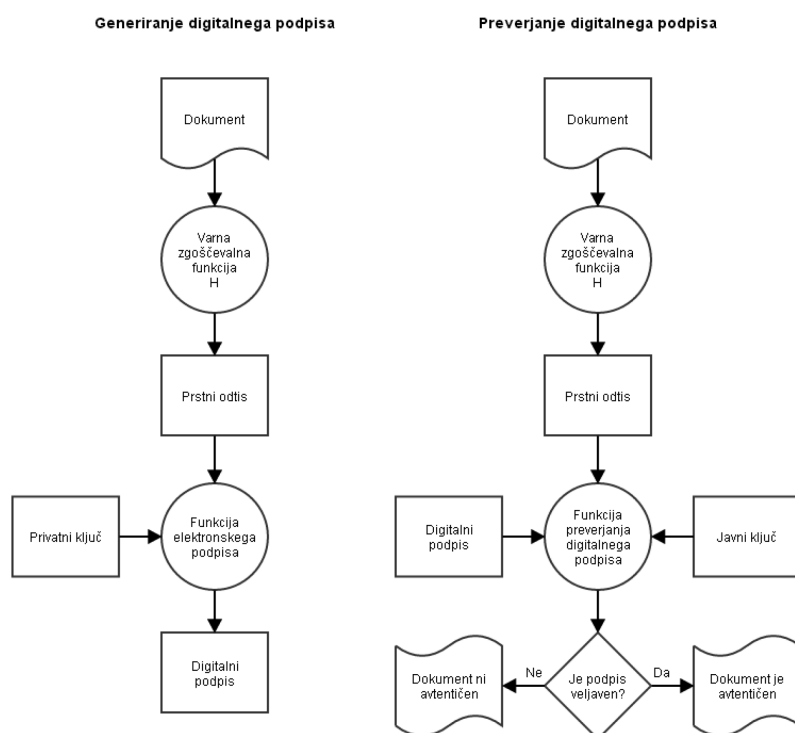
Slika 8: Delovanje zgoščevalne funkcije

### 3.6.2.2 Elektronski podpis z digitalnim potrdilom

Elektronski podpis temelji na infrastrukturi javnih ključev (angl. Public Key Infrastructure – PKI) in matematično zagotavlja avtentičnost elektronskega dokumenta.

Shema elektronskega podpisa temelji na treh algoritmih:

- Ustvarjanje ključev: ustvarita se privatni in javni ključ, ki sta ključna za izdelavo in preverjanje podpisa.
- Algoritem za podpisovanje: na podlagi privatnega ključa ter dokumenta se ustvari elektronski podpis.
- Algoritem za preverjanje podpisa: na podlagi elektronskega podpisa in javnega ključa se preveri avtentičnost dokumenta.



Slika 9: Generiranje in preverjanje elektronskega podpisa

Veljavnost elektronskega podpisa je pogojena z veljavnostjo digitalnega potrdila.

Glede na 32. člen Uredbe za elektronsko poslovanje in elektronsko podpisovanje omejeno na največ 5 let. Za ohranjanje avtentičnosti dokumenta je potrebno dokument podpisati z novim digitalnim potrdilom pred iztekom veljavnosti starega.

### 3.6.2.3 Časovni žig

Postopek časovnega žigosanja je ekvivalenten elektronskemu podpisovanju, le da je vključen tudi izdajatelj varnih časovnih žigov (angl. Time Stamping Authority – TSA).

Slednji elektronskemu podpisu doda časovno komponento, ki enolično določa čas elektronskega podpisa dokumenta. Enako, kot pri elektronskemu podpisu, je tudi veljavnost časovnega žiga omejena z veljavnostjo digitalnega potrdila,

ki ga je potrebno za zagotavljanje avtentičnosti dokumenta podaljševati.

Časovni žig se uporablja za podaljševanje veljavnosti elektronskih podpisov.

Gre za praktično rešitev zlasti v primeru, ko je vsebino podpisalo več oseb, ki jim bo poteklo digitalno potrdilo. Brez časovnega žiga bi morali za zagotovitev avtentičnosti vsebine vsi podpisniki, ki jim je digitalno potrdilo preteklo še enkrat elektronsko podpisati vsebino.

Na ta način časovni žig zagotavlja avtentičnost vsebine tudi, ko so digitalna potrdila podpisnikov že pretečena.

Vsi zgoraj našteti načini (prstni odtis, elektronski podpis z digitalnim potrdilom, časovni žig) imajo pomanjkljivosti, tako tehnološke (prstni odtis) kakor tudi časovne (veljavnost digitalnega potrdila). Zato uporaba posameznega načina ni primerna za zagotavljanje dolgoročne avtentičnosti dokumenta.

Tako obstaja kar nekaj standardov, ki za dolgoročno zagotavljanje avtentičnosti dokumentov uporabljajo kombinacijo prstnih odtisov, elektronskih podpisov in časovnih žigov:

- Standardi ETSI.
- Sintaksa evidenčnih podatkov (angl. Evidence Record Syntax – ERS).
- Okolje revidiranega nadzora (angl. Auditing Control Environment – ACE).
- Servis celovitosti vsebine (angl. Content Integrity Service – CIS).

Strežnik IMiS®/ARChive Server za dolgoročno zagotavljanje avtentičnosti dokumentov uporablja ERS standard v njegovi XML obliki (XMLERS, RFC 6283) opisan v nadaljevanju.

### 3.6.3 Shramba digitalnih potrdil

Za delo z digitalnimi potrdili (certifikati) uporablja strežnik IMiS®/ARChive Server shrambo digitalnih potrdil (angl. Certificate Store). Temelji na odprtokodni knjižnici OpenSSL.

Shramba digitalnih potrdil omogoča:

- Dodajanje digitalnih potrdil.
- Omogočanje in onemogočanje digitalnih potrdil.
- Iskanje digitalnih potrdil.
- Iskanje po seznamih preklicanih digitalnih potrdil.

Za hitrejše pridobivanje digitalnih potrdil in aktualnih informacij o preklicih je v shrambi izvedeno predpomnenje (angl. Caching) trenutno uporabljenih verig digitalnih potrdil (angl. Certificate chain) in informacij o preklicih.

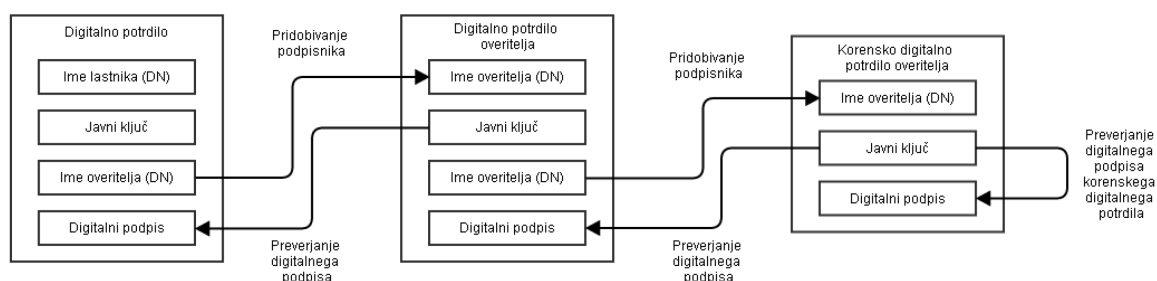
#### 3.6.3.1 Veriga digitalnih potrdil

Veriga digitalnih potrdil je seznam digitalnih potrdil, ki dokazujejo avtentičnost posameznega digitalnega potrdila. Vsako digitalno potrdilo v seznamu je podpisano s privatnim ključem naslednjega digitalnega potrdila v tem seznamu.

Na koncu seznama je korensko digitalno potrdilo overitelja (angl. Certificate authority root certificate), ki je samo sebi podpisnik (angl. Self-signed certificate).

Tako verigo imenujemo veriga zaupanja (angl. Chain of trust) in zagotavlja avtentičnost vseh digitalnih potrdil v njej.

Spodnja slika prikazuje primer verige s tremi digitalnimi potrdili ter postopek preverjanja posameznih digitalnih potrdil.



Slika 10: Veriga digitalnih potrdil

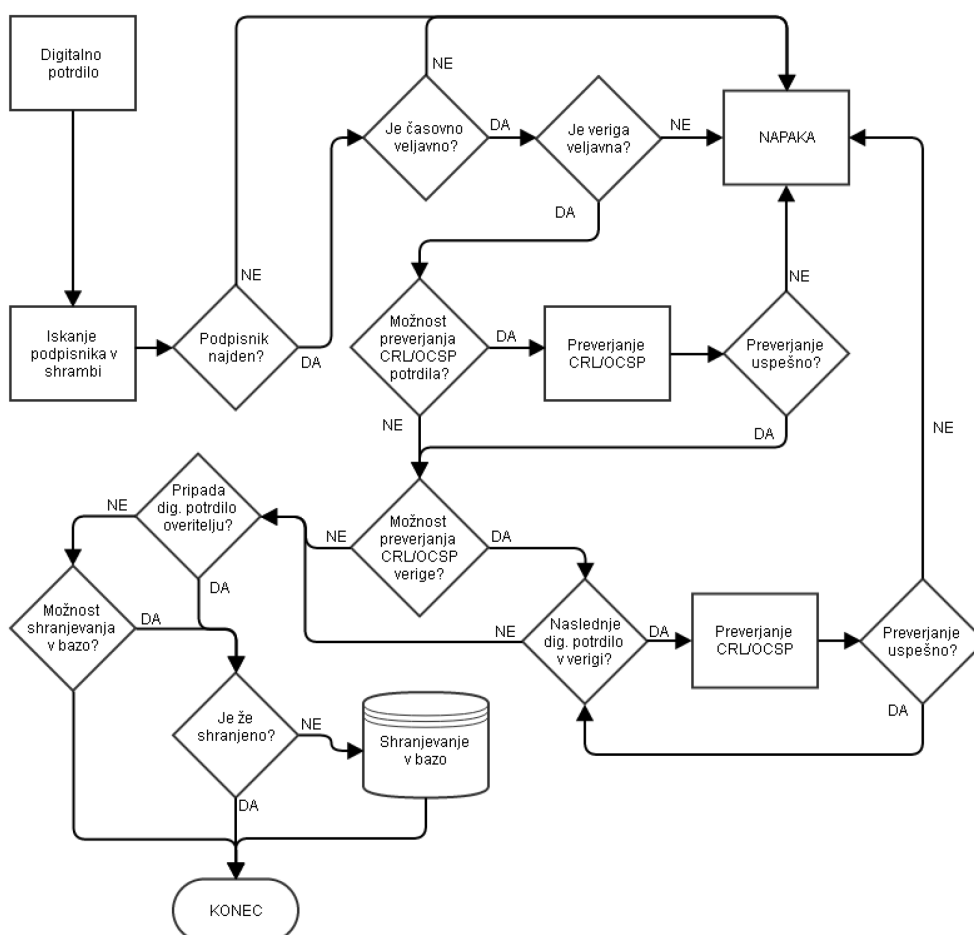
### 3.6.3.2 Dodajanje digitalnih potrdil

Dodajanje digitalnih potrdil v shrambo je uspešno, če so zadoščeni naslednji pogoji:

- Digitalno potrdilo mora biti veljavno v času dodajanja v shrambo (ne sme biti pretečeno).
- Shramba mora vsebovati vsa predhodna digitalna potrdila, ki tvorijo verigo zaupanja.
- Vsa predhodna digitalna potrdila morajo biti omogočena.
- V primeru, da želimo pri dodajanju digitalnega potrdila preveriti informacije o preklicu le tega ali informacije o preklicih vseh digitalnih potrdil, je dodajanje uspešno le v primeru preverjanja digitalnih potrdil, da le-ta niso preklicana.

Obvezna pogoja za dodajanje digitalnega potrdila v shrambo sta:

- Digitalno potrdilo je bilo veljavno v času dodajanja.
- V shrambi so že predhodna digitalna potrdila (in so omogočena), ki tvorijo verigo zaupanja.



Slika 11: Postopek dodajanja digitalnega potrdila v shrambo

### 3.6.3.3 Omogočanje in onemogočanje digitalnih potrdil

Z omogočanjem in onemogočanjem digitalnih potrdil nadziramo, katerim digitalnim potrdilom zaupamo in katerim ne. Z onemogočanjem posameznih digitalnih potrdil avtomatsko onemogočimo celotno vejo, katero sestavlja onemogočeno digitalno potrdilo. Če se v veji nahaja onemogočen certifikat, potem je taka veja neveljavna oziroma se tak certifikat v veji ne upošteva.

### 3.6.3.4 Iskanje digitalnih potrdil

Digitalna potrdila lahko iščemo po shrampi po njegovem prstnem odtisu (uporablja se zgoščevalni algoritem SHA-512) ali po njegovem 32-bitnem unikatnem identifikatorju, ki ga dobi ob shranjevanju v podatkovno bazo. Digitalna potrdila, ki niso shranjena v bazi, tega identifikatorja nimajo.

### 3.6.3.5 Iskanje informacij o preklicih

Iskanje informacij o preklicih je možno le po 64-bitnem unikatnem identifikatorju, ki ga strežnik dodeli v primeru shranjevanja v bazo. Shranjevanje informacij o preklicih se izvaja pri preverjanju časovnega žiga v postopku zagotavljanja avtentičnosti dolgoročno arhiviranih podatkov. Za več informacij glej poglavja [ERS](#) in [Časovno žigosanje](#).

Vsako digitalno potrdilo ima t.i. podaljške (angl. Certificate extensions), ki so podrobneje opisani v specifikaciji RFC 5280 (<http://tools.ietf.org/html/rfc5280>).

Podaljški vsebujejo informacije o distribucijskih točkah, kjer se dobijo informacije o:

- Preklicih digitalnega potrdila.
- Informacije o tipu digitalnega potrdila.
- Informacije o namenski uporabi digitalnega potrdila.
- ...

Strežnik pri obdelavi digitalnih potrdil, poleg informacij o distribucijskih točkah, uporablja še podaljške imenovane osnovne omejitve (angl. Basic constraint) in razširjena uporaba ključa (angl. Extended key usage).

### 3.6.3.6 Osnovne omejitve

Podaljšek vsebuje informacije o tem, ali digitalno potrdilo pripada overitelju ali ne. Informacija se zapiše v parameter »mCACertificate« digitalnega potrdila in ima lahko vrednosti »1« ali »0«.

Vrednost »1« pomeni, da digitalno potrdilo pripada overitelju, »0« pa pomeni da ne.

### 3.6.3.7 Razširjena uporaba ključa

Podaljšek vsebuje parametre z informacijami o namenu uporabe digitalnega potrdila.

Parameter: »mServerAuthentication«

Veljavne vrednosti: »1« ali »0«

Opis: Če ima vrednost »1«, potem se digitalno potrdilo lahko uporablja za overjanje strežnika pri vzpostavljanju šifrirane povezave med strežnikom in odjemalcem.

Parameter: »mClientAuthentication«

Veljavne vrednosti: »1« ali »0«

Opis: Če ima vrednost »1«, potem se digitalno potrdilo lahko uporablja za overjanje odjemalca pri vzpostavljanju šifrirane povezave med strežnikom in odjemalcem.

Parameter: »mEmailProtection«

Veljavne vrednosti: »1« ali »0«

Opis: Če ima vrednost »1«, potem se digitalno potrdilo lahko uporablja za podpisovanje elektronske pošte.

Parameter: »mCodeSigning«

Veljavne vrednosti: »1« ali »0«

Opis: Če ima vrednost »1«, potem se digitalno potrdilo lahko uporablja za podpisovanje izvršljive kode (angl. Executable code).

Parameter: »mMicrosoftServerGatedCrypto«

Veljavne vrednosti: »1« ali »0«

Opis: Parameter se ne uporablja

Parameter: »mNetscapeServerGatedCrypto«

Veljavne vrednosti: »1« ali »0«

Opis: Parameter se ne uporablja

Parameter: »mOcspSign«

Veljavne vrednosti: »1« ali »0«

Opis: Če ima vrednost »1«, potem se digitalno potrdilo lahko uporablja za podpisovanje OCSP odgovora strežnika, ki posreduje informacije o preklicih digitalnih potrdil.

Parameter: »mTimestamp«

Veljavne vrednosti: »1« ali »0«

Opis: Če ima vrednost »1«, potem se digitalno potrdilo lahko uporablja za časovno žigosanje.

Parameter: »mDvcs«

Veljavne vrednosti: »1« ali »0«

Opis: Če ima vrednost »1«, potem se digitalno potrdilo lahko uporablja za podpisovanje komponent v DVCS protokolu (protokol opisuje specifikacija RFC 3029 - <http://tools.ietf.org/html/rfc3029>).

### 3.6.3.8 Kriptografska razširitev

S kriptografsko razširitvijo JCA (angl. Java Cryptography Extension) je omogočena uporaba shrambe digitalnih potrdil tudi v vtičnikih (vtičniki za imeniške storitve, vtičniki za časovno žigosanje, ...). S tem je omogočena enotna uporaba shrambe digitalnih potrdil v vseh komponentah strežnika IMiS®/ARChive Server. Shrambo digitalnega potrdila v vtičnikih omogočimo tako, da v konfiguracijo vtičnika dodamo rezervirano besedo »IAKS«, ki predstavlja shrambo digitalnega potrdila. Naslednji zapis predstavlja konfiguracijo vtičnika, ki uporablja strežniško shrambo digitalnih potrdil za varno povezovanje na LDAP strežnik.

*<Arguments>*

*<Class>com.imis.imisarc.server.aaa.impl.ActiveDirectory</Class>*

*<LdapURL>ldaps://pot.do.streznika</LdapURL>*

*...*

*<SSLTSType>IAKS</SSLTSType>*

*...*

*</Arguments>*



### 3.6.4 ERS

Sintaksa evidenčnih podatkov (angl. Evidence Record Syntax - ERS) je standard, ki opisuje sistem za zagotavljanje avtentičnosti dolgoročno arhiviranega gradiva.

Predpisuje kako naj se dokazila ustvarjajo, podaljšujejo in kako naj bodo strukturirana, da bodo nedvoumno dokazovala avtentičnost arhiviranega gradiva od trenutka, ko je to vstopilo v postopek dolgoročnega zagotavljanja avtentičnosti.

V strežniku IMiS®/ARChive Server je izveden ERS v XML formatu po specifikaciji RFC 6283 (<https://tools.ietf.org/html/rfc6283>).

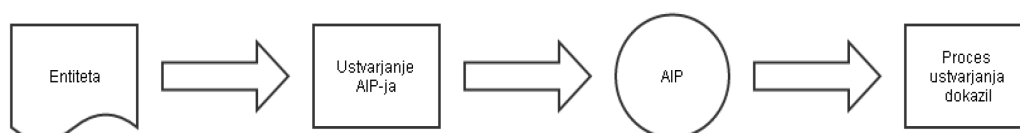
Ključna postopka za dolgoročno zagotavljanje avtentičnosti arhiviranega gradiva sta:

- Ustvarjanje dokazil.
- Podaljševanje dokazil.

Pred pričetkom postopka ustvarjanja dokazil je potrebno najprej izbrati vsebino in metapodatke, ki jih bo sintaksa evidenčnih podatkov ščitila, oziroma dokazovala, da so le-ti avtentični.

To se naredi z ustvarjanjem arhivskega informacijskega paketa (AIP) za vsako entiteto, ki ustreza predpogojem za zagotavljanje avtentičnosti dolgoročno shranjenih podatkov.

Za več informacij glej poglavje [Predpogoji](#).



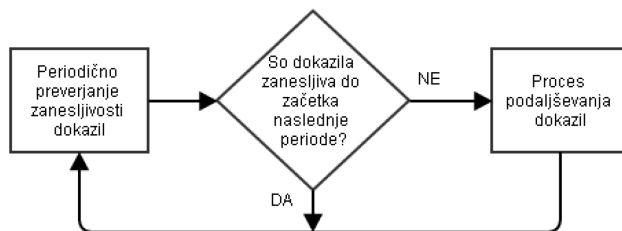
Slika 12: Ustvarjanje AIP za postopek ustvarjanja dokazil

Dokazila za dokazovanje avtentičnosti (prstni odtis, elektronski podpis, časovni žig) imajo omejeno življenjsko dobo. Veljavnost elektronskega podpisa in časovnega žiga sta omejena s časovno veljavnostjo digitalnega potrdila, ki ju je ustvaril.

Zato je potrebno dokazila podaljševati in sicer z generiranjem novega elektronskega podpisa ali časovnega žiga. To imenujemo tudi postopek enostavnega podaljševanja dokazil.

S časom se varnost algoritma za ustvarjanje prstnega odtisa zmanjša, saj se poveča verjetnost sovpadanja zgoščenih vrednosti. Zato je potrebno algoritem nadomestiti z novejšim. S tem zagotovimo, da dokazila ne izgubijo zanesljivosti, kljub slabljenju matematičnih algoritmov, ki jih ustvarjajo. To imenujemo tudi postopek kompleksnega podaljševanja dokazil.

Ustvarjena dokazila je potrebno periodično preverjati ter jih pred izgubo zanesljivosti podaljšati, kot je prikazano na spodnji sliki.

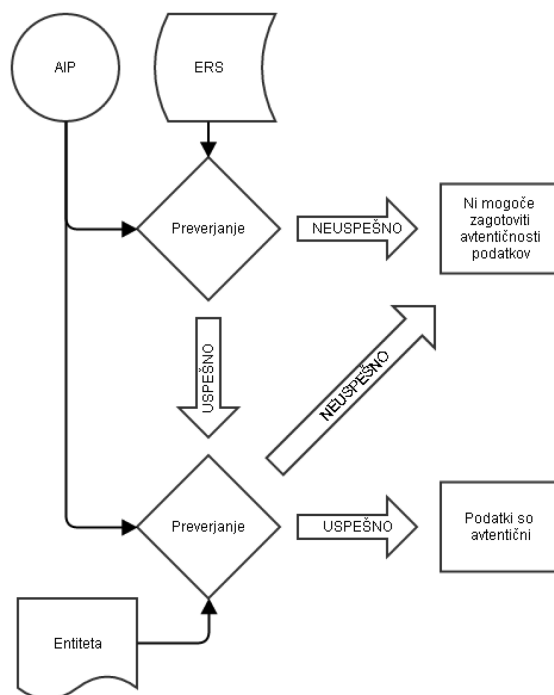


Slika 13: Podaljševanje zanesljivosti dokazil

Preverjanje avtentičnosti arhiviranega gradiva poteka v dveh stopnjah:

- Preverjanje AIP s podatki v ERS.
- Preverjanje vsebine in metapodatkov entitete z vrednostmi v AIP.

Če sta obe preverjanji uspešni pomeni, da so vsebina entitete in metapodatki ostali nespremenjeni skozi ves čas hrambe. Če je katerokoli od preverjanj neuspešno pomeni, da ni zagotovila, da so podatki avtentični.



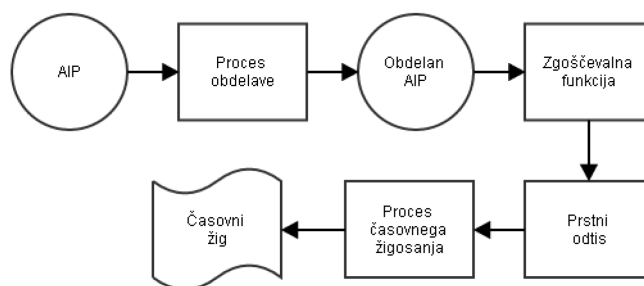
Slika 14: Primer preverjanja avtentičnosti podatkov

### 3.6.4.1 Postopek ustvarjanja dokazil

Za vsako entiteto, ki pride v postopek zagotavljanja avtentičnosti dolgoročno arhiviranih podatkov se ustvari arhivski informacijski paket (AIP). Tak paket strežnik IMiS®/ARChive Server obdela glede na informacije, ki se nahajajo v glavi paketa. Za več informacij glej poglavje [AIP](#).

Za obdelan paket se nato izračuna prstni odtis, ki je osnova za časovno žigosanje.

Časovni žig nam nedvoumno dokazuje, da je prstni odtis (ter posledično AIP, kateremu pripada) obstajal pred časom, navedenem v časovnem žigu.



Slika 15: Postopek časovnega žigosanja posameznega AIP-ja

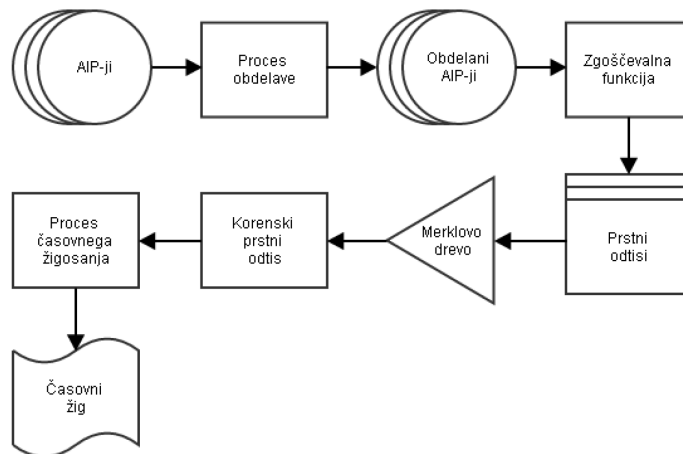
Ker je postopek časovnega žigosanja časovno precej zahteven, istočasno pa večina ponudnikov časovnega žigosanja svojo storitev zaračunava, je žigosanje posameznih prstnih odtisov neracionalno.

Zato se večinoma uporablja paketno časovno žigosanje, ki se izvaja v naslednjih korakih:

- Za vse entitete, za katere je potrebno ustvariti dokazila o verodostojnosti se ustvarijo AIP.
- Vse ustvarjene AIP strežnik IMiS®/ARChive Server obdela, ter se za njih ustvari prstne odtise.
- Iz izračunanih prstnih odtisov se zgradi drevo prstnih odtisov (angl. Hash tree) – za časovno žigosanje strežnik uporablja Merklovo drevo (angl. Merkle tree). Za več informacij glej poglavje [Merklovo drevo](#).
- Iz Merklovega drevesa se izračuna korenski prstni odtis, ki ščiti celotno drevo prstnih odtisov.
- Korenski prstni odtis se časovno žigosa, tako se ustvari dokazilo o obstoju vseh prstnih odtisov (ter pripadajočih AIP) v Merklovem drevesu pred časom, navedenim v časovnem žigu.

Z uporabo Merklovega drevesa lahko paketno žigosamo večje število entitet.

S tem racionaliziramo postopek ustvarjanja dokazil. Ko so dokazila enkrat ustvarjena, je potrebno poskrbeti za njihovo zanesljivost s podaljšanjem le-teh.



Slika 16: Postopek časovnega žigosanja z uporabo Merklovega drevesa

### 3.6.4.2 Postopek podaljševanja dokazil

Vsa ustvarjena dokazila je potrebno pred izgubo zanesljivosti podaljšati, saj drugače ne morejo zagotavljati avtentičnosti dolgoročno arhiviranih podatkov.

Podaljševanje dokazil lahko ločimo na dva načina:

- Enostavno podaljševanje.
- Kompleksno podaljševanje.

#### 3.6.4.2.1 Enostavno podaljševanje

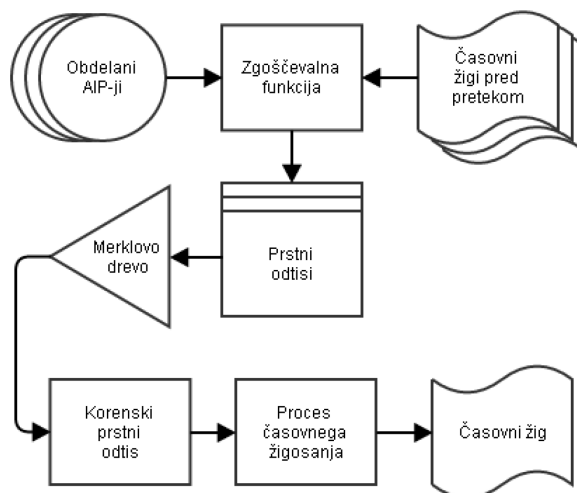
Enostavno podaljševanje se izvede v primeru, ko je digitalno potrdilo, ki je ustvarilo časovni žig pred iztekom. Tak časovni žig enostavno podaljšamo tako, da iz njega izračunamo prstni odtis ter ga časovno žigosamo. Tako nov časovni žig podaljša zanesljivost starega kljub temu, da bodisi digitalno potrdilo starega časovnega žiga preteče. Temu pravimo veriga časovnih žigov (angl. Timestamp chain).

Zaradi neracionalnosti podaljševanja posameznih časovnih žigov, se večinoma za podaljševanje uporablja Merklovo drevo po enakem postopku kot pri paketni obdelavi AIP.

Postopek enostavnega podaljševanja združimo s postopkom ustvarjanja dokazil.

Uporabimo Merklovo drevo, ki mu skozi postopek zgoščevanja dodamo prstne odtise AIP in časovne žige pred potekom veljavnosti.

S časovnim žigovanjem korenskega prstnega odtisa Merklovega drevesa tako ustvarimo dokazilo za obstoj AIP ter hkrati podaljšamo veljavnost časovnih žigov pred pretekom.



Slika 17: Postopek enostavnega podaljševanja v kombinaciji z ustvarjanjem dokazil

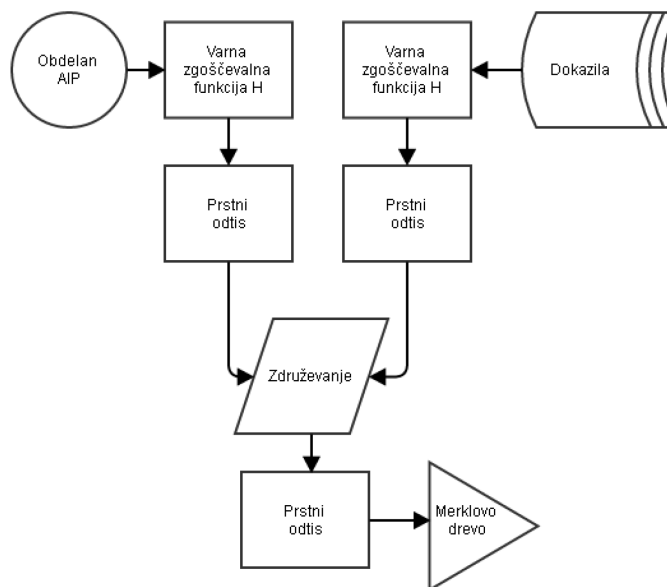
### 3.6.4.2.2 Kompleksno podaljševanje

Kompleksno podaljševanje se izvede takrat, ko se napove zmanjšanje varnosti zgoščevalnega algoritma, s katerim so bili narejeni prstni odtisi AIP.

V tem primeru je potrebno, preden zgoščevalni algoritem postane šibek izvesti podaljševanje po naslednjih korakih:

1. Izberemo novo varno zgoščevalno funkcijo.
2. Izračunamo nov prstni odtis za arhivski informacijski paket (AIP).
3. Izračunamo nov prstni odtis iz vseh dokazil, ki pripadajo AIP iz točke 2.
4. Prstna odtisa iz točke 2 in 3 združimo, njun skupni prstni odtis pa dodamo v Merklovo drevo. Za več informacij glej poglavje [Merklovo drevo](#).
5. Za vsak arhivski informacijski paket (AIP), za katerega je bil v postopku ustvarjanja dokazil uporabljen šibek algoritem je potrebno izvesti operacije, naštetje v točkah 2, 3 in 4.
6. Iz Merklovega drevesa se izračuna korenski prstni odtis.
7. Korenski prstni odtis se časovno žigosa.

S kompleksnim podaljševanjem zagotovimo zanesljivost AIP in vseh pripadajočih dokazil. Z novim časovnim žigom začnemo novo verigo časovnih žigov, ki se jih podaljšuje z enostavnim podaljševanjem, dokler velja za varno nova zgoščevalna funkcija, uporabljena pri zadnjem kompleksnem podaljševanju.



Slika 18: Del postopka kompleksnega podaljševanja, opisanega v točkah 2, 3 in 4

### 3.6.4.3 Merklovo drevo

Merklovo drevo je drevesno urejena podatkovna struktura, pri katerem so vozlišča drevesa prstni odtisi zgoščevalne funkcije enakega tipa.

Lastnosti drevesa so:

- Vsebuje samo prstne odtise zgoščevalnih funkcij enakega tipa (drevo ne more vsebovati prstnih odtisov narejenih na primer z MD5 in SHA1 zgoščevalnim algoritmom).
- Prstni odtisi se v drevo dodajajo kot končna vozlišča (angl. Leaf node). Gre za vozlišča, brez podrejenih vozlišč.
- Dodajanje in odvzemanje prstnih odtisov je mogoče le, ko drevo še ni zgrajeno.
- Korenski prstni odtis je odtis, izračunan pri gradnji drevesa in ščiti celotno drevo.
- Zgrajeno drevo lahko zmanjšamo samo na vozlišča, ki so nujno potrebna za izračun korenkega prstnega odtisa iz posameznega končnega vozlišča.

Na strežniku IMiS®/ARChive Server je izvedeno Merklovo drevo z uporabo dvojiškega drevesa. Dvojiško drevo je podatkovna struktura z vozliščem, ki ima lahko največ dve podrejeni vozlišči.

### 3.6.4.3.1 Gradnja Merklovega drevesa

Gradnja drevesa je postopek gradnje vozlišč od končnih vozlišč do korenkega vozlišča.

Gradnja vozlišča ali skupine poteka na naslednji način:

- Vzamemo dva prstna odtisa (vrednosti iz končnih vozlišč).
- Binarne vrednosti prstnih odtisov razvrstimo po velikosti v naraščajočem vrstnem redu.
- Razvrščene vrednosti združimo.
- Iz združenih vrednosti prstnih odtisov izračunamo nov prstni odtis istega tipa, ki predstavlja novo vozlišče v drevesu.

Ta postopek ponavljamo dokler imamo na voljo več kot eno vozlišče. Ko nam ostane samo še eno vozlišče pomeni, da je drevo zgrajeno. Vozlišče, ki je ostalo pa predstavlja korenski prstni odtis.

*Primer:* Merklovo drevo, ki ima štiri končna vozlišča s prstnimi odtisi, označena s H1, H2, H3 in H4.

*Predpostavimo, da za vrednosti prstnih odtisov veljajo naslednje relacije:*

- *Binarna vrednost prstnega odtisa H1 je manjša od H2 ( $H1 < H2$ ).*
- *Binarna vrednost prstnega odtisa H3 je večja od H4 ( $H3 > H4$ ).*

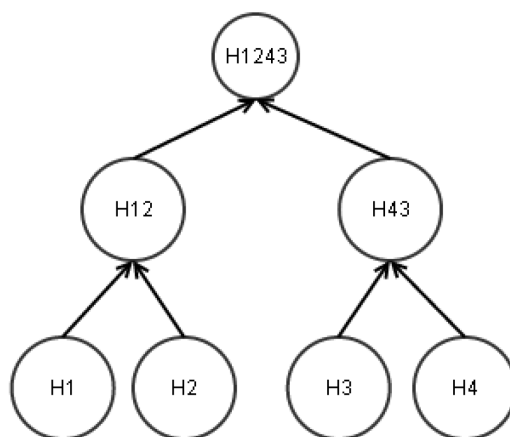
*Na podlagi teh relacij izračunamo novi vozlišči H12 in H43 po naslednjih formulah:*

- *$H12 = \text{HASH}(H1 || H2)$  – ker velja  $H1 < H2$ , sortiranje ohrani vrstni red, zato oba prstna odtisa samo združimo (operacija ||).*
- *$H43 = \text{HASH}(H4 || H3)$  – ker je H3 večji kot H4, sortiranje obrne vrstni red prstnih odtisov.*

*Za vozlišči H12 in H43 predpostavimo, da velja naslednja relacija:  $H12 < H43$ .*

*Tako iz teh dveh vozlišč izračunamo zadnje vozlišče:  $H1243 = \text{HASH}(H12 || H43)$ .*

*Ker je H1243 zadnje vozlišče v drevesu pomeni, da je drevo zgrajeno, vrednost vozlišča pa je korenski prstni odtis.*



Slika 19: Primer Merklovega drevesa

### 3.6.4.3.2 Reducirano Merklovo drevo

Zgrajeno Merklovo drevo lahko zreduciramo na število vozlišč, ki so nujno potrebna za izračun korenkega prstnega odtisa.

Reduciranje poteka na naslednji način:

- Izberemo končno vozlišče, za katerega hočemo reducirano Merklovo drevo.
- Za izbrano vozlišče pogledamo njegovo neposredno nadrejeno vozlišče in za to vozlišče vzamemo vsa neposredna podrejena vozlišča (kamor spada tudi na začetku izbrano vozlišče). Vrednosti prstnih odtisov v vozliščih razvrstimo naraščajoče (enako kot pri gradnji vozlišča).
- Iskanje nadaljujemo za vsa neposredno nadrejena vozlišča, dokler jih ne zmanjka (kar pomeni, da smo prišli do korenkega vozlišča). Vsa dobljena vozlišča razvrstimo naraščajoče.
- Neposredno nadrejenih vozlišč ne vključujemo v reducirano drevo, saj se jih da izračunati po pravilu gradnje Merklovega drevesa.

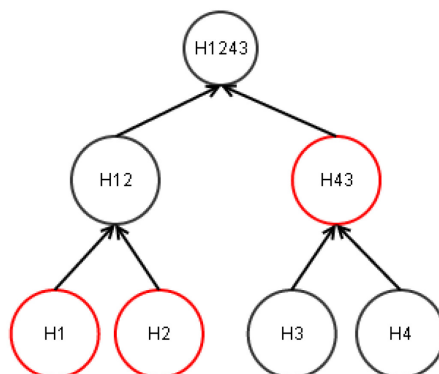
*Primer:* Reducirano Merklovo drevo, ki smo ga uporabili pri gradnji drevesa.

Izberemo končno vozlišče H1. Neposredno nadrejeno vozlišče je H12, njegovi podrejeni vozlišči pa sta H1 in H2. Obe vozlišči vzamemo ter ju razvrstimo po velikosti njihovih prstnih odtisov (velja relacija  $H1 < H2$ ). Vozlišču H12 je neposredno nadrejeno vozlišče H1243, njegovi podrejeni vozlišči pa sta H12 in H43. Ker se da vozlišče H12 izračunati iz vozlišč H1 in H2 ga izpustimo in v reducirano drevo vključimo samo vozlišče H43. Vozlišče H1243 nima neposredno nadrejenega vozlišča, zato se reduciranje drevesa za vozlišče H1 konča.



Reducirano drevo tako vsebuje vozlišča v naslednjem vrstnem redu: H1, H2, H43.

Kot je razvidno iz spodnje slike, je reducirano drevo za vozlišče H2 enako, saj imata H1 in H2 isto nadrejeno vozlišče H12.



Slika 20: Primer reduciranega drevesa za vozlišči H1 in H2

Primer izračuna korenskega prstnega odtisa:

Korenski prstni odtis se iz reduciranega drevesa izračuna na naslednji način:

$$H1243 = \text{HASH}(\text{HASH}(H1 \parallel H2) \parallel H43).$$

Postopek izračuna je naslednji:

- $H12 = \text{HASH}(H1 \parallel H2)$  – izračun vmesnega vozlišča H12;
- $\text{SORT}(H12, H43) = [H12, H43]$  – rezultat sortiranja H12 in H43 ( $H12 < H43$ );
- $H1243 = \text{HASH}(H12 \parallel H43)$  – izračun korenskega prstne odtisa.

Vzemimo za primer še reducirano drevo za vozlišči H3 in H4, ki vsebuje vozlišča v naslednjem vrstnem redu: H4, H3, H12.

Korenski prstni odtis izračunamo na naslednji način:

$$H1243 = \text{HASH}(H12 \parallel \text{HASH}(H4 \parallel H3)).$$

Postopek je naslednji:

- $H43 = \text{HASH}(H4 \parallel H3)$  – izračun vmesnega vozlišča H43;
- $\text{SORT}(H43, H12) = [H12, H43]$  – rezultat sortiranja H43 in H12 ( $H12 < H43$ );
- $H1243 = \text{HASH}(H12 \parallel H43)$  – izračun korenskega prstnega odtisa.

### 3.6.4.4 Sintaksa

Kot je bilo že omenjeno ima strežnik IMiS®/ARChive Server izveden ERS v XML obliki.

#### 3.6.4.4.1 Etiketa »EvidenceRecord«

Korenski element XML je etiketa »EvidenceRecord«, ki vsebuje elemente iz spodnje tabele.

Ime XML elementa	Tip XML elementa	Obveznost
Version	Atribut	DA
ArchiveTimeStampSequence	Etiketa	DA

Tabela 15: XML elementi etikete »EvidenceRecord«

#### **Atribut »Version«**

Vrednost atributa je fiksna vrednost »1.0« in predstavlja verzijo ERS.

#### **Etiketa »ArchiveTimeStampSequence«**

Vsebina etikete je zaporedje vseh verig arhivskih časovnih žigov (angl. Archive Timestamp chain), ki prikazuje ustvarjanje in podaljševanje ustvarjenih dokazil za avtentičnost dolgoročno hranjenih entitet. Za več informacij glej poglavje [Postopek ustvarjanja dokazil](#) in [Postopek podaljševanja dokazil](#).

Vsako zaporedje časovnih žigov je označeno z etiketo »ArchiveTimeStampChain«.

*Primer:* XML zapis, ki predstavlja ERS z dvema verigama časovnih žigov.

```
<EvidenceRecord xmlns="urn:ietf:params:xml:ns:ers" version="1.0">
  <ArchiveTimeStampSequence>
    <ArchiveTimeStampChain order="1">...</ArchiveTimeStampChain>
    <ArchiveTimeStampChain order="2">...</ArchiveTimeStampChain>
  </ArchiveTimeStampSequence>
</EvidenceRecord>
```

### 3.6.4.4.2 Etiketa »ArchiveTimeStampChain«

Etiketa vsebuje verigo arhivskih časovnih žigov, ki si bili ustvarjeni v postopku ustvarjanja in postopku podaljševanja z istim tipom zgoščevalne funkcije.

Elementi etikete so opisani v spodnji tabeli.

Ime XML elementa	Tip XML elementa	Obveznost
Order	Atribut	DA
DigestMethod	Etiketa	NE
CanonicalizationMethod	Etiketa	DA
ArchiveTimeStamp	Etiketa	DA

Tabela 16: XML elementi etikete »ArchiveTimeStampChain«

#### **Atribut »Order«**

Vrednost atributa predstavlja vrstni red zaporedja verig časovnih žigov.

Pri ustvarjanju prvega arhivskega časovnega žiga, se začne graditi veriga časovnih žigov z vrednostjo atributa »1«. V to verigo se nato dodajajo vsi arhivski časovni žigi, ki so bili ustvarjeni z enostavnim podaljševanjem.

Za vsak postopek kompleksnega podaljševanja se ustvari nova veriga arhivskih časovnih žigov, z vrednostjo atributa »2«, »3« itn. Za več informacij glej poglavje [Enostavno podaljševanje](#) in [Kompleksno podaljševanje](#).

#### **Etiketa »DigestMethod«**

Etiketa vsebuje obvezen atribut »Algorithm«. Vrednost atributa je URI, ki predpisuje zgoščevalni algoritem uporabljen v verigi. Etiketa ni obvezna, saj se informacija o zgoščevalnem algoritmu nahaja tudi v posameznem časovnem žigu.

#### **Etiketa »CanonicalizationMethod«**

Etiketa vsebuje atribut »Algorithm«. Njegova vrednost je enotni označevalnik vira (angl. Uniform resource identifier – URI), ki predpisuje algoritem za pretvorbo verige v normalizirano.

### 3.6.4.4.2.1 Etiketa »ArchiveTimeStamp«

Arhivski časovni žig vsebuje časovni žig (z vsemi pripadajočimi podatki, ki so potrebni za preverjanje le-tega) in reducirano Merklovo drevo, če se je časovno žigosalo večje število AIP. Elementi etikete so opisani v spodnji tabeli.

*Primer:* XML zapis prikazuje verigo, ki vsebuje tri arhivske časovne žige, generirane z zgoščevalnim algoritmom SHA1.

```
<ArchiveTimeStampChain order="1">
<DigestMethod algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<CanonicalizationMethod algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<ArchiveTimeStamp order="1">...</ArchiveTimeStamp>
<ArchiveTimeStamp order="2">...</ArchiveTimeStamp>
<ArchiveTimeStamp order="3">...</ArchiveTimeStamp>
</ArchiveTimeStampChain>
```

Ime XML elementa	Tip XML elementa	Obveznost
Order	Atribut	DA
HashTree	Etiketa	NE
TimeStamp	Etiketa	DA

Tabela 17: XML elementi etikete »ArchiveTimeStamp«

#### **Atribut »Order«**

Vrednost atributa predstavlja vrstni red arhivskega časovnega žiga znotraj verige. Arhivski časovni žig z vrednostjo »1« je bil tako ustvarjen v postopku ustvarjanja dokazil, vsi ostali arhivski časovni žigi pa v postopku enostavnega podaljševanja.

#### **Etiketa »HashTree«**

V primeru, da je etiketa prisotna, le-ta predstavlja reducirano Merklovo drevo, nad katerim je bil narejen pripadajoči arhivski časovni žig. V primeru, da etiketa ni prisotna, arhivski časovni žig pripada objektu, ki ima prstni odtis v časovnem žigu znotraj etikete »TimeStamp«.

Etiketa predstavlja reducirano Merklovo drevo. Vsebuje zaporedje elementov »Sequence«, ki predstavljajo nivoje Merklovega drevesa. Prvi nivo (nivo 0) ni vključen, saj se vrednost korenkega vozlišča lahko izračuna.

Elementi etikete »Sequence« so opisani v spodnji tabeli.

Ime XML elementa	Tip XML elementa	Obveznost
Order	Atribut	DA
DigestValue	Etiketa	DA

Tabela 18: XML elementi etikete »Sequence«

### **Atribut »Order«**

Vrednost atributa predstavlja nivo reduciranega Merklovega drevesa v obratnem vrstnem redu, kot je določena globina drevesa. Za več informacij glej poglavje [Merklovo drevo](#).

Prva veljavna vrednost atributa je »1«, ki predstavlja prstne odtise končnih vozlišč. Vrednost »2« bi tako predstavljala naslednji nivo, itn.

### **Etiketa »DigestValue«**

Vrednost etikete vsebuje Base64 kodiran prstni odtis.

*Primer:* XML zapis prikazuje reducirano Merklovo drevo z dvema nivojema.

*Prvi nivo (order 1) vsebuje Base64 kodirane prstne odtise končnih vozlišč,*

*drugi nivo pa vsebuje prstni odtis vozlišča, ki omogoča izračun prstnega odtisa korenskega vozlišča.*

```
<HashTree>
<Sequence order="1">
<DigestValue>D+/oVEs6CjRHj3UNL1vk4WcsEkA=</DigestValue>
<DigestValue>EBEhfDzZh9+rfb1Kaqe65o7TTok=</DigestValue>
</Sequence>
<Sequence order="2">
<DigestValue>fBuhe8txb00mNt27uvYupJTrgBQ=</DigestValue>
</Sequence>
</HashTree>
```

### **Etiketa »TimeStamp«**

Etiketa vsebuje časovni žig in seznam kriptografskih elementov (celotno vejo digitalnih potrdil in informacije o preklicih digitalnih potrdil), ki so potrebni za preverjanje časovnega žiga.

S temi podatki lahko nedvoumno dokažemo veljavnost časovnega žiga v času, ko je bil narejen in posledično avtentičnost vsebine, ki jo pokriva.

Ime XML elementa	Tip XML elementa	Obveznost
TimeStampToken	Etiketa	DA
CryptographicInformationList	Etiketa	NE

Tabela 19: XML elementi etikete »TimeStamp«

### Etiketa »TimeStampToken«

Etiketa vsebuje časovni žig pridobljen od izdajatelja varnih časovnih žigov.

Ima obvezen atribut »Type«, ki določa tip časovnega žiga.

Tip	Opis
»XMLENTRUST«	Časovni žig je v formatu XML, kot ga predpisuje W3C konzorcij ( <a href="http://www.w3.org/TR/xmldsig-core/">www.w3.org/TR/xmldsig-core/</a> ) in je kar vsebina TimeStampToken.
»RFC3161«	Časovni žig je narejen po standardu RFC3161. Vsebina TimeStampToken je Base64 kodirana zaradi kompatibilnosti z XML-jem.

Tabela 20: Podprti tipi časovnih žigov

### Etiketa »CryptographicInformationList«

Če etiketa je, vsebuje kriptografske elemente, ki omogočajo preverjanje verodostojnosti časovnega žiga. Če etikete ni, potem te elemente vsebuje že sam časovni žig.

Etiketa ima obvezna atributa »Order« in »Type«, ki določa tip kriptografskega elementa.

Tip	Opis
»CERT«	Kriptografski element je Base64 kodirano X509 digitalno potrdilo v binarni obliki.
»CRL«	Kriptografski element je Base64 kodirana lista preklicanih digitalnih potrdil v binarni obliki.
»OCSP«	Kriptografski element je Base64 kodiran odgovor strežnika po protokolu za sprotno preverjanje statusa elektronskega potrdila v binarni obliki.

Tabela 21: Podprti tipi kriptografskih elementov

Naslednji primer prikazuje prvi arhivski časovni žig, ki vsebuje reducirano Merklovo drevo, časovni žig v XML formatu in pripadajoč seznam kriptografskih elementov.

Prvi v seznamu je korensko digitalno potrdilo, ki skupaj z digitalnim potrdilom iz časovnega žiga tvori vejo digitalnih potrdil. Drugi element je lista pretečenih digitalnih potrdil, s katerim lahko preverimo, da digitalno potrdilo, ki je generiralo časovni žig ni pretečeno.

```
<ArchiveTimeStamp order="1">
<HashTree>
<Sequence order="1">
<DigestValue>D+/oVEs6CjRHj3UNL1vk4WcsEkA=</DigestValue>
<DigestValue>EBEhfDzZh9+rfb1Kaqe65o7TTok=</DigestValue>
</Sequence>
<Sequence order="2">
<DigestValue>fBuhe8txb00mNt27uvYupJTrgBQ=</DigestValue>
</Sequence>
</HashTree>
<TimeStamp>
<TimeStampToken type="XMLENTRUST">
<dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">...
</dsig:Signature>
</TimeStampToken>
<CryptographicInformationList>
<CryptographicInformation order="1" type="CERT">MIIEHDCCAwS...
</CryptographicInformation>
<CryptographicInformation order="2" type="CRL">MIISKTCEREC...
</CryptographicInformation>
</CryptographicInformationList>
</TimeStamp>
</ArchiveTimeStamp>
```

### 3.6.4.5 Enostavno podaljševanje

Pri enostavnem podaljševanju se vedno podaljša zadnji arhivski časovni žig v zadnji verigi arhivskih časovnih žigov.

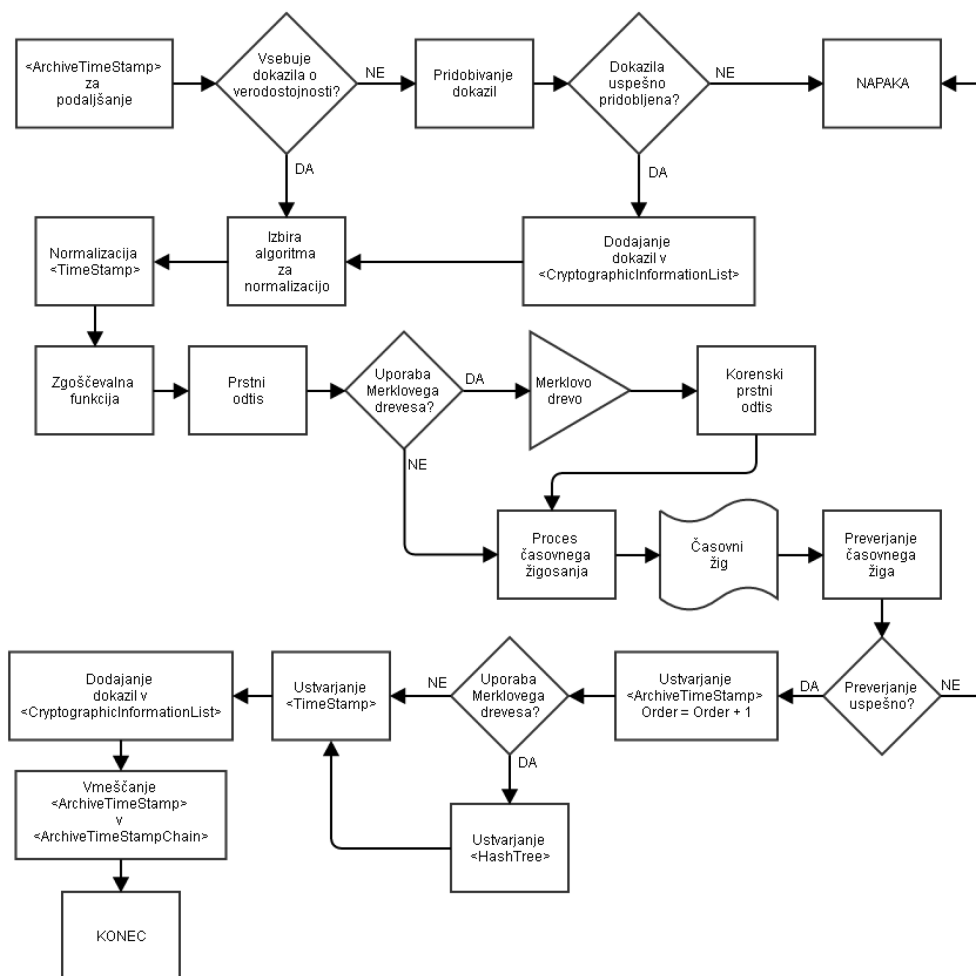
Postopek je naslednji:

1. Preveri se, če zadnji arhivski časovni žig vsebuje vse potrebne kriptografske elemente, ki dokazujejo verodostojnost žiga (certifikate, informacije o preklicanih elektronskih potrdilih). V primeru, da jih ne vsebujejo, jih strežnik samodejno pridobi in doda v pripadajoč seznam kriptografskih elementov.  
Če se dokazil ne more pridobiti, nadaljevanje postopka ni mogoče.
2. Na podlagi etikete »CanonicalizationMethod« iz verige časovnih žigov izberemo algoritem za pretvorbo v normalizirano obliko.

3. Iz zadnjega arhivskega časovnega žiga vzamemo etiketo »TimeStamp« in jo normaliziramo s prej izbranim algoritmom.
4. Z izbrano zgoščevalno funkcijo (določa jo etiketa »DigestMethod« v trenutni verigi ali pa je vsebovana v časovnem žigu, ki ga podaljšujemo) izračunamo prstni odtis normaliziranih podatkov. Tega časovno žigosamo (ali pa dodamo v Merklovo drevo v primeru podaljševanja več časovnih žigov ali kombinacije z ustvarjanjem dokazil).  
Za več informacij glej poglavje [Postopek podaljševanja dokazil](#).
5. Preverimo časovni žig.  
Za več informacij glej poglavje [Preverjanja časovnega žiga](#).
6. Če je preverjanje časovnega žiga neuspešno, je potrebno celoten postopek podaljševanja ponoviti, sicer ne moremo zagotoviti verodostojnosti novega časovnega žiga.
7. Če je preverjanje uspešno, potem ustvarimo novo etiketo »ArchiveTimeStamp« z vrednostjo atributa »Order«, ki je za 1 večje od arhivskega časovnega žiga, ki smo ga podaljšali. Če smo arhivski časovni žig podaljševali s pomočjo Merklovega drevesa, v novi časovni žig vključimo reducirano Merklovo drevo, ki mu pripada. Na koncu ustvarimo etiketo »TimeStamp«, kamor dodamo preverjen časovni žig s seznamom kriptografskih elementov, ki smo jih uporabili v postopku preverjanja.  
Nov arhivski časovni žig dodamo v zadnjo verigo časovnih žigov.



Spodnja slika prikazuje delovanje algoritma za enostavno podaljševanje arhivskih časovnih žigov.



Slika 21: Enostavno podaljševanje arhivskega časovnega žiga

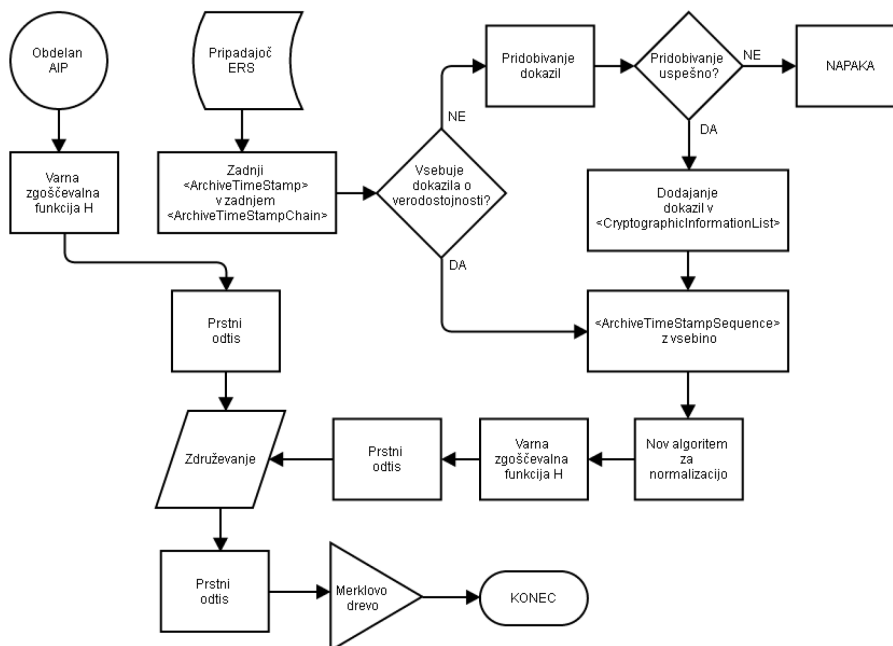
### 3.6.4.6 Kompleksno podaljševanje

Kompleksno podaljševanje se izvede ob menjavi šibkega zgoščevalnega algoritma za računanje prstnih odtisov z močnejšim. V tem primeru je potrebno kompleksno podaljšati vsa dokazila, ki so bila narejena z šibkejšim algoritmom za vse AIP, ustvarjene v postopku dolgoročne hrambe.

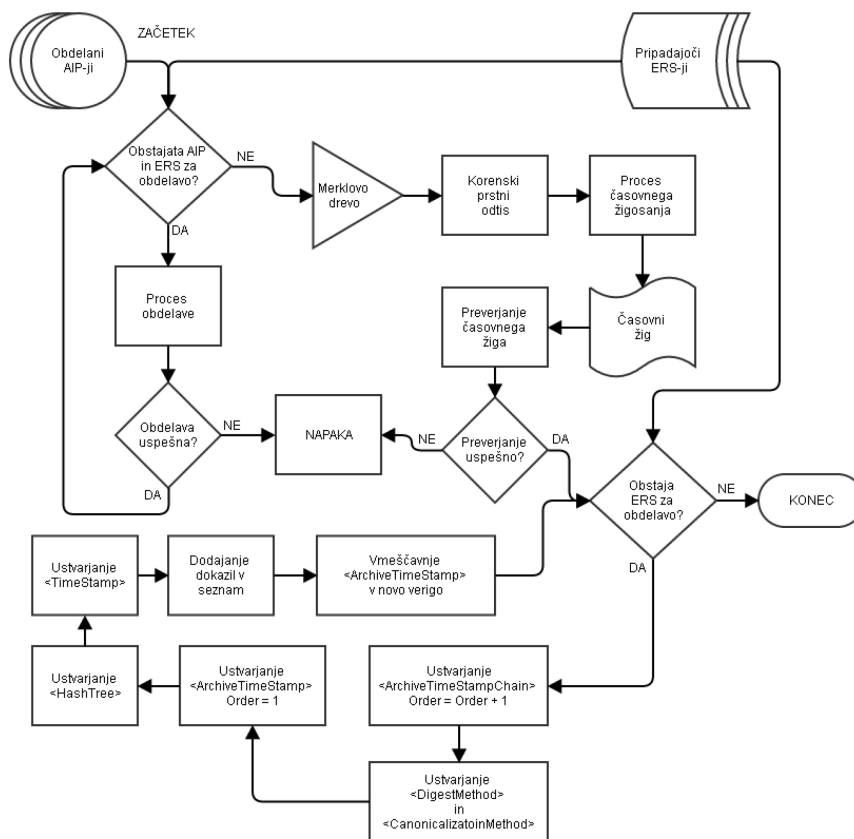
Postopek podaljševanja je naslednji:

1. Izberemo nov močan zgoščevalni algoritem.
2. Izberemo nov algoritem za pretvorbo v normalizirano obliko.
3. Z novim zgoščevalnim algoritmom izračunamo prstni odtis obdelanega AIP.
4. Za pripadajoči ERS preverimo, ali zadnji arhivski časovni žig v trenutni verigi časovnih žigov vsebuje vse potrebne kriptografske elemente za dokazovanje verodostojnosti. Če jih ne vsebuje, potem se jih pridobi in doda v pripadajoč seznam.
5. Če se dokazil ne more pridobiti, nadaljevanje postopka ni mogoče.
6. Iz pripadajočega ERS vzamemo etiketo »ArchiveTimeStampSequence« z njeno vsebino in jo pretvorimo v normalizirano obliko z novim algoritmom za pretvorbo.
7. Za normalizirano vsebino izračunamo prstni odtis z novim zgoščevalnim algoritmom.
8. Prstna odtisa, pridobljena iz obdelanega AIP in normalizirane vsebine združimo (njeni binarni vrednosti razvrstimo v naraščajočem vrstnem redu in ju zlepimo). Z novim zgoščevalnim algoritmom izračunamo prstni odtis in ga dodamo v Merklovo drevo.
9. Postopek iz točk 3. – 7. ponavljamo za vse AIP (in pripadajoče ERS), ki morajo biti kompleksno podaljšani.
10. Preverimo časovni žig. Če je preverjanje neuspešno potem postopka ne moremo nadaljevati.
11. V etiketi »ArchiveTimeStampSequence« izdelamo novo etiketo »ArchiveTimeStampChain« z atributom »Order«. Ta ima vrednost za 1 večjo kot zadnja etiketa »ArchiveTimeStampChain«.
12. Znotraj nove etikete »ArchiveTimeStampChain« zapišemo nov uporabljen zgoščevalni algoritem ter algoritem za pretvorbo v normalizirano obliko (etiketi »DigestMethod« in »CanonicalizationMethod«). Izdelamo novo etiketo »ArchiveTimeStamp« z vrednostjo atributa »Order« 1. Tako začnemo graditi novo verigo arhivskih časovnih žigov.
13. V »ArchiveTimeStamp« vključimo reducirano Merklovo drevo za združen prstni odtis AIP in ERS. Ustvarimo etiketo »TimeStamp«, kamor dodamo preverjen časovni žig s seznamom kriptografskih elementov, ki smo jih uporabili v postopku preverjanja.
14. Postopek iz točk 10. – 12. ponavljamo za vse ERS, ki so bili vključeni v postopek kompleksnega podaljševanja.

Kompleksno podaljševanje z Merklvim drevesom prikazujeta spodnji sliki.



Slika 22: Postopek obdelave AIP in pripadajočega ERS



Slika 23: Postopek kompleksnega podaljševanja z Merklvim drevesom

### 3.6.4.7 Verifikacija

Verifikacija ERS je postopek v katerem preverimo avtentičnost vseh verig arhivskih časovnih žigov. S tem dokažemo avtentičnost AIP, ki ga ščiti ERS.

V osnovi lahko verifikacijo delimo na:

- Verifikacija začetne verige časovnih žigov.
- Verifikacija ostalih verig časovnih žigov.

#### 3.6.4.7.1 Verifikacija začetne verige

Verifikacija začetne verige poteka na naslednji način:

- Iz verige pridobimo algoritem zgoščevalne funkcije in algoritem za normalizacijo (etiketi »DigestMethod in »CanonicalizationMethod«). Če etiketa »DigestMethod« ne obstaja, pridobimo podatke iz prvega arhivskega časovnega žiga verige - TimeStampToken).
- S pridobljenim zgoščevalnim algoritmom izračunamo prstni odtis pripadajočega obdelanega AIP.
- Če prvi arhivski časovni žig vsebuje reducirano Merklovo drevo, potem se mora izračunani prstni odtis AIP nahajati v prvi etiketi »Sequence« znotraj etikete »HashTree«.  
Iz reduciranega drevesa izračunamo korenski prstni odtis, ki se mora ujemati z prstnim odtisom v časovnem žigu.
- Če reduciranega Merklovega drevesa ni, potem se mora izračunani prstni odtis AIP ujemati s prstnim odtisom v časovnem žigu.
- Preverimo digitalno potrdilo časovnega žiga v času, ko je ta nastal (s pripadajočimi kriptografskimi objekti).
- Za vse naslednje arhivske časovne žige v verigi naredimo enako verifikacijo.  
Namesto prstnega odtisa AIP vzamemo predhodni arhivski časovni žig, ga normaliziramo, na normaliziranih podatkih izračunamo prstni odtis ter vrednosti prstnih odtisov preverimo v reduciranem Merklovem drevesu ali v časovnem žigu (glej prejšnje točke).

### 3.6.4.7.2 Verifikacija ostalih verig

Verifikacija verig, ki niso začetne poteka na naslednji način:

- Iz verige pridobimo algoritem zgoščevalne funkcije in algoritem za normalizacijo (etiketi »DigestMethod in »CanonicalizationMethod«). Če »DigestMethod« ne obstaja pridobimo podatke iz prvega arhivskega časovnega žiga verige – TimeStampToken.
- S pridobljenim zgoščevalnim algoritmom izračunamo prstni odtis pripadajočega obdelanega AIP.
- Iz »ArchiveTimeStampSequence« odstranimo trenutno verigo in vse naslednje verige. Tako ostanejo v »ArchiveTimeStampSequence« samo predhodne verige, ki so osnova za normaliziranje. Kot je opisano v kompleksnem podaljšanju, normaliziramo celoten »ArchiveTimeStampSequence« in z zgoščevalno funkcijo izračunamo prstni odtis normaliziranih podatkov.
- Prstna odtisa AIP in »ArchiveTimeStampSequence« združimo (razvrstimo naraščajoče ter zlepimo) in izračunamo skupni prstni odtis.
- Če prvi arhivski časovni žig vsebuje reducirano Merklovo drevo, potem se mora skupni prstni odtis nahajati v prvi etiketi »Sequence« znotraj etikete »HashTree«.  
Iz reduciranega drevesa izračunamo korenski prstni odtis, ki se mora ujemati z prstnim odtisom v časovnem žigu.
- Če reduciranega Merklovega drevesa ni, potem se mora skupni prstni odtis ujemati s prstnim odtisom v časovnem žigu.
- Verifikacija ostalih arhivskih časovnih žigov poteka po enakem postopku, kot je opisan v verifikaciji začetne verige časovnih žigov.

Po uspešni verifikaciji vseh verig po zgoraj opisanih postopkih lahko rečemo, da se vsebina AIP ni spremenila skozi čas (od njenega nastanka do trenutka verifikacije). Če se podatki v AIP ujemajo s podatki v entiteti potem lahko zagotovimo avtentičnost arhivirane entitete.

Če je verifikacija v katerikoli točki neuspešna, potem ne moremo zagotoviti avtentičnosti arhivirane entitete.

### 3.6.5 AIP

Arhivski informacijski paket (angl. Archival Information Package - AIP) je povzetek metapodatkov in vsebine entitete, ki je predmet zaščite postopkov zagotavljanja avtentičnosti, zbrane v XML datoteki.

AIP potrebujemo za grupiranje metapodatkov in vsebine entitete v arhivski informacijski paket, ki predstavlja vsebino za dolgoročno hrambo podatkov. Za več informacij glej poglavje [Predpogoji](#).

AIP se izdelava v naslednjih primerih:

- če lastnosti entitete ustrezajo vsaj enemu pravilu;
- ko ima zaprta entiteta vsaj en metapodatek ali vsebino, označeno za vključitev v arhivski informacijski paket.

Za več informacij glej poglavja [Predpogoji](#) in [Predloge](#).

AIP se shranjuje v podatkovno bazo strežnika IMiS®/ARChive Server. Dostopen je preko odjemalca IMiS®/wClient, ki lahko AIP po potrebi pridobi (skupaj z ERS), tudi pri izvozu.

AIP zapis je sestavljen iz naslednjih sekcij:

- glava
- metapodatki
- digitalna potrdila
- informacije o preklicih digitalnih potrdil.

#### 3.6.5.1 Glava

V sekcijo »Glava« so uvrščeni vsi potrebni podatki za pravilno obdelavo in interpretacijo arhivskega informacijskega paketa. Glava je obvezen del AIP.

Etiketa »Header« vsebuje elemente navedene v spodnji tabeli.

Ime XML elementa	Tip XML elementa	Obveznost
Version	Atribut	DA
CanonicalizationMethod	Etiketa	DA

Tabela 22: XML elementi etikete »Header«

**Atribut »Version«**

Atribut »Version« je ne-predznačeno 32-bitno število, ki predstavlja verzijo arhivskega informacijskega paketa. Verzija predpisuje način, kako naj se AIP obdeluje in interpretira pri preverjanju avtentičnosti entitete.

Vrednosti atributa »Version« in njihov pomen so opisane v spodnji tabeli.

Vrednost atributa	Interpretacija AIP
»1«	<p>Arhivski informacijski paket verzije »1« se obravnava kot celota.</p> <p>Na podlagi vrednosti etikete »CanonicalizationMethod« se izbere predpisano kanonikalizacijsko metodo, ki celoten XML pretvori v normalizirano obliko.</p> <p>Taka oblika je osnova za obdelavo (računanje prstnega odtisa, ...) in preverjanje avtentičnosti vsebine entitete in njenih metapodatkov.</p>

Tabela 23: Interpretacija AIP v odvisnosti od vrednosti atributa »Version«

**Etiketa »CanonicalizationMethod«**

Etiketa vsebuje atribut »Algorithm«. Njegova vrednost je enotni označevalnik vira (angl. Uniform Resource Identifier – URI), ki predpisuje algoritem za pretvorbo AIP v normalizirano obliko.

W3C konzorcij predpisuje naslednje URI vrednosti:

- <http://www.w3.org/TR/2001/REC-xml-c14n-20010315> (algoritem verzije 1.0).
- <http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718> (ekskluzivna verzija algoritma 1.0).
- <http://www.w3.org/TR/2008/REC-xml-c14n11-20080502> (algoritem verzije 1.1).

*Primer:* XML zapis prikazuje AIP verzije 1, ki uporablja algoritem verzije 1.0 za pretvorbo v normalizirano obliko.

```
<aip:Header version="1">
<ds:CanonicalizationMethod algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
</aip:Header>
```

### 3.6.5.2 Metapodatki

V sekcijo »Metapodatki« so uvrščeni metapodatki entitete, ki so v predlogah nastavljeni za vključitev v arhivski informacijski paket ne glede na to, ali vsebujejo kakšno vrednost ali ne. Za več informacij glej poglavje [Povezava s predlogami](#).

Sekcija je sestavljena iz zaporedja »Attribute« etiket, ki vsebujejo elemente navedene v spodnji tabeli.

Ime XML elementa	Tip XML elementa	Obveznost
Id	Atribut	DA
Type	Atribut	DA
Value	Etiketa	NE

Tabela 24: XML elementi etikete »Attribute«

#### **Atribut »Id«**

Vrednost atributa »Id« je naziv metapodatka.

#### **Atribut »Type«**

Vrednost atributa »Type« predstavlja tip metapodatka.

Za več informacij glej poglavje [Vrste atributov](#).

#### **Etiketa »Value«**

Vsebina etikete »Value« predstavlja vrednost atributa oziroma vrednosti, v primeru, da gre za atribut z več vrednostmi. Vsebina je lahko enostavna (prisotna je samo vrednost atributa ali prstni odtis vrednosti) ali kompleksna (poleg vsebine ali prstnega odtisa so prisotni še podatki o digitalnih podpisih vsebine).

V primeru ko je za vrednost prisoten prstni odtis vsebine potem etiketa vsebuje še etiketo »Digest« z elementi, ki so opisani v naslednji tabeli.

Ime XML elementa	Tip XML elementa	Obveznost
DigestMethod	Etiketa	DA
DigestValue	Etiketa	DA

Tabela 25: XML elementi etikete »Digest«



**Etiketa »DigestMethod«**

Etiketa vsebuje atribut »Algorithm«, ki je obvezen in katerega vrednost je URI. Ta predpisuje algoritem za izračun prstnega odtisa vsebine. Podprti algoritmi so naštetih v spodnji tabeli, ki predstavlja podprte algoritme za izračun prstnih odtisov in pripadajoče URI, določene pri W3C konzorciju (<http://www.w3.org/TR/2013/NOTE-xmlsec-algorithms-20130124>) ter v specifikaciji RFC 4051 (<http://www.ietf.org/rfc/rfc4051.txt>).

Algoritem	URI
MD5	<a href="http://www.w3.org/2001/04/xmlsig-more#md5">http://www.w3.org/2001/04/xmlsig-more#md5</a>
SHA1	<a href="http://www.w3.org/2000/09/xmlsig#sha1">http://www.w3.org/2000/09/xmlsig#sha1</a>
SHA224	<a href="http://www.w3.org/2001/04/xmlsig-more#sha224">http://www.w3.org/2001/04/xmlsig-more#sha224</a>
SHA256	<a href="http://www.w3.org/2001/04/xmlenc#sha256">http://www.w3.org/2001/04/xmlenc#sha256</a>
SHA384	<a href="http://www.w3.org/2001/04/xmlsig-more#sha384">http://www.w3.org/2001/04/xmlsig-more#sha384</a>
SHA512	<a href="http://www.w3.org/2001/04/xmlenc#sha512">http://www.w3.org/2001/04/xmlenc#sha512</a>

Tabela 26: Algoritmi in pripadajoči URI

**Etiketa »DigestValue«**

Etiketa predstavlja Base64 kodirano vrednost digitalnega prstnega odtisa, narejenega z algoritmom, ki je zapisan v atributu »Algorithm« v etiketi »DigestMethod«.

*Primer:* enostavna vsebina metapodatkov entitete, kjer je naveden avtor in njegov naslov.

- Metapodatek »Author« je tipa »String50«, »Client Address1« in »Client Address2« pa sta tipa »String100«, MultiValue.
- Metapodatek »Client Address2« nima vrednosti, a je vseeno vključen v arhivski informacijski paket.

```
<aip:Attribute id="Author" type="22">
<aip:Value>Janez Novak</aip:Value>
</aip:Attribute>
<aip:Attribute id="Client Address1" type="23">
<aip:Value>Brnciceva 41g</aip:Value>
<aip:Value>1231 Ljubljana</aip:Value>
</aip:Attribute>
<aip:Attribute id="Client Address2" type="23"/>
```

*Primer:* enostavna vsebina metapodatkov entitete, kjer se za vrednost uporablja digitalni prstni odtis vsebine.

```
<aip:Attribute Id="sys:Content" type="42">
  <aip:Value>
    <aip:Digest>
      <ds:DigestMethod algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>xcwyBBmUzLqoHNSt+O9IGdmCiw=</ds:DigestValue>
    </aip:Digest>
  </aip:Value>
</aip:Attribute>
```

Kompleksna vsebina vsebuje še podatke o digitalnih podpisih vsebine. Digitalni podpis je vsebovan v etiketi »Signature« in je kodiran v Base64. Etiketeta vsebuje elemente, ki so opisani v spodnji tabeli.

Ime XML elementa	Tip XML elementa	Obveznost
Version	Atribut	DA
Type	Atribut	DA

Tabela 27: XML elementi etikete »Signature«

### **Atribut »Version«**

Vrednost etikete predstavlja verzijo digitalnega podpisa.

### **Atribut »Type«**

Vrednost etikete predstavlja tip digitalnega podpisa. Trenutno podprt format je »XMLDSIG«.

Naslednji primer prikazuje kompleksno vsebino, kjer se poleg digitalnega prstnega odtisa nahajata še dva digitalna podpisa vsebine.

```
<aip:Attribute Id="sys:Content" type="42">
  <aip:Value>
    <aip:Signature Version="1" Type="XMLDSIG">ajM5dHogIGlqZ...aip:Signature>
    <aip:Signature Version="1" Type="XMLDSIG">Ym52ODMgl...</aip:Signature>
    <aip:Digest>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>xQmFgsuudE4gOkT3Hg/QB65caiQ=</ds:DigestValue>
    </aip:Digest>
  </aip:Value>
</aip:Attribute>
```

### 3.6.5.3 Digitalna potrdila

V to sekcijo so uvrščene celotne veje digitalnih potrdil, ki pripadajo elektronskim podpisom in so Base64 kodirana. Sekcija je sestavljena iz etiket »Certificate«, ki vsebuje obvezen atribut »Type«, ki predstavlja tip digitalnega potrdila. Trenutno podprt format je »X509DER«. Naslednji zapis prikazuje primer dveh digitalnih potrdil.

```
<aip:Certificate Type="X509DER">bmlzOHYg...</aip:Certificate>
<aip:Certificate Type="X509DER">Ym4zdmJk...</aip:Certificate>
```

### 3.6.5.4 Informacije o preklicih digitalnih potrdil

Poleg preverjanja časovne veljavnosti digitalnih potrdil so ključnega pomena tudi informacije o preklicih.

Digitalno potrdilo lahko izdajatelj zaradi različnih vzrokov prekliče (izguba zaupanja v tajnost privatnega ključa, izguba zaupanja v izdajatelja digitalnega potrdila, ...).

Preklicano digitalno potrdilo ni več veljavno (zaupanja vredno), prav tako izgubijo veljavnost vsi elektronski podpisi in časovni žigi, ki so bili z njim izdelani.

V arhivskem informacijskem paketu sta podprta CRL in OCSP tipa informacij o preklicih, ki sta šifrirana v Base64 obliki.

Sekcija je sestavljena iz etiket »RevocationData«, ki vsebujejo elemente opisane v spodnji tabeli.

Ime XML elementa	Tip XML elementa	Obveznost
Id	Atribut	DA
Type	Atribut	DA

Tabela 28: XML elementi etikete »RevocationData«

#### **Atribut »Id«**

Vrednost atributa »Id« je unikatni identifikator.

**Atribut »Type«**

Vrednost atributa »Type« predstavlja tip informacije o preklicih digitalnih potrdil.

Spodnja tabela prikazuje podprte vrednosti.

Vrednost	Opis
CRLDER	Informacija je seznam preklicanih digitalnih potrdil v binarni obliki.
OCSP	Informacija je rezultat protokola za sprotno preverjanje statusa elektronskega potrdila v binarni obliki

Tabela 29: Podprti tipi informacij o preklicu digitalnih potrdil

*Primer:* XML zapis za oba podprta tipa informacij.

```
<aip:RevocationData id="1" type="CRLDER">MIISKTCCERECAQEwDQ...
</aip:RevocationData>
<aip:RevocationData id="2" type="OCSP">MIIDBjCB7wI...
</aip:RevocationData>
```

**3.6.6 Časovno žigosanje**

Časovni žigi so dokazila, ki dokazujejo obstoj vsebine v času navedenim v časovnem žigu.

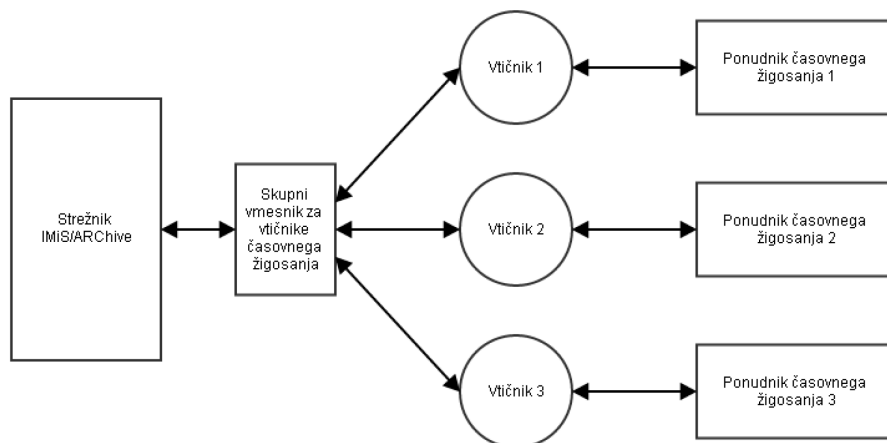
Storitev časovnega žigosanja opravljajo zaupanja vredni ponudniki

(npr. SI-TSA: <http://www.si-tsa.si/>). Ti morajo izpolnjevati stroge varnostne ukrepe,

sicer bi lahko podvomili v verodostojnost časovnih žigov, ki so jih ustvarili.

Strežnik IMiS®/ARChive Server uporablja koncept vtičnikov (angl. Plug-in) za pridobivanje časovnih žigov. Za vsakega ponudnika varnih časovnih žigov, ki svoje žige ponujajo preko tehnološko heterogenih načinov/vmesnikov, ponudimo svoj vtičnik.

Ta zna komunicirati s ponudnikom časovnih žigov in jih na strežniku poznan način vključevati v postopke zagotavljanja avtentičnosti hranjenega gradiva.



Slika 24: Koncept vtičnikov

### 3.6.6.1 Pridobivanje časovnega žiga

Postopek pridobivanja časovnega žiga je naslednji:

1. Strežnik izračuna prstni odtis podatkov, kateri so predmet časovnega žigosanja.
2. Prstni odtis se preko skupnega vmesnika pošlje vtičniku za časovno žigosanje.
3. Če ponudnik časovnega žiga podpira uporabo poljubne kode (angl. Nonce ali Arbitrary number), vtičnik s pomočjo generatorja naključnih števil ustvari naključno vrednost, ki jo skupaj s prstnim odtisom pošlje ponudniku časovnega žigosanja. Poljubna koda preprečuje napade s ponavljanjem (angl. Replay attack - [http://en.wikipedia.org/wiki/Replay\\_attack](http://en.wikipedia.org/wiki/Replay_attack)).
4. Ponudnik časovnega žigosanja k prejetim podatkom doda časovno komponento in vse skupaj podpiše s privatnim ključem.
5. Če je vtičnik uporabil poljubno kodo, jo preveri, če se ista vrednost nahaja tudi v časovnem žigu. Če ga ne najde, časovni žig zavrže saj se upošteva, da je neveljaven.

### 3.6.6.2 Preverjanje časovnega žiga

Preverjanje časovnega žiga izvaja strežnik. Postopek preverjanja je naslednji:

- Preveri se veljavnost digitalnega potrdila, ki je ustvarilo časovni žig.
- Preverijo se informacije o preklicih vseh potrdil v verigi vključno z digitalnim potrdilom, ki je ustvarilo časovni žig.
- Preveri se parameter »mTimestamp« v podaljških digitalnega potrdila, ki je ustvarilo časovni žig. Za več informacij glej poglavje [Razširjena uporaba ključa](#).
- Preveri se veljavnost elektronskega podpisa časovnega žiga.

Če je katerokoli preverjanje neuspešno, se časovni žig obravnava kot neveljaven in ga strežnik zavrže. V tem primeru je potrebno postopek pridobivanja časovnega žiga ponoviti.

### 3.6.6.3 Primer

Primer v nadaljevanju prikazuje časovni žig v XML formatu. Za preverjanje časovnega žiga v XML formatu strežnik uporablja odprtokodno knjižnico XMLSec (<http://www.aleksey.com/xmlsec>).

```
<dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" id="TimeStampToken">
<dsig:SignedInfo>
<dsig:CanonicalizationMethod algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
<dsig:SignatureMethod algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<dsig:Reference URI="#TimeStampInfo-13ED106F54C2C33ED42000000000007B81">
<dsig:DigestMethod algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<dsig:DigestValue>LaeChaxwlaM8e9WZIRDOQjxzFrw=
</dsig:DigestValue>
</dsig:Reference>
<dsig:Reference URI="#TimeStampAuthority">
<dsig:DigestMethod algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<dsig:DigestValue>j8bwhFukHoD6jcmzgzEztXDF/ko=
</dsig:DigestValue>
</dsig:Reference>
</dsig:SignedInfo>
<dsig:SignatureValue>
sxbZkdzdWPcXHP06k1WhZzglyTtYLXUqaOzPaT/7VkwJ3haur5yiL
qDC01zRogaPojVCO6Ee545/VrdP1JmnczwFXAW3UU+q6VrDDHLYd
z4uW9hXxEy31YNkQmJ7BOicHNY9m2TOIk8tjCSec6s5UJxhJP49tY
u8wE7gMSgWpLlnMeAZCE/DVOPiqesVTUYzaLSbEqELpL5qFkvCmNC
TBjnaNuyKe/YhQWbvZ0clvHePqyADNwX+IPOsAOS8NezpZHYriBO8
B+cAwglep/gZb1h8zDlqejHS8ibnFmvbIk3Z0lbG/Y1SK36yk+Fu5
ya12KHIFOACzx/im3GE8vWQ==
</dsig:SignatureValue>
<dsig:KeyInfo id="TimeStampAuthority">
<dsig:X509Data>
<dsig:X509Certificate>
MIIFYDCCBEigAwIBAgIEQLMGwDANBgkqhkiG9w0BAQUFADA+MQswC
QYDVQQGEwJzaTEbMBkGA1UEChMSc3RhZGUtaW5zdG10dXRpb25zMR
lwEAYDVQQLEwJzaXRlc3QtY2EwHhcNMTIwNTIxMDc0ODM4WhcNMTc
wNTIxMjExMDU2WjBvMQswCQYDVQQGEwJzaTEbMBkGA1UEChMSc3Rh
dGUtaW5zdG10dXRpb25zMRlwEAYDVQQLEw1TSVRFU1QtQQExLzAUB
gNVBAMTDXRzYS10ZXNOLTIwMTIwFwYDVQQFEwAxMTEwMTExMTExMT
ExMTEwMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvsX
FScylvL5dbkj/df82Ego08QH41xuz5TcKoBHCME+9fKcNiGVivJll
sZOihB4jta1JABKCEA4yJDEphNV9IK5MIYaqYW/3trijvCSZefGWr
W0kHt3gcIDLpR2SbGDEACxpledIA2MZR1bnSDekgCOGbPiiz/jk4Q
PDGaGZ00/FI5WfazvKqwnvHySsoSiUk7uUH8XgAv3Uv/ghYPjSfas
xXSvy/SKJAusKOyVFXiIT+SmaX+p60KroDkxhuKM9WzoehHcCPLzy
2JUPerr02+AX4zBytPsb+AVS9XjI3KQIFpovSlph510H9hTused1g
b7gizt/leY3T3Nf4BglxwIDAQABo4ICMzCCAi8wDgYDVROPAQH/BA
QDAgeAMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMIMEAGA1UdIAQ5MDc
wNQYKKwYBBAGvWQEFaZAnMCUGCCsGAQUFBwBFhloDHRwOi8vd3d3
LmNhLmdvdi5zaS9jcHMvMBoGA1UdEQQTMGBD3RzYS10ZXNOQGdvd
```

```
i5zaTAbBgNVHQkEFDASMBAGCSqGSIb2fQdEHTEDAqEKMIH2BgNVHR
BEge4wgeswVaBTOfGkTzBNMQswCQYDVQQGEwJzaTEbMBkGA1UEChM
Sc3RhdGUtaW5zdGI0dXRpb25zMRlwEAYDVQQLwzEwZaXRlc3QtY2Ex
DTALBgNVBAMTBENSTDMwgZGggY6ggYuGWGxkYXA6Ly94NTAwLmdvd
i5zaS9vdT1zaXRlc3QtY2Esbz1zdGF0ZS1pbmN0aXR1dGlbnMsYz
1zaT9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2WGL2h0dHA
6Ly93d3cuc2lnZW4tY2Euc2kvY3JsL3NpdGVzdC9zaXRlc3QtY2Eu
Y3JsMCsGA1UdEAQkMCKADzlwMTlwNTlxMDc0ODM4WoEPMjAxNTA1M
jEyMjE0NDlaMB8GA1UdIwQYMBaAFFRJB0aHxz2JncqucqeooKBpty
HnMBOGA1UdDgQWBBSwflsAtvqW4RKcSTY5n4Mbg/dTAJBgNVHRM
EAjAAMBkGCSqGSIb2fQdBAQAQMMAobBFY3LjEJEDAgSwMAOGCSqGSIb3
DQEBBQUAA4IBAQBh2Vgmo+MrbwqVcSvMln7aA9HLjw+HIM5KbXXvM
/XEmFWHvVrWFhbqX1f+OoizSfDv4sErCPb3zzeSG2mnEREzk9gqzbt
NlqfvzdZ7Xkd7bGUEzwHEcVE8DSW2bJGeSkhyX2AWvt4eHyqwgXply
MzFOVSWteivgwgVmtUZjSbeClpELUbiGWzwyxW15SHufOdJdtgcnn
r2hCLtkYJ9ky4T0m5gvvy0xmQi+o3rLvPa5yLeHYa//KzPo+H8CPf
UGqRFTPVSykaln6evTg6CDQvG9jfi1PbaeKQRmOxLQPpVNYFA66e
2DwVv+9UdKzcoBfujvZRtEuPlnphHBlzxEkFU3
</dsig:X509Certificate>
</dsig:X509Data>
</dsig:KeyInfo>
<dsig:Object id="TimeStampInfo-13ED106F54C2C33ED42000000000007B81">
<ts:TimeStampInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:ts="http://www.entrust.com/schemas/timestamp-protocol-20020207">
<ts:Policy id="http://www.si-tsa.si/dokumenti/SI-TSA-politika-za-casovni-zig-1.pdf"/>
<ts:Digest>
<ds:DigestMethod algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>93WQD+wSgMA5KCzcmjYe55NBKEc=
</ds:DigestValue>
</ts:Digest>
<ts:SerialNumber>108487637460984003369566416624147310345089
</ts:SerialNumber>
<ts:CreationTime>2014-03-31T15:00:00.089Z
</ts:CreationTime>
<ts:Nonce>10600496071266535864
</ts:Nonce>
</ts:TimeStampInfo>
</dsig:Object>
</dsig:Signature>
```

**Etiketa »dsig:SignedInfo«**

Etiketa vsebuje informacije, kaj je v XML predmet elektronskega podpisa in metode za normalizacijo XML pri preverjanju časovnega žiga:

- dsig:CanonicalizationMethod: metoda za normalizacijo XML.
- dsig:SignatureMethod: uporabljen algoritem pri ustvarjanju elektronskega podpisa.
- dsig:Reference URI="#TimeStampInfo-13ED106F54C2C33ED42000000000007B81": referenca na etiketo dsig:Object, ki je predmet vsebine elektronskega podpisa. Vsebuje tudi algoritem ter prstni odtis, ki pripadata tej etiketi.
- dsig:Reference URI="#TimeStampAuthority": referenca na etiketo »dsig:KeyInfo«, ki je prav tako predmet vsebine elektronskega podpisa. Vsebuje algoritem ter prstni odtis, ki pripadata etiketi.

**Etiketa »dsig:SignatureValue«**

Etiketa vsebuje vrednost elektronskega podpisa.

**Etiketa »dsig:KeyInfo«**

Etiketa vsebuje informacije o digitalnem potrdilu, ki je ustvarilo časovni žig:

- dsig:X509Data – etiketa vsebuje etiketo dsig:X509Certificate, ki vsebuje digitalno potrdilo, ki je ustvarilo elektronski podpis.

**Etiketa »dsig:Object«**

Etiketa vsebuje naslednje podatke:

- ts:TimeStampInfo: informacije o protokolu.
- ts:Policy: informacije o politiki ponudnika časovnega žigosanja.
- ts:Digest: prstni odtis (ter URI algoritma, ki ga je izdelal), ki ga je ponudnik prejel v časovno žigosanje.
- ts:SerialNumber: serijska številka.
- ts:CreationTime: datum in čas nastanka časovnega žiga.
- ts:Nonce: poljubna koda, ki je bila uporabljena v postopku ustvarjanja zahtevka za časovno žigosanje.



### 3.6.7 Pravila

Pravila določajo pogoje, kdaj naj se izvajata postopka ustvarjanja in podaljševanja dokazil, ter katere vsebine so predmet teh postopkov. Ustvarjanje in podaljševanje dokazil poteka paketno. Uporablja se Merklovo drevo, razen v primeru, če se v paketu nahaja samo en AIP ali arhivski časovni žig. Paketi so določeni kot minimalno in maksimalno število arhivskih informacijskih paketov, ki se časovno žigosajo z enim časovnim žigom.

Primer konfiguracije paketa prikazuje naslednji XML zapis:

```
<Settings>
  <MinBatchSize>1</MinBatchSize>
  <MaxBatchSize>300</MaxBatchSize>
</Settings>
```

#### **Etiketa »MinBatchSize«**

Vsebuje minimalno število arhivskih informacijskih paketov, ki se časovno žigosajo z enim časovnim žigom. Vrednost ne sme biti manjša od 1 in večja od vrednosti »MaxBatchSize«.

#### **Etiketa »MaxBatchSize«**

Vsebuje maksimalno število arhivskih informacijskih paketov, ki se časovno žigosajo z enim časovnim žigom. Vrednost ne sme biti manjša od »MinBatchSize« in večja od 1.000.000.

### 3.6.7.1 Pravila za ustvarjanje dokazil

Pravila za ustvarjanje dokazil se uporabljajo pri preverjanju, ali entiteta ustreza pogojem za zagotavljanje avtentičnosti. Če lastnosti entitete ustrezajo vsaj enemu pravilu, potem se bo za tako entiteto ustvarilo dokazilo, ki ga pravilo določa. V primeru, da lastnostim entitete ustreza več pravil, potem se upošteva prvo tako pravilo. Prednost imajo pravila, ki veljajo tudi za vsebovane entitete.

Primer pravila prikazuje naslednji XML zapis:

```
<Rule>
  <Id>307a8c60-390c-470d-9692-a43311bd51ef</Id>
  <Enabled>true</Enabled>
  <Type>Explicit</Type>
  <IncludeChildren>true</IncludeChildren>
  <Scope type="ClassificationCode">C=57</Scope>
  <Expression>[sys:Status]="2"</Expression>
  <TemplateFilter></TemplateFilter>
  <TimeStampProviderId>a48d9c39-456a-470c-9c8b-e54bb91fc1dc</TimeStampProviderId>
</Rule>
```

**Etiketa »Id«**

Etiketa vsebuje unikatni identifikator pravila.

**Etiketa »Enabled«**

Vrednost etikete je lahko »True« ali »False« in določa, ali je pravilo omogočeno ali ne.

**Etiketa »Type«**

Vrednost etikete je lahko »Explicit« ali »Implicit«. Eksplicitna pravila se preverjajo pri operacijah nad entitetami (shranjevanje, sprememba statusa...), v procesu časovnega žigosanja pa se preverjajo vsa pravila.

**Etiketa »IncludeChildren«**

Vrednost etikete je lahko »True« ali »False«, določa pa veljavnost pravila na pod entitetah.

**Etiketa »Scope«**

Vrednost etikete vsebuje identifikator entitete, pod katero se pravilo upošteva pri preverjanju lastnosti entitete. Če entiteta ni vsebovana, potem tako pravilo za njo ne velja.

**Etiketa »Expression«**

Vrednost vsebuje iskalni niz, ki se preverja z lastnostmi entitete. Če iskalni niz ne ustreza vrednostim v entiteti, potem pravilo za entiteto ne velja.

**Etiketa »TemplateFilter«**

Vrednost etikete vsebuje imena predlog, s katerimi morajo biti entitete narejene, da lahko ustrezajo pravilu. Vrednost se uporablja kot dodatni filter za vrednost »Expression«.

Če je vrednost »TemplateFilter« prazen niz, potem se vrednost ne upošteva pri preverjanju pravila z vrednostjo entitete.

**Etiketa »TimeStampProviderId«**

Vrednost etikete predstavlja unikatni identifikator ponudnika časovnih žigov, s katerim se bodo entitete, ki ustrezajo pravilu, časovno žigosale.

Primer: Pravilo iz našega primera tako velja za entitete, ki so pod razredom s klasifikacijsko oznako »57« (velja tudi za sam razred) in imajo vrednost »sys:Status« enako 2 (zaprta entiteta) ali pa so pod entitete razreda ali zadeve, ki je zaprta (recimo dokumenti v zaprti zadevi).

### 3.6.7.2 Pravila za podaljševanje dokazil

Pravila za podaljševanje dokazil se uporabljajo pri enostavnem in kompleksnem podaljševanju.

Primer prikazuje naslednji XML zapis:

```
<Rule>
  <Id>6062074f-6d05-4f24-8592-866623ade8bf</Id>
  <Enabled>true</Enabled>
  <Digest>SHA1</Digest>
  <CertificateExpirationTreshold>90d</CertificateExpirationTreshold>
  <TimeStampProviderId>bac87d4d-fd1b-4065-bb36-5d03eeb25b6e</TimeStampProviderId>
</Rule>
```

#### **Etiketa »Id«**

Etiketa vsebuje unikatni identifikator pravila.

#### **Etiketa »Enabled«**

Vrednost etikete je lahko »True« ali »False« in določa, ali je pravilo omogočeno ali ne.

#### **Etiketa »Digest«**

Vrednost etikete predstavlja tip zgoščevalne funkcije, ki se bo uporabila pri časovnem žigosanju.

#### **Etiketa »CertificateExpirationTreshold«**

Vrednost predstavlja časovni okvir, v katerem bodo zajeti vsi časovni žigi z istim tipom zgoščevalne funkcije in katerih digitalna potrdila pretečejo v danem časovnem okvirju.

#### **Etiketa »TimeStampProviderId«**

Vrednost predstavlja unikatni identifikator ponudnika časovnih žigov, s katerim se bodo dokazila pred iztekom podaljšala.

Pravilo iz našega primera tako velja za vsa dokazila, ki so bila narejena z zgoščevalno funkcijo SHA1, in katerih digitalna potrdila potečejo v roku 90 dni.

### 3.7 Odbiranje in izločanje

Odbiranje in izločanje je nadzorovan in načrtovan postopek za izvedbo prenosa, uničenja ali trajne hrambe elektronskega gradiva. Vsak razred, zadeva ali dokument (uvrščen neposredno pod razredom) mora imeti določen vsaj en rok hrambe. Za več informacij glej poglavje [Upravljanje s povezavami politik hrambe](#). Ta določa koliko časa je potrebno posamezno entiteto hraniti v arhivskem sistemu.

Poleg časovnega okvira rok hrambe vsebuje še privzeto akcijo, ki se bo izvedla v postopku odbiranja in izločanja. Akcijo lahko spremenijo uporabniki s pravicami (člani komisije), ki izvajajo odbiranje in izločanje.

Postopek delimo v naslednje faze:

- priprava
- odločanja
- izvedba.

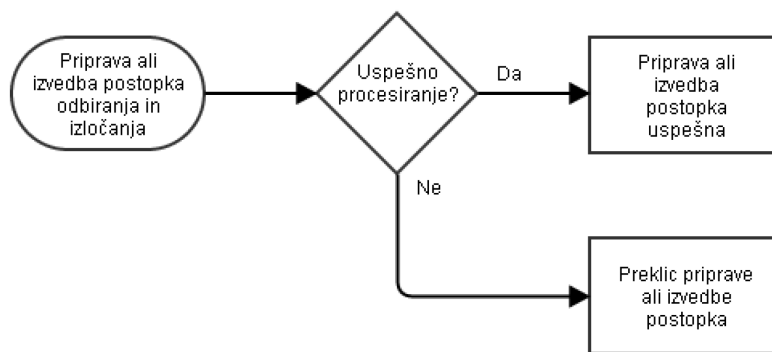
V postopku priprave in izvedbe odbiranja in izločanja lahko pride do napake zaradi različnih vzrokov. V primeru napake se postopek samodejno prekliče.

Izvedejo se naslednje spremembe:

- Status se spremeni v »Zaprto« (angl. Closed).
- Stanje se spremeni v »Neuspešno« (angl. Failed). Vrednost stanja se nahaja v atributu »sys:ret:rev:State«.
- V atribut »sys:ret:rev:Message« se zapiše vzrok preklica.

Postopka pri katerem je prišlo do napake se ne da ponovno pripraviti ali izvesti. Prav tako ni dovoljeno njegovo urejanje. Pri postopku priprave ali izvedbe je potrebno poudariti, da se vse akcije nad entitetami izvajajo v imenu uporabnika, ki je pripravo ali izvedbo sprožil.

Tako na postopek priprave in izvedbe vplivajo uporabniške pravice in stopnja tajnosti na entitetah. V nadaljevanju je prikazan diagram poteka postopka odbiranja in izločanja v primeru priprave ali izvedbe.



Slika 25: Diagram poteka izvajanja postopka odbiranja in izločanja

### 3.7.1 Postopek priprave za odbiranje in izločanje

Prva faza postopka odbiranja in izločanja je priprava. Uporabnik s pravico ustvari entiteto, ki bo kasneje prešla v postopek odbiranja in izločanja.

Poleg vseh obveznih atributov mora vnesti še vrednost enega izmed naslednjih atributov:

- »sys:ret:rev:Query«: vrednost predstavlja iskalni niz za entitete, ki bodo vključene v postopek odbiranja in izločanja. Za več informacij glej poglavje [Pravila iskalnega niza](#). Uporaba iskalnega niza pri postopku priprave za odbiranje in izločanje je namenjena ad-hoc upravljanju z entitetami mimo politik hrambe.
- »sys:ret:rev:Schedules«: vrednosti predstavljajo unikatne identifikatorje politik hrambe, ki se bodo upoštevale v postopku priprave za odbiranje in izločanje.

V primeru, da imata oba atributa določene vrednosti, se postopek priprave odbiranja in izločanja prekliče, saj gre za neveljavno stanje.

Pomembno vlogo v postopku odbiranja in izločanja ima atribut »sys:ret:rev:Scope«.

Vrednost atributa je klasifikacijska oznaka entitete, pod katero se bo izvedlo iskanje vseh entitet, ki ustrezajo pogojem. Če vrednost atributa ni nastavljena se bo iskanje izvedlo po celotnem arhivu.

Pripravo postopka odbiranja in izločanja delimo na:

- Priprava glede na iskalni niz.
- Priprava glede na roke hrambe.

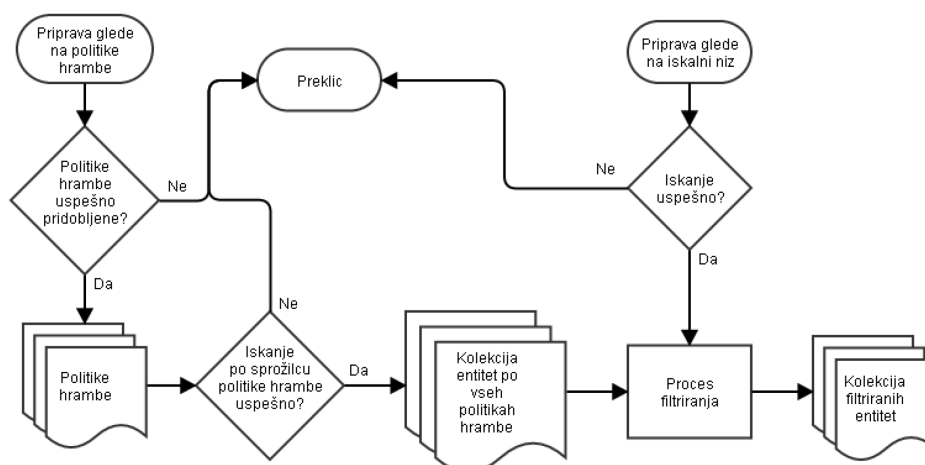
Pri postopku priprave glede na iskalni niz se izvede iskanje entitet, ki ustrezajo pogojem v iskalnem nizu. Rezultat je zbirka entitet, nad katero se izvede filtriranje. Filtriranje iz zbirke odstrani vse entitete, ki ne sodijo v postopek odbiranja in izločanja. Za več informacij glej poglavje [Postopek filtriranja](#). Iz filtrirane zbirke se nato izdelajo XML dokumenti z informacijami o entitetah in dovoljenih akcijah nad njimi, s katerimi lahko uporabniki s pravicami (člani komisije) upravljajo v postopku odločanja.

Pri postopku priprave glede na roke hrambe velja podobno. Iz vsake politike hrambe, ki je del postopka odbiranja in izločanja, se iz sprožilca vzame iskalni niz (vrednost atributa »sys:ret:pol:Trigger«) in izvede iskanje entitet. Ko je iskanje po vseh rokih hrambe končano, se zbirke vseh iskanj združijo v unijo, ki predstavlja zbirko entitet po vseh rokih hrambe. Ta zbirka gre skozi postopek filtriranja kjer se dodatno preveri, ali ima entiteta vsaj en efektiven rok hrambe, ki je del postopka odbiranja in izločanja.

Če ta pogoj ni izpolnjen, entiteta ne pripada trenutnemu postopku odbiranja in izločanja.

Na koncu se iz filtrirane zbirke izdelajo XML dokumenti z informacijami o entitetah in dovoljenimi akcijami, katere lahko uporabnik spreminja v postopku odločanja.

Če pri postopku priprave pride do kakršne koli napake (npr. neveljaven iskalni niz, izbrisana politika hrambe, ipd.) se postopek samodejno prekliče. Za ponovno pripravo je potrebno celoten postopek priprave ponoviti. V nadaljevanju je prikazan postopek priprave odbiranja in izločanja.



Slika 26: Priprava postopka odbiranja in izločanja

Po uspešno izvedenem postopku priprave se izdelajo XML dokumenti, ki predstavljajo vsebino postopka.

Ločimo dva tipa XML dokumentov:

- Dokumenti samo za branje (nahajajo se v atributu »sys:ret:rev:Lists«).
- Dokumenti, ki jih člani komisije v postopku odločanja spreminjajo (nahajajo se v atributu »sys:Content«).

Dokument samo za branje vsebuje poleg informacij o entiteti tudi nabor akcij, ki so dovoljene za izvajanje nad entiteto. Nabor akcij je odvisen od številnih dejavnikov, ki so podrobneje opisani v poglavju. Za več informacij glej poglavje [Postopek filtriranja](#). Dokumenti, katere člani komisije lahko spreminjajo v postopku odločanja vsebujejo poleg informacij o entiteti tudi privzeto akcijo in razlog.

### 3.7.2 Postopek odločanja pri odbiranju in izločanju

V postopku odločanja člani komisije sprejemajo odločitve, kaj se bo zgodilo z entitetami, ki so bile predmet postopka priprave. Člani komisije izberejo akcijo, ki je dovoljena za posamezno entiteto, dodajo komentar, spremenijo razlog za izbrano akcijo, ipd.

V primeru prenosa entitet v tretji arhivski sistem, lahko dodajo tudi referenco na prenesene entitete ali potrdijo uspešen prenos entitete. V kolikor uspešnega prenosa ne potrdijo, je uničenje entitet na strežniku zavrnjeno.

Po končanem postopku odločanja se postopek izvede ali prekliče.

V primeru izvedbe postopka, se vrednost atributa »sys:ret:rev:Action« postavi na »Zaključeno« (angl. Complete), kar je znak strežniku, da je postopek izveden.

V primeru preklica, se vrednost atributa postavi na »Zavržen« (angl. Discard), kar je znak strežniku za preklic postopka odbiranja in izločanja.

### 3.7.3 Izvedba postopka odbiranja in izločanja

Izvedbo postopka odbiranja in izločanja delimo na:

- Preklic postopka odbiranja in izločanja.
- Izvedba postopka odbiranja in izločanja.

Pri preklicu postopka odbiranja in izločanja:

- Strežnik vrednost atributa »sys:ret:rev:State« nastavi na »Zavržen« (angl. Discarded).
- Status se spremeni v »Zaprto« (angl. Closed).
- V atribut »sys:ret:rev:Message« se zapiše sporočilo, da je bil postopek odbiranja in izločanja preklican na zahtevo uporabnika.

Pri postopku izvedbe odbiranja in izločanja se najprej naložijo vse informacije o entitetah iz XML dokumentov, ki so samo za branje. Nato se izvede preverjanje po naslednjih postavkah:

- Oblika XML dokumentov mora ustrezati predpisani XSD shemi.
- Vse entitete iz XML dokumentov, ki so samo za branje morajo biti prisotne v spremenljivih XML dokumentih in obratno.
- Izbrane akcije na entitetah morajo ustrezati dovoljenim akcijam za te entitete.

Če je preverjanje katere koli postavke neuspešno, se postopek odbiranja in izločanja izvede z napako. Celoten postopek je potrebno ponoviti.

Izjema je preverjanje izbrane akcije na entitetah. V tem primeru se izvajanje prekine z napako. Stanje postopka odbiranja in izločanja se postavi na »InReview«. To omogoča uporabniku, da popravi izbrane akcije na entitetah in ponovi postopek. Po uspešnem preverjanju se nad zbirko entitet ponovno izvede postopek filtriranja. Za več informacij glej poglavje [Postopek filtriranja](#).

V nadaljevanju sledi še nekaj praktičnih primerov, zakaj lahko pride do prekinitve izvajanja akcij v postopku izvedbe odbiranja in izločanja.

*Primer 1: V postopku odbiranja in izločanja imamo poleg drugih entitet tudi zadevo z dvema vsebovanima zadevama:*

*F=2015-00011*

*F=2015-00011^F=00001*

*F=2015-00011^F=00002*

*V postopku odločanja je izbrana akcija »Dispose« za vse tri entitete. Člani komisije ugotovijo, da je na zadevo »F=2015-00011« vezano zadržanje postopka. Izvedba akcije je na vseh treh entitetah prekinjena, saj zadržanje postopka rekurzivno vpliva na vse vsebovane entitete. Akcija se izvede na vseh ostalih entitetah, ki so predmet postopka odbiranja in izločanja.*



Primer 2: Vzemimo kombinacijo iz prvega primera, le da sedaj na zadevo »F=2015-00011« ni vezano zadržanje postopka odbiranja in izločanja. Zadeva vsebuje novo zadevo »F=2015-00011^F=00003«, ki v postopku priprave postopka še ni obstajala:

F=2015-00011

F=2015-00011^F=00001

F=2015-00011^F=00002

F=2015-00011^F=00003

V tem primeru se akcija »Dispose« izvede na vsebovanih zadevah »F=2015-00011^F=00001« in »F=2015-00011^F=00002«, uničenje zadeve »F=2015-00011« pa ni mogoče, saj le ta vsebuje novo vsebovano zadevo »F=2015-00011^F=00003«, ki pa ni predmet postopka odbiranja in izločanja.

Če pride do napake pri izvajanju akcije na določeni entiteti, se izvedba akcije prekine na vseh nadrejenih entitetah, ki so del postopka odbiranja in izločanja.

Primer 3: Vzemimo kombinacijo iz prvega primera, pri čemer se v vsebovani zadevi »F=2015-00011^F=00002« nahajata dva dokumenta:

F=2015-00011^F=00002

F=2015-00011^F=00002^D=00001

F=2015-00011^F=00002^D=00002

Uporabnik, v imenu katerega se izvaja postopek odbiranja in izločanja nima pravice brisanja dokumenta »F=2015-00011^F=00002^D=00002«. Posledično se tudi vsebovana zadeva »F=2015-00011^F=00002« in njena nadrejena zadeva »F=2015-00011« ne uničita. Uniči pa se vsebovana zadeva »F=2015-00011^F=00001«.

Primer 4: Vzemimo kombinacijo iz prvega primera, kjer je akcija za vsebovanih zadevah »F=2015-00011^F=00001« in »F=2015-00011^F=00002« nastavljena na »Permanent«. Akcija na zadevi »F=2015-00011« je nastavljena na »Dispose«.

Ob uspešni izvedbi akcije »Premanent« je izvedba akcije »Dispose« neuspešna, saj zadeva »F=2015-00011« vsebuje dve vsebovani zadevi, ki se hranita trajno. Posledično se zadeva ni uniči.

Izvedba vseh akcij se zapiše v revizijsko sled (če je le ta omogočena), poleg tega pa se zapišejo še v ločeno poročilo. Poročilo je sestavljeno iz XML in tekstovnega dokumenta.

V XML dokumentu so zabeležene akcije na entitetah, ki so del postopka odbiranja in izločanja.

V tekstovnem dokumentu so zabeležene tudi akcije na entitetah, ki niso del postopka odbiranja in izločanja (dokumenti v zadevah). Takšne entitete so posredno odvisne, saj nadrejene entitete določajo akcije, ki se bodo na njih izvedle.

### 3.7.4 Postopek filtriranja

V postopku filtriranja se za celotno zbirko entitet preveri, ali ustrezajo vsem pogojem postopka odbiranja in izločanja. Iz postopka priprave se izločijo vse entitete (ter posledično tudi vse njihove nadrejene entitete), ki ustrezajo naslednjim pogojem:

- Uporabnik, v imenu katerega se izvaja postopek priprave nima pravice videti obstoja entitete.
- Na entiteti je prisotno vsaj eno zadržanje postopka odbiranja in izločanja.
- Entiteta ne vsebuje vsaj enega efektivnega roka hrambe, ki bi ustrezal naboru rokov hrambe, s katerimi se izvaja postopek priprave za odbiranje in izločanje.

V primeru postopka priprave odbiranja in izločanja po iskalnem nizu tega preverjanja ni.

- Entiteta vsebuje podrejene entitete, ki so predmet odbiranja in izločanja, vendar niso prisotne v zbirki entitet za trenutno pripravo odbiranja in izločanja.
- Entiteta ima vrednost atributa »sys:Significance« nastavljeno na »Delete«.

Vrednost atributa »sys:Significance« vpliva tudi na privzete akcije, ki se lahko izvajajo nad entiteto:

- Vrednosti »Vital« ali »Permanent« na entiteti: vplivajo na to, da se privzeta akcija postavi na »Permanent«. Uporabnik ne more izbrati druge akcije kot »Review«, saj atribut določa pomembnost entitete. Vrednost vpliva tudi na vse nadrejene entitete, ki se jim posledično spremeni privzeta akcija.
- Vrednost »Retain«: predstavlja opozorilo, da se mora entiteta ohraniti, zato se privzeta akcija nastavi na »Review«. Uporabnik ima možnost spremembe te akcije. Vrednost nima vpliva na nadrejene entitete.

Na privzeto akcijo entitete vplivajo tudi naslednji pogoji:

- Če ima entiteta več efektivnih rokov hrambe pomeni, da je entiteta v konfliktu. Privzeta akcija se postavi na »Review«. Uporabnik ima možnost izbire vseh akcij, ki so na voljo.
- Če entiteta vsebuje druge entitete, ki so že bile v drugih postopkih odbiranja in izločanja ter so postale trajno gradivo, se tudi dotični entiteti privzeta akcija postavi na »Permanent«. To velja tudi za vse nadrejene entitete. Uporabnik nima možnosti izbire druge akcije razen »Review«.

Če stanje entitete ne ustreza nobenemu zgoraj opisanemu pogoju, se privzeta akcija nastavi na vrednost, ki jo vsebuje politika hrambe, ki je za to entiteto veljavna. Uporabnik ima možnost izbire vseh akcij, ki so na voljo.

Postopek filtriranja se uporablja tudi pri postopku izvedbe odbiranja in izločanja.

V tem primeru se označijo entitete (ter posledično vse nadrejene entitete), nad katerimi se izbrane akcije zaradi različnih vzrokov ne smejo izvesti:

- Na entiteto je vezano vsaj eno zadržanje postopka odbiranja in izločanja.
- Med izvajanjem akcije na vsebovanih entitetah je prišlo do napake (npr.: uporabnik, v imenu katerega se izvaja postopek odbiranja in izločanja nima zadostnih pravic za izvedbo operacije, ipd).
- Stanje na strežniku ob izvedbi odbiranja in izločanja je drugačno od stanja ob pripravi postopka.

*Primer:* nove entitete, ki so predmet odbiranja in izločanja, niso pa prisotne v trenutnem postopku, ipd.

- Izbrane akcije so v konfliktu.

*Primer:* vsebovana zadeva ima izbrano akcijo »Review«, nadrejena zadeva pa akcijo »Dispose«. V tem primeru se izbrana akcija na zadevi ne more izvesti, ker vsebuje zadevo, ki se bo odbirala v drugem postopku odbiranja in izločanja.

### 3.7.5 XML format dokumentov

V postopku odbiranja in izločanja nastopajo naslednje vrste XML dokumentov:

- dokumenti samo za branje
- dokument za urejanje
- poročila.

#### 3.7.5.1 Sintaksa dokumentov samo za branje

Dokumenti samo za branje vsebujejo stanje na strežniku v postopku priprave za odbiranje in izločanje. Vsebujejo tudi informacije o entiteti (klasifikacijsko oznako, interni Id, naslov), veljavne akcije, razlog in efektivne roke hrambe, ki veljajo za to entiteto.

### 3.7.5.1.1 Etiketa »Review«

Etiketa predstavlja korenski element in vsebuje elemente iz spodnje tabele.

Ime XML elementa	Tip XML elementa	Obveznost
Header	Etiketa	Da
Entity	Etiketa	Ne

Tabela 30: XML elementi etikete "Review"

### 3.7.5.1.2 Etiketa »Header«

Etiketa vsebuje verzijo XML dokumenta, datum začetka postopka priprave odbiranja in izločanja, klasifikacijsko oznako entitete (predstavlja obseg iskanja entitet za postopek odbiranja in izločanja), akcije, ki so na voljo, vnaprej določene razloge ter identifikatorje vseh rokov hrambe. Elementi etikete so opisani v spodnji tabeli.

Ime XML elementa	Tip XML elementa	Obveznost
Version	Atribut	Da
StartDate	Atribut	Da
Scope	Atribut	Ne
Action	Etiketa	Da
Reason	Etiketa	Da
Schedule	Etiketa	Da

Tabela 31 XML elementi etikete "Header"

#### **Atribut »Version«**

Atribut predstavlja verzijo XML dokumenta.

#### **Atribut »StartDate«**

Atribut predstavlja datum in čas začetka priprave postopka odbiranja in izločanja.

#### **Atribut »Scope«**

Atribut predstavlja klasifikacijsko oznako entitete, pod katero se je izvedlo iskanje entitet v postopku priprave. Če atribut ni prisoten pomeni, da je bilo iskanje izvedeno po celotnem arhivu.

#### **Etikete »Action«**

Etikete predstavljajo nabor akcij, ki so na voljo v postopku izvedbe odbiranja in izločanja.

Etiketa ima obvezen atribut »Id«.

**Etikete »Reason«**

Etikete predstavljajo privzete razloge za akcije, ki se bodo izvršile nad entitetami. Etiketa ima obvezen atribut »Id«, ki predstavlja unikatni identifikator katerega naslavljajo druge etikete.

**Etikete »Schedule«**

Etikete vsebujejo »Id« politik hrambe za trenutni postopek odbiranja in izločanja. Te so učinkovite za posamezne entitete ter politike hrambe, nad katerimi se izvaja postopek priprave. Etiketa ima obvezen atribut »Id«, ki predstavlja unikatni identifikator katerega naslavljajo druge etikete.

**3.7.5.1.3 Etiketa »Entity«**

Etikete vsebujejo informacije o entiteti, ki je vključena v postopek odbiranja in izločanja.

Elementi etikete so opisani v spodnji tabeli.

Ime XML elementa	Tip XML elementa	Obveznost
Id	Atribut	Da
IdType	Atribut	Da
Type	Atribut	Da
Id85	Atribut	Da
Title	Atribut	Da
Action	Atribut	Da
Reason	Atribut	Ne
Schedule	Etiketa	Da

Tabela 32: XML elementi etikete "Entity"

**Atribut »Id«**

Atribut predstavlja identifikator entitete.

**Atribut »IdType«**

Atribut predstavlja tip identifikatorja entitete. Veljavne vrednosti so:

- »C«: identifikator je klasifikacijska oznaka
- »E«: identifikator je unikatni zunanji identifikator
- »I«: identifikator je interni identifikator entitete.

**Atribut »Type«**

Atribut predstavlja tip entitete. Veljavne vrednosti so:

- »C«: entiteta predstavlja razred
- »F«: entiteta predstavlja zadevo
- »D«: entiteta predstavlja dokument.

**Atribut »Id85«**

Atribut predstavlja interni »Id« entitete.

**Atribut »Title«**

Atribut predstavlja naslov entitete.

**Atribut »Action«**

Atribut je 32-bitna ne-predznačena vrednost, ki vsebuje informacije o veljavnih akcijah na entiteti ter privzeto akcijo za entiteto.

Prvi štirje biti vrednosti (od desne proti levi oz. z LSB strani) predstavljajo veljavne akcije in so opisani v spodnji tabeli. Če je vrednost bita »1«, je akcija dovoljena, v nasprotnem primeru akcija ni dovoljena.

Bit 3 – »Review«	Bit 2 – »Transfer«	Bit 1 – »Permanent«	Bit 0 – »Dispose«
------------------	--------------------	---------------------	-------------------

Tabela 33: Pozicija bitov ki predstavljajo dovoljene akcije

Naslednjih 24-bitov se ne uporablja. Vrednost v končnih 4-bitov predstavlja vrednost atributa »Id« v »Action« etiketi znotraj etikete »Header« in obenem privzeto akcijo za entiteto.

**Atribut »Reason«**

Atribut predstavlja referenco na atribut »Id« v »Reason« etiketah v etiketi »Header«, vrednost »Reason« pa predstavlja privzet razlog za odbiranje in izločanje entitete.

**Etiketa »Schedule«**

Etiketa vsebuje obvezen atribut »Id«, ki vsebuje referenco na atribut »Id« v »Schedule« etiketah v etiketi »Header«. Vrednost predstavlja interni identifikator za rok hrambe, ki je efektiven za entiteto.

Primer:

```

<Review>
  <Header StartDate="2015-08-17T18:14:19.170+02:00" Version="1">
    <Action Id="1">Dispose</Action>
    <Action Id="2">Permanent</Action>
    <Action Id="3">Transfer</Action>
    <Action Id="4">Review</Action>
    <Reason Id="R0">Razlog 1</Reason>
    <Reason Id="R1">Razlog 2</Reason>
    <Schedule
      Id="S0">0d5021dd60c06fc09fe42d6ac61a4434727e5a69d9253d5ed17ef84879e1996
    </Schedule>
    <Schedule
      Id="S1">098197cff3ea91e9feadfd2a629ec4ad0cf3d06e6025c616853a58363819c8f6
    </Schedule>
  </Header>
  <Entity Id="C=99" IdType="C" Type="C"
    Id85="jkh920856nvgbhd84ikfnbj2185hwqbo58djhn378jck085jd" Title="Legacy object containers"
    Action="536870927" Reason="R1">
    <Schedule Id="S1"/>
  </Entity>
  <Entity Id="C=04^F=2015-00012^F=00001" IdType="C" Type="F"
    Id85="b43ghjf983jxcgfsa6r9fhnnbnd84hfcfsk93e7tb184jshfg" Title="Review test"
    Action="536870927" Reason="R1">
    <Schedule Id="S1"/>
  </Entity>
</Review>

```

Vrednost atributa »Action« za entiteto »C=04^F=2015-00012^F=00001« je: 536870927.

Binarna reprezentacija je naslednja: 0010000000000000000000000000001111.

Na tej entiteti so vse akcije omogočene (vrednost prvih 4 bitov je 1111). Zadnji 4 biti nam dajo vrednost 0010 (2), kar je vrednost »Id« atributa za akcijo »Permanent«.

### 3.7.5.2 Sintaksa dokumentov za urejanje

Sintaksa XML dokumentov, ki se urejajo v postopku odločanja je zelo podobna dokumentom samo za branje. Vsebuje nekaj dodatnih atributov, ki se uporabljajo v postopku izvajanja odbiranja in izločanja.

#### 3.7.5.2.1 Etiketa »Review«

Etiketa predstavlja korenski element dokumenta in vsebuje elemente iz spodnje tabele.

Ime XML elementa	Tip XML elementa	Obveznost
Header	Etiketa	Da
Entity	Etiketa	Ne

Tabela 34: Elementi etikete »Review«

### 3.7.5.2.2 Etiketa »Header«

Etiketa vsebuje verzijo XML dokumenta, akcije, ki so na voljo in pripadajoči razlogi.

Elementi etikete so opisani v spodnji tabeli.

Ime XML elementa	Tip XML elementa	Obveznost
Version	Atribut	Da
Action	Etiketa	Da
Reason	Etiketa	Da

Tabela 35: Elementi etikete »Header«

#### **Atribut »Version«**

Atribut predstavlja verzijo XML dokumenta.

#### **Etiketa »Action«**

Etikete predstavljajo nabor akcij, ki so na voljo. Vsebujejo obvezen »Id« atribut, ki predstavlja referenco na akcijo, ki je izbrana za posamezno entiteto v postopku izvajanja odbiranja in izločanja.

#### **Etiketa »Reason«**

Etikete predstavljajo nabor vzrokov za izvedbo akcij nad entitetami v postopku izvajanja odbiranja in izločanja. Vsebujejo obvezen atribut »Id«, ki predstavlja referenco na vzrok, na katerega se posamezna entiteta sklicuje.

### 3.7.5.2.3 Etiketa »Entity«

Poleg atributov, ki se nanašajo na entiteto, etiketa vsebuje še izbrano akcijo in vzrok.

V primeru akcije »Transfer« je potrebno z atributom potrditi še uspešen prenos entitete.

Opcijsko se lahko vnese referenca na preneseno entiteto ter komentar.



Elementi etikete so opisani v spodnji tabeli.

Ime XML elementa	Tip XML elementa	Obveznost
Id	Atribut	Da
IdType	Atribut	Da
Action	Atribut	Da
Reason	Atribut	Da
TrfSucceed	Atribut	Ne
TrfRefId	Atribut	Ne
Comment	Atribut	Ne

Tabela 36: Elementi etikete »Entity«

Atributa »Id« in »IdType« predstavljata identifikator entitete in tip identifikatorja ter sta enaka kot v dokumentu samo za branje. Za več informacij glej poglavje [Sintaksa dokumentov samo za branje](#).

#### **Atribut »Action«**

Vrednost atributa je referenca na izbrano akcijo v etiketi »Header«.

#### **Atribut »Reason«**

Vrednost atributa je referenca na izbran razlog v etiketi »Header«.

#### **Atribut »TrfSucceed«**

V kolikor je atribut prisoten, ta vrednost atributa pove, ali je bil prenos entitete uspešen ali ne (vrednosti »True« ali »False«).

#### **Atribut »TrfRefId«**

Atribut vsebuje vrednost, ki predstavlja referenco na preneseno entiteto.

#### **Atribut »Comment«**

Atribut vsebuje komentar uporabnika, ki izvaja postopek odločanja.

Primer:

```

<Review>
  <Header Version="1">
    <Action Id="A0">Dispose</Action>
    <Action Id="A1">Permanent</Action>
    <Action Id="A2">Transfer</Action>
    <Action Id="A3">Review</Action>
    <Reason Id="R0">Razlog 1</Reason>
    <Reason Id="R1">Razlog 2</Reason>
  </Header>
  <Entity Id="C=99" IdType="C" Action="A2" Reason="R1" TrfSucceed="true" TrfRefId="IMiSARC-1-19274994839398576934758956949387485"/>
  <Entity Id="C=99^C=01" IdType="C" Action="A0" Reason="R1"/>
  <Entity Id="C=99^C=02" IdType="C" Action="A0" Reason="R1"/>
</Review>

```

V postopku odločanja se je zgodilo naslednje:

- Entiteti »C=99^C=01« in »C=99^C=02« sta označeni za uničenje (vrednost atributa »Action« je »A0, kar je referenca na akcijo »Dispose«).
- Entiteta »C=99« je bila uspešno prenesena (atribut »TrfSucceed« ima vrednost »true«). Vnesla se je tudi referenca na preneseno entiteto.

### 3.7.5.3 Sintaksa poročil

Poročila vsebujejo informacije o entiteti, izbrani akciji in informacijo, ali je bila izbrana akcija uspešno izvedena.

#### 3.7.5.3.1 Etiketeta »Report«

Etiketeta predstavlja korenski element in vsebuje elemente iz spodnje tabele.

Ime XML elementa	Tip XML elementa	Obveznost
Header	Etiketeta	Da
Entity	Etiketeta	Ne

Tabela 37: Elementi etikete »Report«

### 3.7.5.3.2 Etiketa »Header«

Etiketa vsebuje verzijo XML dokumenta in akcije, ki si bile izbrane za posamezno entiteto.

Elementi etikete so opisani v spodnji tabeli.

Ime XML elementa	Tip XML elementa	Obveznost
Version	Atribut	Da
Action	Etiketa	Da

Tabela 38: Elementi etikete »Header«

### **Etiketa »Action«**

Etikete predstavljajo nabor akcij, ki so na voljo. Vsebujejo obvezen »Id« atribut, ki predstavlja referenco na akcijo, ki je izbrana za posamezno entiteto v postopku izvajanja odbiranja in izločanja.

### 3.7.5.3.3 Etiketa »Entity«

Poleg atributov, ki se nanašajo na entiteto, etiketa vsebuje tudi izbrano akcijo in informacijo, ali je bila akcija uspešno izvedena. Elementi etikete so opisani v spodnji tabeli.

Ime XML elementa	Tip XML elementa	Obveznost
Id	Atribut	Da
IdType	Atribut	Da
Action	Atribut	Da
Error	Atribut	Ne
Message	Etiketa	Ne

Tabela 39: Elementi etikete »Entity«

Atributa »Id« in »IdType« predstavljata identifikator entitete in tip identifikatorja in sta enaka kot v dokumentu samo za branje. Za več informacij glej poglavje [Sintaksa dokumentov samo za branje](#).

### **Atribut »Action«**

Vrednost atributa je referenca na izbrano akcijo v etiketi »Header«.

### **Atribut »Error«**

Če je atribut prisoten ima vrednost »True«. To pomeni, da izbrana akcija na entiteti ni bila uspešno izvedena. Vzrok za napako je opisan v znački »Message«.

### **Atribut »Message«**

Če je značka prisotna vsebuje opis napake, ki se je zgodil na strežniku pri izvedbi akcije.

#### *Primer:*

```
<Report>
  <Header Version="1">
    <Action Id="A0">Dispose</Action>
    <Action Id="A1">Permanent</Action>
    <Action Id="A2">Transfer</Action>
    <Action Id="A3">Review</Action>
  </Header>
  <Entity Id="C=01^C=05" IdType="C" Action="A0"/>
  <Entity Id="C=01^C=06" IdType="C" Action="A0" Error="true">
    <Message>Access denied. Insufficient rights to disposed the entity.</Message>
  </Entity>
</Report>
```

*Iz poročila je razvidno, da je bila entiteta »C=01^C=05« uspešno uničena, pri entiteti »C=01^C=06« pa je prišlo do napake, saj uporabnik, v imenu katerega se je izvajal postopek odbiranja in izločanja nima pravice brisanja na tej entiteti.*

## **3.8 Imeniške storitve**

Imeniške storitve omogočajo delo z strežniškim imenikom, ki vsebuje registrirane uporabnike in uporabniške skupine. So pomemben del strežniške infrastrukture, saj nudijo podporo za naslednje postopke in operacije:

- Preverjanje istovetnosti (angl. Authentication).
- Pridobivanje informacij o registrirani entiteti v strežniškem imeniku preko atributov.
- Upravljanje z seznamom dostopnih pravic (angl. Access Control List - ACL).

### **Preverjanje istovetnosti**

Preverjanje istovetnosti je postopek, ki se izvede pri vzpostavitvi uporabniške seje.

Če je preverjanje uspešno, imeniška storitev potrdi identiteto uporabnika, ki se povezuje na strežnik IMiS®/ARChive Server. Identiteta uporabnika je potrjena, ko se uporabniške poverilnice (angl. User credentials) ujemajo s podatki v strežniškem imeniku. Poverilnice so preprosto rečeno skupina informacij, ki nedvoumno zagotovijo, da so avtentikacijski podatki, uporabljeni za izdelavo podatkov poverilnice enaki tistim, ki so bili uporabljeni za izdelavo podatkov v strežniški podatkovni bazi poverilnic.

Tako nek ključ ali geslo z matematičnimi postopki izdelava podatke poverilnice, ki strežniku zagotovijo, da so izdelane s ključem, ki ga je uporabnik uporabil pri zadnji spremembi poverilnic.

### **Pridobivanje informacij preko atributov**

Imeniške storitve omogočajo pridobivanje informacij o registriranih entitetah v strežniškem imeniku preko atributov. Pridobivajo se na podlagi unikatnega 32-bitnega identifikatorja, ki je dodeljen vsaki registrirani entiteti v strežniškem imeniku.

Na podlagi identifikatorja lahko pridobimo informacije kot so uporabniški račun, ime in priimek uporabnika, opis in drugi podatki imeniške entitete. Za več informacij glej poglavje [Vrste atributov](#).

### **Upravljanje s seznamom dostopnih pravic**

Seznam dostopnih pravic prav tako uporablja 32-bitni unikatni identifikator, kamor so vezane pravice in vloge. Imeniške storitve so povezovalni člen med entiteto v imeniku in pripadajočim unikatnim identifikatorjem.

Istočasno tudi razrešujejo uporabniške skupine, ki jim posamezni uporabniki pripadajo. Te podatke uporablja ACL pri računanju efektivnih pravic. Za več informacij glej poglavje [Efektivne pravice](#).

#### **3.8.1 Tipi**

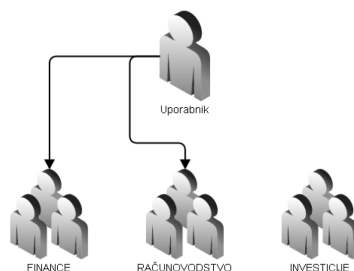
Strežniški imenik podpira dva tipa entitet:

- uporabnike
- uporabniške skupine.

### 3.8.1.1 Uporabniki

Uporabniki so osebe, ki dostopajo do informacij na strežniku. Uporabnike lahko poljubno umeščamo v uporabniške skupine brez omejitev.

*Primer:* Uporabnik pripada dvema skupinama: »FINANCE« in »RAČUNOVODSTVO«. Administrator lahko za posameznega uporabnika določi, ali je uporabnik aktiven ali neaktiven. Neaktivnim uporabnikom je vzpostavljane seje s strežnikom onemogočeno.

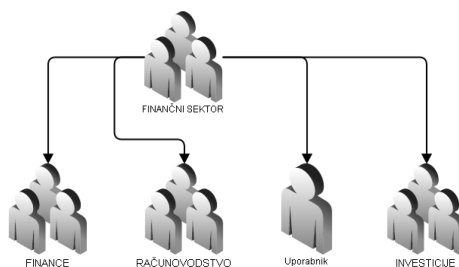


Slika 27: Pripadnost uporabnika v uporabniških skupinah

### 3.8.1.2 Uporabniške skupine

Uporabniške skupine so imeniške entitete, ki so jim dodeljene skupinske pravice na strežniku. S tem na lažji način kontroliramo dostop do posameznih dokumentov, razredov in zadev za večje število uporabnikov. Uporabniške skupine lahko poljubno gnezdimo, tudi rekurzivno. V primeru, da se pri razreševanju uporabniških skupin zazna rekurzija, potem se taka skupina preskoči, saj je njena vsebina že razrešena.

*Primer:* V uporabniški skupini »FINANČNI SEKTOR« so gnezdene skupine »FINANCE«, »RAČUNOVODSTVO« in »INVESTICIJE«, hkrati pa vsebuje tudi enega uporabnika.



Slika 28: Primer gnezdenja uporabniških skupin

### 3.8.2 Sistemsko določene entitete

Strežnik IMiS®/ARChive Server ima v svojem imeniku vnaprej določene naslednje sistemske ali navadne entitete:

- sys:Administrator
- sys:Administrators
- sys:CurrentUser
- sys:Server
- sys:Everyone
- Anonymous.

#### **Entiteta »sys:Administrator«**

Entiteta imenika predstavlja uporabnika, lokalnega administratorja s polnimi dostopnimi pravicami. Privzeto se nahaja v uporabniški skupini »sys:Administrators«.

Na strežniku je prepovedano nastavljanje vsakršnih pravic, povezanih s to entiteto.

#### **Entiteta »sys:Administrators«**

Entiteta imenika predstavlja uporabniško skupino s polnimi dostopnimi pravicami na strežniku. Prav tako kot za uporabnika »sys:Administrator«, je tudi za skupino prepovedano nastavljanje vsakršnih pravic, povezanih s to entiteto.

Če se uporabnik nahaja v tej uporabniški skupini, pravice te skupine prevladajo nad vsemi pravicami ostalih skupin v katerih se isti uporabnik še nahaja.

#### **Entiteta »sys:CurrentUser«**

Entiteta imenika predstavlja abstrakcijo uporabnika v strežniškem sistemu. Identifikator »sys:CurrentUser« se v postopku ustvarjanja nove entitete (razreda, zadeve ali dokumenta) zamenja z identifikatorjem uporabnika, ki ustvarja entiteto.

S tem uporabnik prevzame dovoljenja in prepovedi, ki postanejo eksplicitne za uporabnika na tej entiteti.

### **Entiteta »sys:Server«**

Entiteta imenika predstavlja strežniškega uporabnika, v imenu katerega se izvajajo strežniške storitve, kot je na primer servis za dolgoročno arhiviranje vsebin. Strežniškega uporabnika od drugih uporabnikov loči to, da se ga ne da uporabiti za prijavo na strežnik ter izvajanje operacij v njegovem imenu.

### **Entiteta »sys:Everyone«**

Entiteta imenika predstavlja uporabniško skupino, katere člani so vsi imeniški uporabniki, članstva v skupini pa se ne sme spreminjati. Za razliko od drugih sistemskih skupin se za to skupino lahko spreminjajo dostopne pravice, kar posledično pomeni, da se dostopne pravice spreminjajo tudi za vse imeniške uporabnike.

### **Entiteta »Anonymous«**

Entiteta imenika predstavlja uporabnika, ki se na strežnik povezuje s starejšimi odjemalci, ki ne podpirajo avtentikacije uporabnika. Takega uporabnika strežnik obravnava kot anonimnega in ima take dostopne pravice, kot so nastavljene za Anonymous entiteto.

## **3.8.3 Komponente entitete**

Komponente entitet v imeniških storitvah določajo lastnosti in tip entitet (uporabnike ali uporabniške skupine). Komponente z njihovimi opisi so predstavljene v nadaljevanju.

### **»Id«**

32-bitni unikatni identifikator, ki se samodejno dodeli vsaki entiteti v postopku njenega ustvarjanja in je nespremenljiv. Identifikator se uporablja tako za pridobivanje dodatnih informacij preko atributov, kot tudi pri računanju efektivnih dostopnih pravic v ACL.

### **»Type«**

8-bitna vrednost, ki predstavlja tip entitete v imeniških storitvah.

Veljavni vrednosti sta naslednji:

- TYPE\_GROUP: Vrednost predstavlja uporabniško skupino.
- TYPE\_USER: Vrednost predstavlja uporabnika.



**»Account«**

Znakovni niz je unikatna vrednost, ki predstavlja uporabniški račun ali ime uporabniške skupine. Vrednost se med življenjskim ciklom entitete ne more spreminjati. Največja velikost znakovnega niza je omejena s 256 zlogi UTF-8 znakov.

**»FirstName«**

Znakovni niz predstavlja ime uporabnika. Vrednost ni unikatna in se lahko med življenjskim ciklom entitete spreminja. Največja velikost znakovnega niza je omejena s 256 bajti UTF-8 znakov.

**»LastName«**

Znakovni niz predstavlja priimek uporabnika. Vrednost ni unikatna in se lahko med življenjskim ciklom entitete spreminja. Največja velikost znakovnega niza je omejena s 256 zlogi UTF-8 znakov.

**»Description«**

Znakovni niz predstavlja opis entitete. Vrednost ni unikatna in se lahko med življenjskim ciklom entitete spreminja. Največja velikost znakovnega niza je omejena s 256 zlogi UTF-8 znakov.

**»Email«**

Znakovni niz predstavlja elektronsko pošto uporabnika ali uporabniške skupine. Vrednost ni unikatna in se lahko med življenjskim ciklom entitete spreminja. Največja velikost znakovnega niza je omejena s 512 zlogi UTF-8 znakov.

### **»Flags«**

32 bitna ne-predznačena vrednost opisuje lastnosti entitete:

- Enabled: določa ali je uporabniški račun omogočen ali onemogočen.
- Deleted: določa ali je uporabnik ali skupina izbrisana.
- Locked: določa ali je uporabniški račun zaklenjen zaradi preseženega števila neuspešnih prijav.
- IdentityLinkingEnabled: določa, ali ima uporabnik pravico svoj račun povezati z identitetami pri drugih ponudnikih identitet (Google, Microsoft ...).
- AdvancedAuthenticationEnabled: določa, ali uporabniški račun omogoča avtentikacijo preko napredne avtentikacijske metode.
- PreSharedKeyAuthenticationEnabled: določa, ali uporabniški račun omogoča avtentikacijo preko napredne avtentikacijske metode s šifriranjem preko deljenega ključa.
- SRP6aAuthenticationEnabled: določa, ali uporabniški račun omogoča avtentikacijo preko SRP-6a avtentikacijske metode.
- ExternalAuthenticationEnabled: določa, ali uporabniški račun omogoča zunanjo avtentikacijo z LDAP in/ali Kerberos.
- HTTPAuthenticationEnabled: določa, ali uporabniški račun omogoča HTTP avtentikacijo.

### **»AuthenticationType«**

Številčna vrednost predstavlja tip avtentikacije, ki jo uporabnik lahko izbere za avtentikacijo na strežniku. Trenutno podprte vrednosti so:

- TYPE\_SRP6A predstavlja avtentikacijo na strežniku po SRP protokolu (angl. Secure Remote Password protocol).
- TYPE\_HTTPDIGEST predstavlja HTTP avtentikacijo za dostop do administracijskega vmesnika.
- TYPE\_EXTERN predstavlja zunanje avtentikacijske mehanizme kot sta LDAP in Kerberos.
- TYPE\_LINKED\_IDENTITY predstavlja povezano identiteto drugih ponudnikov identitet.

### **»SRP6Acredentials«**

Entiteti, ki predstavlja uporabnika se lahko dodeli poverilnico, ki je osnova za preverjanje avtentikacije uporabnika na strežniku. Parametra poverilnice sta znakovni niz v UTF-8 obliki, ki predstavlja uporabniško geslo in številčna vrednost, ki predstavlja SRP skupino.

Slednja določa uporabo praštevil v SRP protokolu. Za več informacij glej poglavje [SRP](#).

### **»SecurityClass«**

Številčna vrednost predstavlja stopnjo tajnosti, ki je nastavljena uporabniku ali uporabniški skupini. Ta določa dostop do entitet z nižjo ali enako stopnjo tajnosti.

Za več informacij glej poglavje [Dostopi](#).

### **»Icon«**

Binarni niz predstavlja sliko uporabnika ali skupine. Strežnik podpira naslednje formate slik:

- JPEG (angl. Joint Photographic Experts Group).
- PNG (angl. Portable Network Graphics).
- GIF (angl. Graphics Interchange Format).
- BMP (angl. Bitmap Image File).

### **»Delegates«**

Seznam registriranih uporabnikov (njihovih unikatnih identifikatorjev), ki se lahko v procesu avtentikacije predstavijo kot pooblašcene osebe za druge uporabnike, ter tako v njihovem imenu izvajajo operacije.

## **3.8.4 Sinonimi**

Strežnik omogoča uporabo sinonimov uporabniških računov. Funkcionalnost je uporabna, ko želimo povezati arhivski sistem z obstoječimi sistemi za avtentikacijo tretjih ponudnikov. Entiteti imenika lahko pripišemo poljubno število sinonimov, ki jih lahko uporabniki uporabljajo pri prijavi. Sinonim mora biti med sinonimi unikatna, prav tako ne sme ustrezati nobeni vrednosti atributa imeniške entitete »Account«.

## **3.8.5 Avtentikacija**

Avtentikacija uporabnika je del postopka, ki se izvede pri vzpostavljanju uporabniške seje z arhivskim strežnikom. Strežnik podpira dve vrsti avtentikacij:

- Avtentikacija s uporabo PAKE (angl. Password-Authenticated Key Agreement) protokola (SRP). Avtentikacijo s PAKE protokolom lahko uporabljajo vsi uporabniki (lokalni in sinhronizirani), če imajo poverilnice shranjene v podatkovni bazi strežnika.

V postopku avtentikacije IMiS®/ARChive Server preveri, ali se poverilnice, ki jih je poslal uporabnik ujemajo s poverilnicami, shranjenimi v podatkovni bazi strežnika.

- Avtentikacija z uporabo zunanjih servisov (Active Directory ...).  
V postopku avtentikacije zunanji servis preveri poverilnice ter sporoči strežniku, ali se poverilnice ujemajo ali ne.
- Avtentikacijo pri zunanjih ponudnikih identitet. Podprta protokola sta OIDC in SAML2.  
IMiS®/ARChive Server preveri veljavnost OIDC ali SAML2 žetonov, iz podatkov v žetonu sestavi povezano identiteto (ki jo je pred tem uporabnik moral povezati na svoj račun), ter avtenticira uporabnika, kateremu povezana identiteta pripada.

Če se ujemajo, je uporabnik dokazal istovetnost in lahko opravlja operacije na strežniku skladno z njegovimi pravicami. Če se poverilnice ne ujemajo, strežnik zavrne uporabniško sejo, saj uporabnik ni dokazal svoje verodostojnosti.

### **3.8.5.1 Avtentikacija z uporabo PAKE protokola**

Za postopek avtentikacije strežnik uporablja protokol SRP, ki je razširitev protokola PAKE (angl. Password-Authenticated Key Agreement).

PAKE protokol je interaktivna metoda, ki omogoča dvema ali več stranem, da vzpostavijo varni komunikacijski kanal, brez uporabe infrastrukture javnih ključev (PKI), samo s poznavanjem gesla ([http://en.wikipedia.org/wiki/Password-authenticated\\_key\\_agreement](http://en.wikipedia.org/wiki/Password-authenticated_key_agreement)).

PAKE protokol mora zadostovati naslednjim varnostnim zahtevam:

- Odpornost na pasiven napad s slovarjem (angl. Off-line dictionary attack resistance).
- Odpornost na aktiven napad s slovarjem (angl. On-line dictionary attack resistance).
- Prihodnjo tajnost (angl. Forward secrecy).
- Zaščita pred vplivanjem na druge seje (angl. Known-session security).

#### **Odpornost na pasiven napad s slovarjem**

Napadalec je lahko pasiven (lahko samo opazuje protokol) ali aktiven (aktivno spreminja podatke, prenesene po protokolu). V obeh primerih se po protokolu ne sme pošiljati nobenih podatkov (prstnih odtisov, gesla, ...), kar bi napadalcu omogočalo razkritje gesla s pomočjo mavričnih tabel (angl. Rainbow tables) ali z uporaba napada z grobo silo (angl. Brute force attack).

### **Odpornost na aktiven napad s slovarjem**

V primeru, da je napadalec aktiven (aktivno spreminja podatke, prenesene po protokolu), je praktično nemogoče napadalcu preprečiti, da bi naključno ugibal geslo. Kljub temu mora PAKE protokol zagotoviti, da je storjena najmanjša možna škoda v primeru, da napadalcu napad uspe (v primeru da je napad uspešen lahko napadalec ugame natanko eno geslo). Take vrste napadov se da preprosto zaznati na strežniku, ter jih preprečiti (npr. z zavrnitvijo vzpostavljanja seje z določene IP številke po določenem številu neuspešnih poizkusov avtentikacije).

### **Prihodnja tajnost**

Ker ni zagotovila, da bo geslo ostalo dolgoročno tajno, mora PAKE protokol zagotoviti zaščito preteklih sejnih ključev, tudi če se geslo razkrije. Poleg tega mora protokol tudi zagotoviti, da v primeru, ko napadalec pasivno opazuje izmenjavo ključev (angl. Key exchange), ne more uganiti sejnega ključa kljub temu, da pozna geslo.

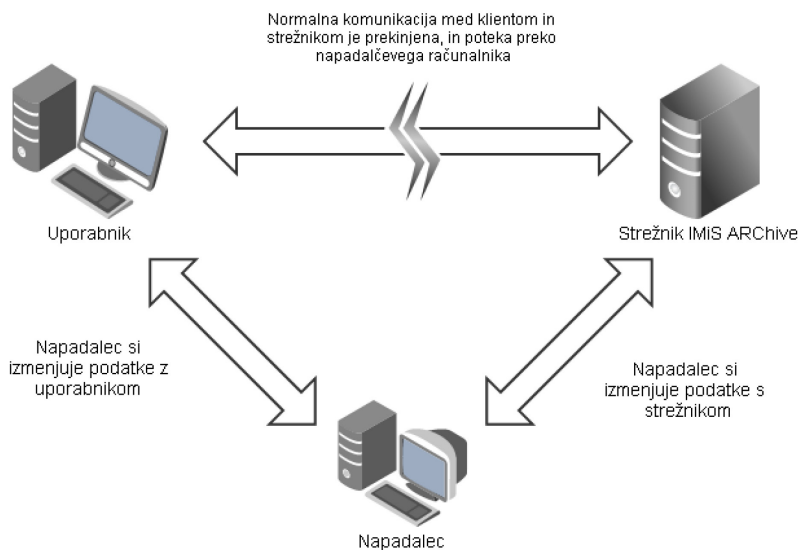
### **Zaščita pred vplivanjem na druge seje**

Če napadalcu uspe napad in vzpostavi sejo s strežnikom v imenu nekoga drugega (angl. Impersonation attack) se predvideva, da napadalec pozna celoten postopek vzpostavljanja seje (vključno z vsemi vmesnimi koraki, ki jih izvajata strežnik in odjemalec in niso javno znani, oziroma se ne pošiljajo po protokolu).

PAKE protokol mora omogočiti, da kompromitacija seje ne ogrozi varnosti drugih, že vzpostavljenih sej. Več informacij o PAKE protokolu je na voljo na spletnem naslovu <https://eprint.iacr.org/2010/190.pdf>.

#### **3.8.5.1.1 SRP**

SRP protokol je razširjena različica PAKE protokola, ki preprečuje vrinjenemu napadalcu (angl. Man-in-the-middle) pridobivanje informacij. S temi informacijami bi lahko z grobo silo uganil geslo, ne da bi aktivno spreminjal podatke, ki si jih izmenjujeta strežnik in odjemalec.



Slika 29: Primer napada na IMiS®/ARChive Server z vrinjenim napadalcem

Lastnosti SRP protokola so naslednje:

- Omogoča avtentikacijo na strežnik.
- Odporen je na napad s slovarjem.
- Ne potrebuje infrastrukture javnih ključev ter posledično ni potrebe po zaupanju vrednih tretjih osebah (angl. Trusted third party), kot so izdajatelji digitalnih potrdil.
- Odjemalec posreduje strežniku t.i. ničelni dokaz o poznavanju gesla (angl. Zero-knowledge password proof). To je interaktivna metoda, pri kateri odjemalec dokaže strežniku, da pozna vrednost gesla, ne da bi strežniku poslal kakršenkoli dokaz (prstni odtis gesla, ...) o vrednosti le-tega.

SRP (verzija 6) se uporablja pri /v:

- Zagotavljanju varnosti transportnega sloja (angl. Transport layer security – SRP verzijo opisuje povezava <http://en.wikipedia.org/wiki/TLS-SRP>).
- EAP protokolu (angl. Extensible authentication protocol –RFC 3748).
- SAML protokolu.

SRP je poleg tega še del standardov IETF (RFC 2944, RFC 2945, RFC 5054), IEEE (P1363.2) in ISO (IEC 11770-4).

### 3.8.5.1.2 Protokol

Vse matematične operacije v SRP protokolu so omejene na operacije, ki so določene znotraj matematičnega obroča (angl. Mathematical ring - [http://en.wikipedia.org/wiki/Ring\\_%28mathematics%29](http://en.wikipedia.org/wiki/Ring_%28mathematics%29)).

Parametri protokola so naslednji:

- $N$  – varno praštevilo, ki mora ustrezati formuli:  $N = 2 \times q + 1$ , kjer je  $q$  praštevilo. Praštevilo  $N$  določa velikost matematičnega obroča in je javno znana vrednost.
- $g$  – generator multiplikativne skupine (kombinacije  $g$  in  $N$  so opisane v RFC 5054 - <http://www.tools.ietf.org/html/rfc5054>).
- $H()$  – zgoščevalna funkcija.
- $k$  – množiteljski parameter, ki ustvari asimetrijo v SRP protokolu in s tem pripomore k odpornosti na aktiven napad.
- $s$  – naključna vrednost imenovana sol (angl. Salt, ki se uporablja pri ustvarjanju prstnega odtisa gesla; [http://en.wikipedia.org/wiki/Salt\\_%28cryptography%29](http://en.wikipedia.org/wiki/Salt_%28cryptography%29)).
- $I$  – uporabniško ime.
- $p$  – geslo v čistopisu.
- $x$  – privatni ključ.
- $v$  – strežniški verifikator.
- $u$  – mešalni parameter (angl. Scrambling parameter).
- $a, b$  – naključni števili, ki predstavljata kratko veljavna ključa.
- $A, B$  – javna parametra.
- $S$  – sejni ključ.
- $K$  – varen sejni ključ, ki je rezultat uspešne avtentikacije.
- $M_1$  – dokaz odjemalca o poznavanju gesla.
- $M_2$  – dokaz strežnika o poznavanju gesla.

Predpogoj za začetek avtentikacije s SRP protokolom je, da ima strežnik shranjen verifikator » $v$ «, s katerim bo preveril vsebino uporabniškega gesla. Za ustvarjanje verifikatorja je potreben privatni ključ » $x$ «, ki se izračuna na naslednji način:

$$x = H(s, p)$$

Pri računanju privatnega ključa uporabimo naključno vrednost » $s$ « in geslo v čistopisu. Vrednost in geslo združimo in izračunamo prstni odtis, ki predstavlja vrednost privatnega ključa.

Nato izračunamo strežniški verifikator po formuli:

$$v = g^x$$

Strežnik IMiS®/ARChive Server shrani verifikator skupaj z naključno vrednostjo » $s$ «, privatni ključ pa uniči, saj ga ne potrebuje več. Izračunan verifikator (skupaj z naključno vrednostjo) tako pripada natančno določenemu uporabniku, zato je potrebna povezava med verifikatorjem in uporabnikom, kateremu ta pripada. To funkcijo na strežniku opravlja imenik, oziroma imeniške storitve.

Sedaj se lahko izvede postopek avtentikacije. Najprej odjemalec in strežnik izračunata množiteljski parameter iz praštevila in generatorja multiplikativne skupine:

$$k = H(N, g)$$

Odjemalec začne avtentikacijo tako, da z varnim generatorjem naključnih števil ustvari naključno število » $a$ « in na podlagi tega izračuna vrednost parametra » $A$ «.

Nato uporabniško ime » $k$ « skupaj s parametrom » $A$ « pošlje strežniku.

Parameter » $A$ « se izračuna po naslednji formuli:

$$A = g^a$$

Strežnik prejme uporabniško ime in parameter » $A$ «, Nato s pomočjo imeniških storitev pridobi pripadajoč verifikator » $v$ « in naključno vrednost » $s$ «. Z varnim generatorjem naključnih števil izračuna vrednost » $b$ « in na podlagi tega izračuna parameter » $B$ «.

Nato se parameter » $B$ « skupaj z naključno vrednostjo » $s$ « pošlje strežniku.

Parameter » $B$ « se izračuna po naslednji formuli:

$$B = k \times v + g^b$$

Po prvi izmenjavi parametrov obe strani preverita veljavnost parametrov » $A$ « in » $B$ «.

Parametra sta veljavna, če ustrezata naslednjim kriterijem:

$$A \neq 0 \pmod{N} - \text{preverjanje na strežniku}$$

$$B \neq 0 \pmod{N} - \text{preverjanje na odjemalcu}$$

Če katerikoli izmed parametrov ne ustreza kriterijem, potem se postopek avtentikacije prekine.



Če parametra ustrežata kriterijem, se postopek avtentikacije nadaljuje s tem, da odjemalec in strežnik izračunata mešalni parameter » $u$ « po naslednji formuli:

$$u = H(A, B)$$

Mešalni parameter mora ustrezati kriteriju  $u \neq 0$ , sicer se postopek avtentikacije prekine.

V nadaljevanju avtentikacije odjemalec in strežnik izračunata vsak svoj dokaz o poznavanju gesla in varen sejni ključ » $K$ «.

#### Računanje varnega sejnega ključa na odjemalcu

Odjemalec iz vpisanega gesla » $p$ « in od strežnika prejete naključne vrednosti » $s$ «, izračuna privatni ključ » $x$ « po že znani formuli  $x = H(s, p)$ . Na podlagi privatnega ključa se izračuna sejni ključ » $S$ « in njegov prstni odtis » $K$ «, ki predstavlja varen sejni ključ. Računanje varnega sejnega ključa poteka po naslednjih formulah:

$$S = (B - k \times g^x)^{(a + u \times x)}$$

$$K = H(S)$$

#### Računanje varnega sejnega ključa na strežniku

Strežnik izračuna varen sejni ključ po naslednjih formulah:

$$S = (A \times v^u)^b$$

$$K = H(S)$$

Odjemalec prvi pošlje strežniku svoj dokaz o poznavanju gesla in o varnem sejnem ključu.

Dokaz je izračunan po naslednji formuli:

$$M_1 = H(H(N) \text{ xor } H(g), H(I), s, A, B, K)$$

Strežnik po enaki formuli izračuna svoj primer dokaz  $M_1$  tako, da v računanje vključi svojo vrednost varnega sejnega ključa » $K$ «. Vrednosti dokazov se morata ujemati, sicer je prišlo do napake pri avtentikaciji in strežnik zavrne sejo.

Če se vrednosti ujemata, potem strežnik izračuna svoj dokaz po naslednji formuli in ga pošlje odjemalcu:

$$M_2 = H(A, M_1, K)$$

Odjemalec po enaki formuli izračuna svoj primer dokaza  $M_2$ , kjer vključi svoj varen sejni ključ »K«. Če se vrednosti dokazov ne ujemata, potem je prišlo do napake pri avtentikaciji in odjemalec zavrne sejo. Če se dokaza ujemata, je avtentikacija uspela. Poleg uspešne avtentikacije pa imata odjemalec in strežnik še varen sejni ključ, ki ga lahko uporabita za šifriranje podatkov in tako vzpostavita varen transportni kanal.

### 3.8.5.2 Avtentikacija z zunanjim servisom

Avtentikacijo z zunanjim servisom lahko uporabljajo vsi uporabniki, ki so bili sinhronizirani v lokalni imenik iz oddaljenega imenika.

Podprte avtentikacijske metode z zunanjim servisom so naslednje:

- LDAP (angl. Lightweight Directory Access Protocol)
- Kerberos.

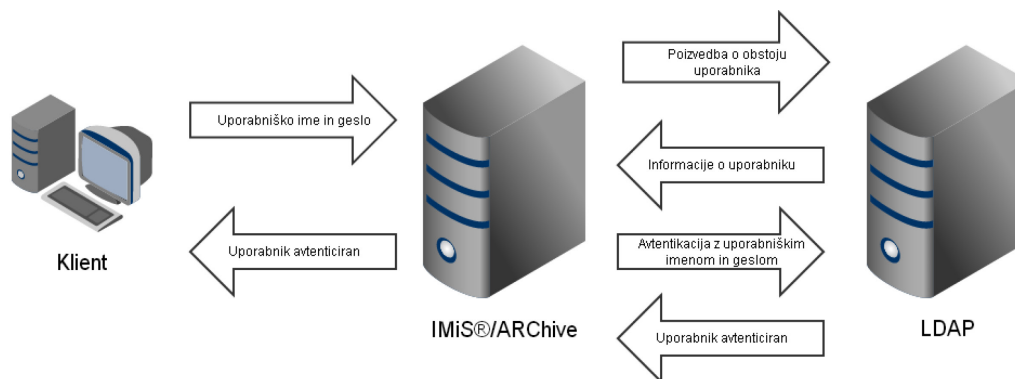
#### 3.8.5.2.1 LDAP

LDAP je aplikacijski protokol za dostop in vzdrževanje porazdeljenih imeniških storitev preko internetnega protokola. Protokol omogoča omrežni dostop do podatkov uporabnikov, skupin, servisov ter drugih entitet na centralnem strežniku. Podroben opis protokola je opisan v RFC 4511 (<https://www.ietf.org/rfc/rfc4511.txt>).

Postopek avtentikacije preko LDAP protokola poteka na strežniku po naslednjih korakih:

1. Odjemalec pošlje strežniku IMiS®/ARChive Server uporabniško ime in geslo za avtentikacijo.
2. Strežnik IMiS®/ARChive Server se poveže na LDAP strežnik ter naredi poizvedbo za uporabnika z uporabniškim imenom, ki ga je odjemalec poslal strežniku.
3. Če uporabnik na LDAP strežniku obstaja, ga strežnik IMiS®/ARChive Server poizkuša avtenticirati z uporabniškim imenom in geslom, ki ga je odjemalec poslal strežniku.
4. Uporabnik je avtenticiran, če je poslal pravilne poverilnice za LDAP strežnik.

Če se katerikoli izmed korakov ne izvede oz. se izvede z napako, potem uporabnik ni avtenticiran in seja s strežnikom IMiS®/ARChive Server ni vzpostavljena. Naslednja slika prikazuje uspešen postopek avtentikacije z uporabo LDAP strežnika.



Slika 30: LDAP avtentikacija

LDAP protokol (verzija 3) podpira naslednje tipe avtentikacije:

- Anonimni dostop (angl. Anonymous); pri povezavi na strežnik se avtentikacija ne izvede.
- Preprosta avtentikacija (angl. Simple); uporabniško ime in geslo se pošljeta v čistopisu.
- SASL avtentikacija (angl. Simple Authentication and Security Layer); protokol uporablja metodo »poziv-odziv« (angl. Challenge-response) za avtentikacijo ter vzpostavitev varne povezave za prenos podatkov.

Ker se uporabniško ime in geslo pri LDAP avtentikaciji pošiljata po mreži je priporočljivo, da se pošiljata po zavarovanem kanalu (angl. Secure Sockets Layer). S tem se izognemo napadu z vrinjenim napadalcem. Zavarovan kanal mora potekati med odjemalcem in strežnikom IMiS®/ARChive Server. V kolikor se za komunikacijo med strežnikom IMiS®/ARChive Server in LDAP strežnikom uporablja anonimni dostop ali preprosta avtentikacija, je priporočeno imeti zavarovan kanal tudi med njima.

### 3.8.5.2.2 Kerberos

Kerberos je omrežni avtentikacijski protokol, ki deluje na principu vstopnic (angl. tickets). Slednje omogočajo varno avtentikacijo po nezavarovanem mrežnem kanalu ter medsebojno avtentikacijo (angl. Mutual Authentication). To pomeni, da lahko odjemalec in strežnik, ki sodelujeta v avtentikacijskem procesu preverita identiteto drug drugega.

Za delovanje protokola je potrebna t.i. zaupanja vredna tretja stran (angl. Trusted Third Party). Ponavadi je to strežnik, ki izdaja s simetričnim ključem šifrirane vstopnice. Protokol je odporen proti prisluškovanju (angl. Eavesdropping) in napadom s ponovitvijo (angl. Replay Attack). Podrobno je obrazložen v specifikaciji RFC 4120 (<https://www.ietf.org/rfc/rfc4120.txt>).

Zaupanja vredna tretja stran je sestavljena iz avtentikacijske storitve (angl. Authentication Service) in storitve za podeljevanje vstopnic (angl. Ticket Granting Service ali TGS).

Obe storitvi skupaj sestavljata center za razdeljevanje ključev (angl. Key Distribution Center ali KDC). Avtentikacija klienta na IMiS®/ARChive strežnik po Kerberos protokolu poteka na naslednji način:

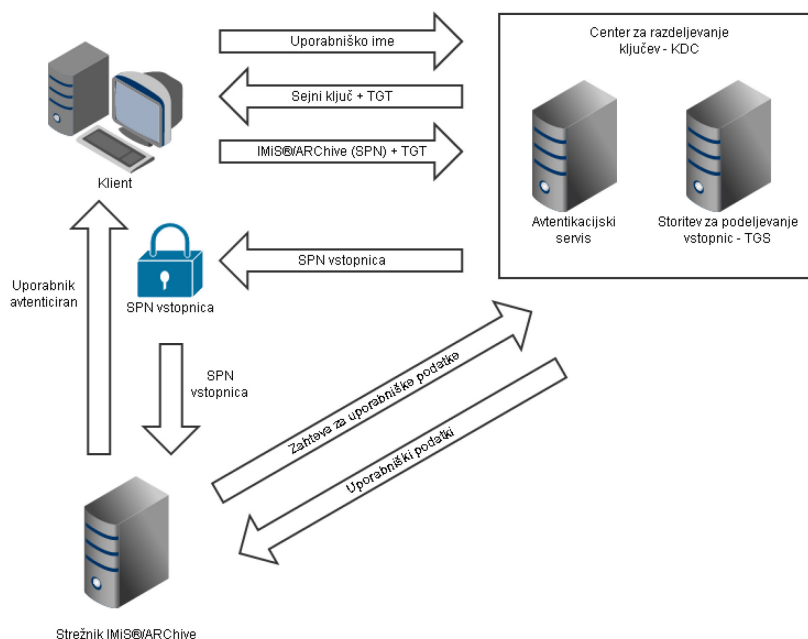
1. Uporabnik vpiše uporabniško ime in geslo v odjemalca, ki nato pošlje uporabniško ime v čistopisu centru za razdeljevanje ključev (KDC). Slednji preveri ali uporabnik obstaja in odjemalcu pošlje šifriran odgovor. Če je uporabnik pravilno vpisal geslo odjemalec odgovor dešifrira. Dešifrirani podatki vsebujejo TGS sejni ključ ter šifrirano vstopnico za podeljevanje vstopnic (angl. Ticket Granting Ticket ali TGT). Sejni ključ se nadalje uporablja za komunikacijo s TGS., TGT vstopnica pa se uporablja za zahteve po servisnih vstopnicah. Če je odjemalec uspešno dešifriral odgovor, je pridobil sejni ključ ter TGT. To je dovolj, da uspešno konča avtentikacijo.
2. Po uspešni avtentikaciji odjemalec zahteva vstopnico za strežnik IMiS®/ARChive Server. Strežnik na KDC pošlje zahtevek, ki vsebuje TGT vstopnico ter servisni indentifikator (angl. Service Principal Name ali SPN). Slednji predstavlja strežnik IMiS®/ARChive Server. KDC preveri obstoj SPN in pošlje šifrirano SPN vstopnico odjemalcu.
3. Odjemalec pošlje strežniku IMiS®/ARChive Server prejeto SPN vstopnico.
4. Strežnik IMiS®/ARChive Server preveri veljavnost vstopnice tako, da jo dešifrira s ključmi, ki so bili ustvarjeni ob registraciji SPN na KDC. Če dešifriranje vstopnice uspe, potem vstopnica pripada trenutnemu SPN. Naknadno strežnik preveri, ali se uporabnik ujema z uporabnikom, za katerega je bila SPN vstopnica narejena (podatke o uporabniku pridobi iz KDC). Če se uporabnik ujema pomeni, da je uporabnik uspešno avtenticiran na KDC. Prav tako je uspešno pridobil vstopnico za SPN kar pomeni, da se lahko avtenticira tudi na IMiS®/ARChive strežniku.

Kerberos protokol omogoča tudi t.i. enkratni vpis (angl. Single Sign On ali SSO).

Uporabnik se v domeno prijavi le enkrat. Ob prijavi pridobi TGT vstopnico, s katero zahteva vstopnice za različne SPN, ne da bi se od uporabnika zahtevalo ponovno vpisovanja gesla.

V primeru SSO vpisa se prvi korak pri avtentikaciji izpusti.

Naslednja slika prikazuje primer uspešne avtentikacije na strežnik IMiS®/ARChive Server z uporabo Kerberos protokola.



Slika 31: Kerberos avtentikacija

Pri Kerberos avtentikaciji je potrebno omeniti, da so vstopnice časovno omejene.

Zato je potrebno poskrbeti za časovno usklajenost KDC in SPN servisa. V nasprotnem primeru lahko pride do težav pri preverjanju SPN vstopnic ter posledično do avtentikacije.

### 3.8.5.3 Avtentikacija z zunanjim ponudnikom identitete

Zunanji ponudniki identitet so servisi, ki hranijo in upravljajo digitalne identitete (Google, Microsoft, Okta ...). Ponudniki identitet omogočajo prijavo uporabnikov kot storitev (angl. Identity provider as a service ali IDaaS). To pomeni, da se lahko uporabniki prijavijo v tretje sisteme preko prijave pri ponudniku identitete. Dodatno omogočajo enkratni vpis (angl. Single sign on ali SSO) kar pomeni, da se uporabnik enkrat prijavi pri ponudniku identitete, zatem pa transparentno dostopa do tretjih sistemov brez ponovnih prijav. Pogoji za transparentni dostop je vzpostavitev zaupanja med tretjim sistemom in ponudnikom identitete.

Na IMiS®/ARChive Server se to zaupanje vzpostavi s konfiguracijo vtičnikov, ki preverjajo žetone ponudnikov identitet.

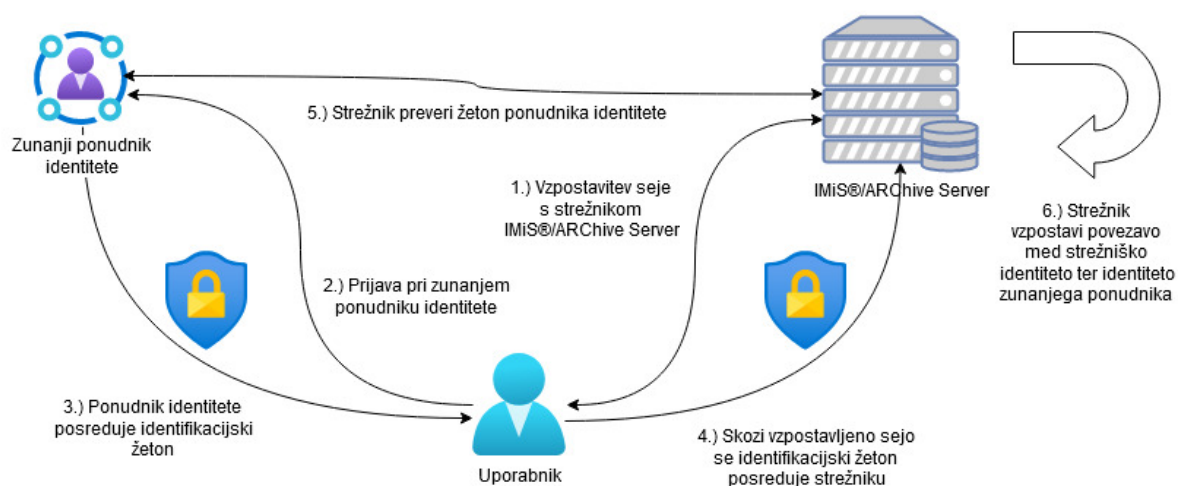
Podprti so naslednji formati žetonov:

- OIDC (angl. OpenID Connect).
- SAML2 (angl. Security Assertion Markup Language 2.0).

Da se lahko uporabnik prijavi na IMiS®/ARChive Server preko zunanjega ponudnika identitete, mora najprej identiteto na strežniku povezati z identiteto pri zunanjem ponudniku.

Postopek povezave je naslednji:

- Uporabnik se na IMiS®/ARChive Server prijavi z obstoječimi poverilnicami preko podprtih protokolov (SRP6A, Kerberos, LDAP ...).
- Če je uporabniku dovoljeno povezovanje identitet, se le-ta prijavi pri zunanjem ponudniku identitete. Pridobljen žeton v okviru obstoječe IMiS®/ARChive Server seje pošlje strežniku, da ga preveri. Po uspešnem preverjanju informacij v žetonu, strežnik na podlagi konfiguracije vtičnika ter informacij iz žetona sestavi identiteto, ter jo poveže z identiteto trenutno prijavljenega uporabnika.
- Uporabnik se lahko nato odjavi iz IMiS®/ARChive Server sistema, za ponovno prijavo pa lahko uporabi prijavo preko zunanjega ponudnika identitet.



Slika 32: Povezovanje identitet

Preverjanje identifikacijskega žetona vsebuje naslednje korake:

- Žeton mora biti elektronsko podpisan, elektronski podpis pa mora biti veljaven.
- Časovna veljavnost žetona mora biti v času preverjanja veljavna.
- Veljavni morajo biti vsi metapodatki, ki so zahtevani po standardu OIDC ([https://openid.net/specs/openid-connect-core-1\\_0.html](https://openid.net/specs/openid-connect-core-1_0.html)) ali SAML2 (<https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>).

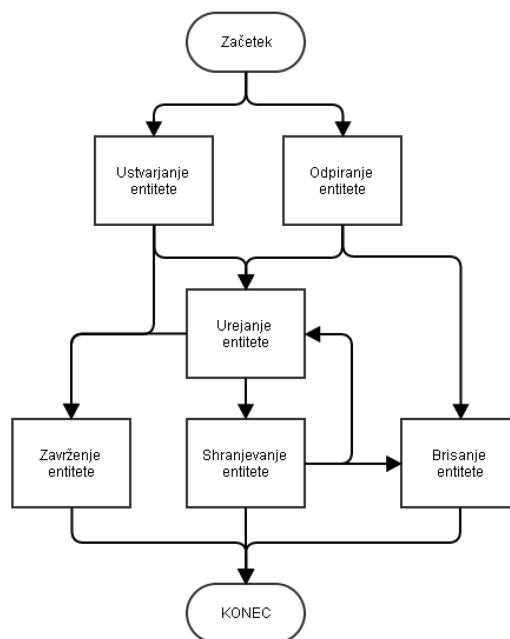
Administrator lahko vsakemu uporabniku kadarkoli dovoli ali prepove povezovanje identitet.

Vsako povezano identiteto lahko tudi onemogoči, omogoči ali izbriše. Uporabnik lahko povezane identitete ustvarja ali izbriše, če mu je to z nastavitvami dovoljeno.

### 3.8.6 Življenjski cikel entitet imenika

Življenjski cikel entitete v imeniških storitvah delimo na naslednje vrste postopkov:

- Ustvarjanje entitete imenika.
- Odpiranje entitete imenika.
- Urejanje entitete imenika.
- Shranjevanje entitete imenika.
- Zavrženje entitete imenika (angl. Discard).
- Brisanje entitete imenika.



Slika 33: Povezava med postopki v življenjskem ciklu entitete v imeniku

### 3.8.6.1 Ustvarjanje entitete imenika

Postopek ustvarjanja entitete imenika je prvi v življenjskem ciklu entitete. Na začetku se določi tip entitete in uporabniški račun ali ime uporabniške skupine, če gre za skupino.

V postopku urejanja lahko nastavimo še dodatne komponente glede na to, za kateri tip entitete gre. V primeru, da se novo ustvarjena entiteta imenika zavrže preden je le-ta shranjena, se vsebina imenika ne spremeni.

### 3.8.6.2 Odpiranje entitete imenika

Odpiranje entitete imenika je postopek pridobivanja primerka (angl. Instance) entitete iz imenika. Strežnik IMiS®/ARChive Server v postopku uvodne nastavitve (angl. Initialization) naloži vse entitete, ki se v imeniku nahajajo. Istočasno pri odpiranju entitete imenika preveri, če je entiteta predhodno naložena. V primeru da je naložena, vrne njen primerek, v nasprotnem primeru pa javi napako.

### 3.8.6.3 Urejanje entitete imenika

Urejanje entitete imenika je mogoče na novo ustvarjenih entitetah ter entitetah, ki so že v imeniku in niso v procesu sinhronizacije. Za več informacij glej poglavje [Sinhronizacija](#).

Pri urejanju entitet imenika se lahko nastavlja in spreminjajo komponente, ki so opisane v poglavju [Komponente entitete](#).



#### **3.8.6.4 Shranjevanje entitete imenika**

Shranjevanje entitete imenika je postopek kjer se vse vrednosti, ki smo jih ustvarili ali spremenili med urejanjem, shranijo v imenik.

#### **3.8.6.5 Zavrženje entitete imenika**

Do zavrženja entitete imenika pride, ko ne želimo shraniti novo ustvarjene entitete ali entitete v urejanju. V obeh primerih se vsebina imenika ne spremeni, saj v primeru urejanja entitete v imeniku ostane entiteta z zadnjimi shranjenimi vrednostmi, novo ustvarjena entiteta imenika pa pride v imenik le v primeru shranjevanja.

#### **3.8.6.6 Brisanje entitete imenika**

Uporabnik lahko briše entitete imenika le, če niso v procesu sinhronizacije. Za več informacij glej poglavje [Sinhronizacija](#). Brisanje entitete imenika poteka tako, da se entiteto v imeniku označi kot izbrisano, atributu »Account« se doda unikatni identifikator, ki omogoča ponovno registriranje entitete z isto »Account« vrednostjo, kot jo je imela entiteta pred izbrisom, fizično pa se entiteta ne izbriše. Tak uporabnik ali uporabniška skupina za strežnik ne obstaja več. Vseeno pa je potrebno ohraniti njihove 32-bitne identifikatorje za podporo atributov in zagotavljanja enoličnost 32-bitnih identifikatorjev, uporabljenih pri računanju efektivnih pravic v ACL.

### **3.8.7 Sinhronizacija**

Sinhronizacija internega strežniškega imenika je predpogoj za uporabo zunanjih avtentikacijskih metod, kot sta LDAP in Kerberos. Strežnik za sinhronizacijo uporablja koncept vtičnikov. Za več informacij glej poglavje [Vtičniki](#). Za vsakega ponudnika oddaljenih imeniških storitev (npr. Microsoft Active Directory, OpenLDAP, ...) uporabnik s pravico (administrator) registrira vtičnik in ga konfigurira za določenega ponudnika. Za pravilno delovanje vtičnikov in s tem sinhronizacije je potrebno nastaviti obvezne parametre za posamezen vtičnik. Natančni opisi vseh parametrov za posamezen tip vtičnika se nahajajo v poglavju [Vtičniki](#).

Obvezni parametri za generičen LDAP in Active Directory vtičnik:

- URL naslov do strežnika imeniške storitve.
- Uporabniško ime in geslo, v imenu katerega se bodo izvajale akcije na strežniku.  
Če je omogočen anonimni dostop, uporabniško ime in geslo nista potrebna).
- Osnovno razločevalno ime (angl. Base Distinguished Name ali BaseDN).  
S tem imenom se okvirno določi predel imenika, ki se bo sinhroniziral.  
Osnovno razločevalno ime ni obvezen podatek, vendar v kombinaciji z razločevalnimi imeni uporabnikov in skupin predstavlja ključno nastavitev za pravilno delovanje sinhronizacije.
- Razločevalno ime uporabnikov (angl. User Distinguished Name ali UserDN) in razločevalno ime skupin (angl. Group Distinguished Name ali GroupDN) nista obvezna podatka.  
Uporabljata se v primeru, ko želimo dodatno segmentirati sinhronizacijo uporabnikov in skupin glede na osnovno razločevalno ime.
- Filtri za iskanje uporabnikov in skupin v imeniku.
- V primeru, da se za dostop do oddaljenega imenika uporablja zaščiten kanal, je potrebno določiti še pot do shrambe certifikatov za vzpostavitev zaščitenega kanala.

Primeri uporabe razločevalnih imen:

- *BaseDN = »DC=example,DC=com«, UserDN in GroupDN nista nastavljena.*  
*Na osnovi nastavitev se bodo sinhronizirali vsi uporabniki in skupine, ki se nahajajo v BaseDN.*
- *BaseDN = »DC=example,DC=com«, UserDN = »OU=Users«, GroupDN ni nastavljen.*  
*Na osnovi nastavitev se bodo iskali vsi uporabniki pod »OU=Users,DC=example,DC=com«.*  
*Grupe se bodo iskale pod BaseDN, torej pod »DC=example,DC=com«.*
- *BaseDN = »DC=example,DC=com«, UserDN = »OU=Users«, GroupDN = »OU=Groups«.*  
*Na osnovi teh nastavitev se bodo iskali vsi uporabniki pod »OU=Users,DC=example,DC=com«,*  
*skupine pa pod »OU= Groups,DC=example,DC=com«.*

Primeri preprostih iskalnih filtrov za Microsoft Active Directory:

- *»(&(objectCategory=person)(objectClass=user))«.* Rezultat filtra so vsi objekti kategorije osebe in razreda uporabnik (vsi uporabniki).
- *»(objectCategory=group)«.* Rezultat filtra so vsi objekti kategorije skupine (vse skupine).

Obvezni parametri za generičen SQL vtičnik:

- Povezovalni niz (angl. Connection string), ki vsebuje podatke za povezavo do strežnika in baze (up. ime in geslo, ime baze ...).
- Ime gonilnika, kateri se bo uporabljal za komunikacijo s strežnikom (primer za MSSQL strežnik: com.microsoft.sqlserver.jdbc.SQLServerDriver).
- Filtri za iskanje uporabnikov ali skupin (SELECT stavek).
- Drugi parametri, ki so obvezni za posamezen SQL vtičnik in se jih posreduje skozi konfiguracijo (etiketa »Property«).

Ob sinhronizaciji iz oddaljenega imenika v lokalni strežniški imenik se vse entitete označijo kot sinhronizirane. Uporabnik s pravico (administrator) jih poveže še z ponudnikom imeniške storitve, s katero je bila entiteta sinhronizirana. Za več informacij glej poglavje [Komponente entitete](#).

Sinhronizacija uporabnikov in skupin je pogojena z naborom polj, ki so del sinhronizacije.

Sinhronizirana polja so spremenljiva samo skozi sinhronizacijo, tako da jih uporabnik s pravicami (administrator) ne more spreminjati.

Brisanje sinhroniziranih uporabnikov ali skupin prav tako ni dovoljeno, saj se le-ti ob sinhronizaciji posebej označijo kot sinhronizirani.

V kolikor želi uporabnik s pravicami spreminjati podatke o uporabnikih ali skupinah, izklopi posamezna polja v nastavitvah, ali pa v celoti izklopi sinhronizacijo za določenega uporabnika ali skupino, kar omogoča tudi izbris entitete.

### 3.8.8 Vtičniki

Vtičniki za imeniške storitve omogočajo sinhronizacijo ter avtentikacijo uporabnikov z zunanjimi servisi. Vtičnike lahko razdelimo v naslednje skupine:

- Vtičnik za Active Directory.
- Generičen LDAP vtičnik.
- Generičen SQL vtičnik.
- Generičen SOAP vtičnik.

Vtičnik za Active Directory omogoča sinhronizacijo in avtentikacijo (LDAP, Kerberos) uporabnikov z Microsoft Active Directory.

Generičen LDAP vtičnik omogoča sinhronizacijo tudi z drugimi servisi (OpenLDAP... ) ter samo LDAP avtentikacijo.

Generičen SQL vtičnik omogoča sinhronizacijo z SQL bazami podatkov (MySQL, MSSQL ...), ne omogoča pa avtentikacije uporabnikov.

Generičen SOAP vtičnik omogoča sinhronizacijo s SOAP servisi, ne omogoča pa avtentikacije uporabnikov.

Uporabnik s pravicami konfigurira vtičnike preko XML zapisa, ki se nahaja znotraj »Arguments« etikete. Vsaka konfiguracija mora vsebovati etiketo »Class«, ki predstavlja ime razreda, kjer je vtičnik implementiran.

Vrednosti so naslednje:

- com.imis.imisarc.server.aaa.impl.ActiveDirectory;
- com.imis.imisarc.server.aaa.impl.GenericLdapConnector
- com.imis.imisarc.server.aaa.impl.GenericSQLConnector.
- com.imis.imisarc.server.aaa.impl.GenericSoapConnector;

Konfiguracija vtičnikov je sestavljena iz obveznih in opsijskih parametrov.

Obvezni parametri za generičen LDAP in Active Directory vtičnik so:

- URL naslov do strežnika imeniške storitve.
- Uporabniško ime in geslo, v imenu katerega se bodo izvajale akcije na strežniku.  
Če je omogočen anonimni dostop, uporabniško ime in geslo nista potrebna.
- Osnovno razločevalno ime (angl. Base Distinguished Name ali BaseDN).  
S tem imenom se okvirno določi predel imenika, ki se bo sinhroniziral.  
Osnovno razločevalno ime ni obvezen podatek, vendar v kombinaciji z razločevalnimi imeni uporabnikov in skupin predstavlja ključno nastavitev za pravilno delovanje sinhronizacije.
- Razločevalno ime uporabnikov (angl. User Distinguished Name ali UserDN) in razločevalno ime skupin (angl. Group Distinguished Name ali GroupDN) nista obvezna podatka.  
Uporabljata se v primeru, ko želimo dodatno segmentirati sinhronizacijo uporabnikov in skupin glede na osnovno razločevalno ime.

- Filtri za iskanje uporabnikov in skupin v imeniku.
- V primeru, da se za dostop do oddaljenega imenika uporablja zaščiten kanal, je potrebno določiti še pot do shrambe certifikatov za vzpostavitev zaščitenega kanala.

Primeri uporabe razločevalnih imen:

- *BaseDN = »DC=example,DC=com«, UserDN in GroupDN nista nastavljena.*  
*Na osnovi nastavitve se bodo sinhronizirali vsi uporabniki in skupine, ki se nahajajo v BaseDN.*
- *BaseDN = »DC=example,DC=com«, UserDN = »OU=Users«, GroupDN ni nastavljen.*  
*Na osnovi nastavitve se bodo iskali vsi uporabniki pod »OU=Users,DC=example,DC=com«.*  
*Skupine se bodo iskale pod BaseDN, torej pod »DC=example,DC=com«.*
- *BaseDN = »DC=example,DC=com«, UserDN = »OU=Users«, GroupDN = »OU=Groups«.*  
*Na osnovi teh nastavitvev se bodo iskali vsi uporabniki pod »OU=Users,DC=example,DC=com«, skupine pa pod »OU= Groups,DC=example,DC=com«.*

Primeri preprostih iskalnih filtrov za Microsoft Active Directory:

- *»(&(objectCategory=person)(objectClass=user))«.* Rezultat filtra so vsi objekti kategorije osebe in razreda uporabnik (vsi uporabniki).
- *»(objectCategory=group)«.* Rezultat filtra so vsi objekti kategorije skupine (vse skupine).

Obvezni parametri za generičen SQL vtičnik:

- Povezovalni niz (angl. Connection string), ki vsebuje podatke za povezavo do strežnika in baze (uporabniško ime in geslo, ime baze ...).
- Ime gonilnika, kateri se bo uporabljal za komunikacijo s strežnikom (primer za MSSQL strežnik: com.microsoft.sqlserver.jdbc.SQLServerDriver).
- Filtri za iskanje uporabnikov ali skupin (SELECT stavek).
- Drugi parametri, ki so obvezni za posamezen SQL vtičnik in se jih posreduje skozi konfiguracijo (etiketa »Property«).

Obvezni parametri za generičen SOAP vtičnik:

- Etiketeta »SoapClient« mora vsebovati ime razreda, kjer je implementacija SOAP odjemalca.
- Etiketeta »<Property key='endpoint'>« mora vsebovati URL storitve.
- Drugi parametri, ki so obvezni za posamezen SOAP odjemalec in se jih posreduje skozi etikete »Property« in »PropertyArray«.

Ostalo konfiguracijo vtičnikov lahko razdelimo v tri skupine:

- Konfiguracija LDAP vtičnikov.
- Konfiguracija SQL vtičnikov.
- Konfiguracija preslikovalnih polj.

### 3.8.8.1 Konfiguracija LDAP vtičnikov

V nadaljevanju so predstavljene tabele z etiketami, ki so skupne LDAP in Active Directory, sledi tabela z etiketami za Active Directory vtičnik.

Ime etikete	Opis
LdapURL	Pot do ldap/ldaps strežnika.
LdapUsername	Uporabnik, v imenu katerega bo vtičnik izvajal poizvedbe na strežniku.
LdapPassword	Uporabniško geslo.
LdapAuthenticationType	Tip ldap avtentikacije: NONE, SIMPLE, DIGEST-MD5, CRAM-MD5
LdapBaseDN	Osnovno razločevalno ime.
LdapUserDN	Razločevalno ime uporabnikov.
LdapGroupDN	Razločevalno ime skupin.
LdapUserObjectFilter	Filter za iskanje uporabnikov (glede na osnovno razločevalno ime ter razločevalno ime uporabnikov).
LdapGroupObjectFilter	Filter za iskanje skupin (glede na osnovno razločevalno ime ter razločevalno ime skupin).
LdapReadTimeout	Časovna omejitev branja odgovora iz strežnika (vrednost v milisekundah).
LdapQueryTimeout	Časovna omejitev izvajanja poizvedbe na strežniku (vrednost v milisekundah).
LdapPageSize	Število rezultatov poizvedbe na eni strani pri uporabi odstranjevanja.

Ime etikete	Opis
LdapRecursiveQueries	»True« za rekurzivne poizvedbe, sicer »false«.
SSLSType	Tip shrambe digitalnih potrdil v primeru, da se uporablja ldap preko ssl.
SSLTSFile	Pot do datoteke, ki predstavlja shrambo digitalnih potrdil.
SSLTSPassword	Geslo za odklepanje shrambe digitalnih potrdil.
SSLProtocols	Podprti ssl protokoli (ločeni z vejico).
LdapAuthenticationFilter	Filter za ldap avtentikacijo uporabnikov.

Tabela 40: Skupne konfiguracijske etikete LDAP vtičnikov

Ime etikete	Opis
KrbServicePrincipal	Servisni indikator za Kerberos.
KrbKeytabLocation	Lokacija Kerberos keytab datoteke.
KrbDebugMode	»True« za Kerberos debug mode, drugače »False« (debug mode omogoča podroben zapis avtentikacije v log).
AccountAliasList	<p>Etiketa se uporablja za nastavitve Active Directory vrednosti za sinhronizacijo »Account« komponente ter sinonimov. Za več informacij glej poglavje <a href="#">Sinonimi</a>. Privzeto se »Account« vrednost entitete sinhronizira z vrednostjo »sAMAccountName« polja, sinonimi se ne sinhronizirajo. Vrednosti v etiketi so ločene z vejico. Prva vrednost predstavlja polje za sinhronizacijo z »Account« komponento, ostale vrednosti pa predstavljajo sinonime. Etiketo lahko priredimo sinhronizaciji uporabnikov ali skupinam tako, da določimo atribut »scope«, ki ima lahko vrednosti »user« ali »group« (če atribut ni prisoten velja tako za uporabnike kot tudi za skupine).</p> <p><i>Primer:</i></p> <pre>&lt;AccountAliasList&gt;sAMAccountName,userPrincipalName&lt;/AccountAliasList&gt;</pre> <p>»Account« takega uporabnika se bo nastavil na vrednost »sAMAccountName« polja, sinonim pa bo vrednost »userPrincipalName« polja.</p>

Tabela 41: Konfiguracijske etikete Active Directory vtičnika

### 3.8.8.2 Konfiguracija SQL vtičnikov

V nadaljevanju je predstavljena tabela z etiketami, katere se lahko uporablja za konfiguracija SQL vtičnikov.

Ime etikete	Opis
ConnectionString	Niz, ki vsebuje informacije o strežniku ter kako se na strežnik povezati. <i>Primer:</i> <code>&lt;ConnectionString&gt;jdbc:sqlserver://localhost:1433;databaseName=testdb &lt;/ConnectionString&gt;</code>
SqlDriver	Ime razreda, kjer je implementiral SQL gonilnik. <i>Primer:</i> <code>&lt;SqlDriver&gt;com.microsoft.sqlserver.jdbc.SQLServerDriver&lt;/SqlDriver&gt;</code>
UserQuery	Predstavlja SQL stavek ali klic procedure, ki se izvede ob sinhronizaciji uporabnikov. Tip se določi z atributom »type«, ki je lahko nastavljen na vrednost »QUERY« ali »PROCEDURE«.
GroupQuery	Predstavlja SQL stavek ali klic procedure, ki se izvede ob sinhronizaciji skupin.
PageSize	Število rezultatov poizvedbe na eni strani pri uporabi odstranjevanja.
ReadOnlyConnection	»True« če bo vtičnik uporabljal read-only povezave, drugače »False«
Property	Značka predstavlja »ključ« - »vrednost« kombinacijo, in je namenjena dodatni konfiguraciji SQL gonilnika. Ključ predstavlja atribut »key«, vrednost pa je kar vrednost značke. <i>Primer:</i> <code>&lt;Property key="user"&gt;sql_user&lt;/Property&gt;</code>

Tabela 42: Konfiguracijske etikete SQL vtičnikov

### 3.8.8.3 Konfiguracija SOAP vtičnikov

V nadaljevanju je predstavljena tabela z etiketami, ki se uporabljajo za konfiguracijo SOAP vtičnikov.

Ime etikete	Opis
SoapClient	Ime razreda, kjer je implementiran SOAP odjemalec. <i>Primer:</i> <code>&lt;SoapClient&gt;com.imis.imisarc.server.aaa.impl.soap.client.TestniSoapOdjemalec &lt;/SoapClient&gt;</code>



Property	<p>Značka predstavlja »ključ« - »vrednost« kombinacijo, in je namenjena konfiguraciji SOAP odjemalca. Ključ predstavlja atribut »key«, vrednost pa je vrednost značke.</p> <p><i>Primer:</i> <code>&lt;Property key='endpoint'&gt;http://localhost/testniSoapStreznik&lt;/Property&gt;</code></p>
PropertyArray	<p>Podobno kot »Property« etiketa tudi ta predstavlja »ključ« - »vrednost« kombinacijo, le da omogoča nastavljanje več vrednosti enemu ključu.</p> <p><i>Primer:</i></p> <pre>&lt;PropertyArray key='nastavitev1'&gt;a&lt;PropertyArray&gt; &lt;PropertyArray key='nastavitev1'&gt;b&lt;PropertyArray&gt; &lt;PropertyArray key='nastavitev1'&gt;c&lt;PropertyArray&gt;</pre> <p><i>S to konfiguracijo smo nastavili »nastavitev1« na vrednosti »a, b, c«.</i></p> <p><i>Zaporedje vrednosti v polju je enaka zaporedju podanih nastavitev.</i></p>

Slika 34: Konfiguracijske etikete SOAP vtičnikov

### 3.8.8.4 Konfiguracija preslikovalnih polj

Preslikovalna polja so pogoj za pravilno delovanje generičnih vtičnikov. Preslikovalna polja določajo, kako se bodo podatki iz generičnih vtičnikov (in njihovih implementacij) preslikali v polja entitete na strežniku. Administrator lahko določi tudi svoje ključe, ki pa morajo biti unikatni. Če preslikava ni določena v konfiguraciji, vtičnik vrne privzeto vrednost. Naslednja tabela prikazuje povezave med ključi in komponentami entitete ter njihove privzete vrednosti, v kolikor preslikava ni določena.

Ključ	Komponenta entitete	Privzeta vrednost
sys:dir:Account	Account	Prazen niz.
sys:dir:FirstName	FirstName	Prazen niz.
sys:dir:LastName	LastName	Prazen niz.
sys:dir:Description	Description	Prazen niz.
sys:dir:Email	Email	Prazen niz.
sys:dir:UUID	Vrednost je interna in se uporablja kot unikatni indentifikator za sinhronizacijo.	Prazen niz.
sys:dir:SecurityClass	SecurityClass	Vrednost »0«.

Ključ	Komponenta entitete	Privzeta vrednost
sys.dir:Icon	Icon	Prazen niz.
sys.dir:Delegates	Delegates	Prazen seznam
sys.dir:Aliases	Vrednost nastavlja sinonime (poglavje <a href="#">Sinonimi</a> ).	Prazen seznam vrednosti.
sys.dir:GroupMembers	Vrednost je interna in se uporablja pri sinhronizaciji in razreševanju članstva v skupinah (vrednost se uporablja samo pri sinhronizaciji skupin).	Prazen seznam vrednosti.
sys.dir:Flags:Enabled	Flags.Enabled	True.
sys.dir:Flags:Locked	Flags.Locked – vrednost se sinhronizira samo za uporabnike	False.
sys.dir:Flags:AuthExt	Flags.ExternalAuthenticationEnabled - - vrednost se sinhronizira samo za uporabnike	True
sys.dir:Flags:AuthHTTP	Flags. HTTPAuthenticationEnabled -- vrednost se sinhronizira samo za uporabnike	False
sys.dir:Flags:AuthSRP6A	Flags. SRP6aAuthenticationEnabled -- vrednost se sinhronizira samo za uporabnike	False
sys.dir:Flags:AuthPSK	Flags. PreSharedKeyAuthenticationEnabled - - vrednost se sinhronizira samo za uporabnike	False
sys.dir:Flags:AuthAdv	Flags. AdvancedAuthenticationEnabled -- vrednost se sinhronizira samo za uporabnike	False

Tabela 43: Konfiguracija preslikovalnih polj

Vsaki preslikavi moramo določiti tip preslikave (atribut »type«), le-ta pa naprej določa, kako se bodo podatki v vtičniku obdelali, preden jih vtičnik posreduje sinhronizaciji. Opcijsko lahko z atributom »scope« navedemo, ali velja preslikava samo za sinhronizacijo uporabnikov, skupin ali pa obojega (če atribut ni naveden velja za oboje). Naslednja tabela prikazuje tipe preslikav z njihovimi opisi.

Tip preslikave	Opis
STRING	Vrednost je predstavljena kot niz in se ne obdeluje.
BINARY	Vrednost se kodira v Base64.
BITFIELD	Vrednost se obdela glede na vrednost »typeExt«, rezultat je bodisi »true« ali »false«.
BOOLEAN	Vrednost se obdela glede na vrednost »typeExt«, rezultat je bodisi »true« ali »false«.
INT	Vrednost se obdela glede na vrednost »typeExt«, rezultat je število v desetiški obliki.
EXPRESSION	Vrednost predstavlja izraz za evaluacijo, ki se glede na »typeExt« evaluira v niz ali seznam nizov.
LDAP_AUTHENTICATION	Vrednost se uporablja za LDAP avtentikacijo in ni predmet preslikave.
DISTINGUISHED_NAME	Vrednost predstavlja razločevalno ime in se ne obdeluje.
SQLQUERY	Vrednost predstavlja SQL poizvedbo, katere rezultat se bo evaluiral v niz ali seznam nizov.
SQLPROC	Vrednost predstavlja SQL proceduro, katere rezultat se bo evaluiral v niz ali seznam nizov.

Tabela 44: Tipi preslikav

Vsak tip preslikave, katerega vrednost lahko obdelamo, lahko razširimo z atributom »typeExt«, v katerem naštejemo operacije, ki naj se zgodijo nad vrednostmi. Naslednja tabela prikazuje seznam podprtih operacij za povezovalne tipe.

Rezervirane vrednosti »typeExt«	Opis
MASK	Decimalna številka vrednost, ki se uporablja pri »maskiranju« (izvajanje AND operacije).
RDX	Osnova za številčno pretvorbo.
OFF	Predstavlja pozicijo bita za testiranje (začetni bit je na poziciji 0).
VAL	Seznam vrednosti, ki predstavljajo vrednost »true« (vrednosti so ločene z #).
NEG	»True« negira vrednost, drugače »false«.
DEL	Vrednost predstavlja ločitveni niz za ločevanje vrednosti v EXPRESSION tipu preslikave.
REMEMPTY	»True« pomeni, da se prazni nizi odstranijo iz seznama rezultatov, drugače »false«.
TRIM	»True« pomeni, da se nizi v seznamu rezultatov obrežejo (odstranijo se jim začetni in končni presledki), drugače »false«.
AGRKEY	Vrednost »true« označuje, da je vrednost polja del agregacijskega ključa, ki je uporablja za interno odstranjevanje pri SQL poizvedbah.
SQLCOL	Vrednost predstavlja ime SQL stolpca, iz katerega se bo bralo podatke.

Tabela 45: Vrednosti »typeExt« atributa

Vsak tip preslikave ima omejen nabor »typeExt« vrednosti, katere se izvajajo v določenem vrstnem redu. Vrednosti za vsak tip preslikave in vrstni red so predstavljene v naslednji tabeli, vse »typeExt« vrednosti so opsijske, če ni drugače navedeno.

Tip preslikave	Vrednosti »typeExt« in vrstni red izvajanja
STRING	TRIM, REMEMPTY
BINARY	TRIM, REMEMPTY
BITFIELD	RDX, OFF (obvezno), NEG, TRIM, REMEMPTY
BOOLEAN	VAL (obvezno), NEG, TRIM, REMEMPTY
INT	NEG, MASK, TRIM, REMEMPTY
EXPRESSION	DEL, TRIM, REMEMPTY
LDAP_AUTHENTICATION	/

Tip preslikave	Vrednosti »typeExt« in vrstni red izvajanja
DISTINGUISHED_NAME	/
SQLQUERY	SQLCOL (obvezno), TRIM, REMEMPTY
SQLPROC	Tip preslikave ni podprt za polja

Tabela 46: Vrstni red izvajanja "typeExt" glede na tip preslikave

Vrednost vsakega polja generičnega vtičnika lahko še dodatno obdelamo z uporabo skriptnega programskega jezika Javascript. Strežnik IMiS®/ARChive Server uporablja vgrajen Nashorn pogon (<https://www.oracle.com/technical-resources/articles/java/jf14-nashorn.html>), ki je del Java izvajalnega okolja.

Skripto lahko izvajamo na dva načina:

1. Z definicijo atributa »preScript« v konfiguraciji polja se skripta izvede, ko se vrednost polja preslika glede na tip preslikave.
2. Z definicijo atributa »script« v konfiguraciji polja se skripta izvede ob koncu evaluacije vseh polj, ki so navedene v konfiguraciji.

Vrstni red izvajanja Javascript kode in vgrajenih preslikav je naslednji:

1. Izvedba vgrajene preslikave glede na tip preslikave.
2. Izvedba skriptnega programa, določenega v atributu »preScript«.
3. Izvedba skriptnega programa, določenega v atributu »script«.

Omejitve pri izvajanju Javascript kode:

- Dvopičje v imenih preslikovalnih polj se v Javascript kodi nadomesti s podčrtajem (»sys:dir:Account« se v Javascript kodi naslavlja kot »sys\_dir\_Account«).
- Rezultat izvajanja Javascript kode mora biti niz ali polje nizov (drugi tipi niso podprti).

### 3.8.8.5 Primeri konfiguracije

Sledi par primerov konfiguracije vtičnikov. Primer konfiguracije generičnega LDAP vtičnika za izvajanje sinhronizacije z ActiveDirectory strežnikom predstavlja naslednja xml struktura:

```
<Arguments>
  <Class>com.imis.imisarc.server.aaa.impl.GenericLdapConnector</Class>
  <LdapURL>ldap://pot.do.primarnega.streznika</LdapURL>
  <LdapURL>ldap://pot.do.sekundarnega.streznika</LdapURL>
  <LdapUsername>uporabniskoime</LdapUsername>
  <LdapPassword>geslo</LdapPassword>
  <LdapAuthenticationType>simple</LdapAuthenticationType>
  <LdapBaseDN>dc=my-domain,dc=com</LdapBaseDN>
  <LdapUserDN>u=Userji</LdapUserDN>
  <LdapGroupDN>ou=Grupe</LdapGroupDN>
  <LdapUserObjectFilter>(objectClass=user)</LdapUserObjectFilter>
  <LdapGroupObjectFilter>(objectClass=group)</LdapGroupObjectFilter>
  <LdapReadTimeout>12000</LdapReadTimeout>
  <LdapQueryTimeout>6000</LdapQueryTimeout>
  <LdapPageSize>256</LdapPageSize>
  <LdapRecursiveQueries>true</LdapRecursiveQueries>
  <LdapAuthenticationFilter>(&,(objectCategory=person)(objectClass=user)((
userPrincipalName=%s)(mail=%s)(sAMAccountName=%s)))</LdapAuthenticationFilter>
  <Field key="sys:dir:Account" type="string">sAMAccountName</Field>
  <Field key="sys:dir:FirstName" type="string">givenName</Field>
  <Field key="sys:dir:LastName" type="string">sn</Field>
  <Field key="sys:dir:Description" type="string">description</Field>
  <Field key="sys:dir:Email" type="string">mail</Field>
  <Field key="sys:dir:UUID" type="binary">objectGUID</Field>
  <Field key="sys:dir:Flags:Enabled" type="bitfield" typeExt="OFF=1,
NEG=true">userAccountControl</Field>
  <Field key="sys:dir:Flags:Locked" type="boolean" typeExt="VAL=0,NEG=true"
scope="user">lockoutTime</Field>
  <Field key="sys:dir:Aliases" type="string">distinguishedName</Field>
  <Field key="sys:dir:GroupMembers" type="string" scope="group">member</Field>
</Arguments>
```

Primer konfiguracije generičnega SQL vtičnika za izvajanje sinhronizacije z MySQL strežnikom (uporaba SSL s strežniško hrambo certifikatov):

## &lt;Arguments&gt;

```

<Class>com.imis.imisarc.server.aaa.impl.GenericSQLConnector</Class>
<ConnectionString>jdbc:mysql://pot.do.streznika:3306/baza</ConnectionString>
<SqlDriver>com.mysql.cj.jdbc.Driver</SqlDriver>
<UserQuery type="query">SELECT * FROM directoryEntity WHERE type = "U"</UserQuery>
<GroupQuery type="query">SELECT * FROM directoryEntity WHERE type = "G"</GroupQuery>
<PageSize>256</PageSize>
<Property key="user">uporabnikoime</Property>
<Property key="password">geslo</Property>
<Property key="serverTimezone">UTC</Property>
<Property key="useSSL">>true</Property>
<Property key="verifyServerCertificate">>true</Property>
<Property key="trustCertificateKeyStoreUrl">file:///iarc/work/aaa/dummy_file</Property>
<Property key="trustCertificateKeyStoreType">IAKS</Property>
<Field key="sys.dir:Account" type="string">account</Field>
<Field key="sys.dir:FirstName" type="string">first_name</Field>
<Field key="sys.dir:LastName" type="string">last_name</Field>
<Field key="sys.dir:UUID" type="binary">uuid</Field>
<Field key="sys.dir:Flags:Enabled" type="boolean" typeExt="VAL=1">enabled</Field>
<Field key="sys.dir:Flags:Locked" type="boolean" typeExt="VAL=1">locked</Field>
<Field key="sys.dir:DistinguishedName" type="string">id</Field>
<Field key="sys.dir:Aliases" type="sqlquery" typeExt="sqlcol=alias" scope="user">SELECT * FROM
directoryEntityAlias WHERE dirId = "%sys.dir:DistinguishedName%"</Field>
<Field key="sys.dir:GroupMembers" type="sqlquery" scope="group"
typeExt="sqlcol=directoryId">SELECT directoryId FROM directorygroupmembership WHERE groupId =
(SELECT id FROM directoryentity WHERE account = "%sys.dir:Account%")</Field>
</Arguments>

```

Sledijo primeri različnih konfiguracij preslikovalnih polj. Naslednja tabela prikazuje uporabnike na OpenLDAP strežniku z atributi in njihovimi vrednostmi.

Atribut »cn«	Atribut »telephoneNumber«	Atribut »postalCode«	Atribut »uidNumber«	Atribut »homeDirectory«
test4	00000010	FF	6666	/home/test4
test5	133546	1234321	63361	/home/test5
test6	54321	11112222	62784	/home/test6

Tabela 47: Primer uporabniških atributov in njihove vrednosti

**Primer 1:** Preprosta konfiguracija, kjer se »cn« preslika v »sys\_dir:Account«, »homeDirectory« v »sys:dir:Description«, »uidNumber« v »sys:dir:UUID«, »telephoneNumber« v »sys:dir:Email« in »postalCode« kot »sys:dir:LastName«.

<Arguments>

```
<Field key="sys:dir:Account" type="string">cn</Field>
<Field key="sys:dir:Description" type="string">homeDirectory</Field>
<Field key="sys:dir:UUID" type="string">uidNumber</Field>
<Field key="sys:dir:Email" type="string">telephoneNumber</Field>
<Field key="sys:dir:LastName" type="string">postalCode</Field>
```

</Arguments>

**Primer 2:** Konfiguracijo iz prvega primera spremenimo tako, da »sys:dir:Description« tipiziramo kot »BINARY«, »uidNumber« pa kot »INT« v šestnajstiški obliki, pretvorbo v desetiški sistem izvedemo tako, da v »typeExt« določimo RDX=16.

<Arguments>

```
<Field key="sys:dir:Account" type="string">cn</Field>
<Field key="sys:dir:Description" type="binary">homeDirectory</Field>
<Field key="sys:dir:UUID" type="int" typeExt="RDX=16">uidNumber</Field>
<Field key="sys:dir:Email" type="string">telephoneNumber</Field>
<Field key="sys:dir:LastName" type="string">postalCode</Field>
```

</Arguments>

Rezultati pretvorbe za posameznega uporabnika so prikazani v naslednji tabeli.

Uporabnik	»sys:dir:Description«	»sys:dir:UUID«
test4	L2hvbWUvdGVzdDQ=	26214
test5	L2hvbWUvdGVzdDU=	406369
test6	L2hvbWUvdGVzdDY=	403332

Tabela 48: Rezultati pretvorbe (Primer 2)



**Primer 3:** Konfiguraciji iz prvega primera dodamo preslikavo za »distinguishedName«, ki jo tipiziramo kot »DISTINGUISHED\_NAME«.

<Arguments>

```
<Field key="sys:dir:Account" type="string">cn</Field>
<Field key="sys:dir:Description" type="string">homeDirectory</Field>
<Field key="sys:dir:UUID" type="string">uidNumber</Field>
<Field key="sys:dir:Email" type="string">telephoneNumber</Field>
<Field key="sys:dir:LastName" type="string">postalCode</Field>
<Field key="distinguishedName" type="DISTINGUISHED_NAME"/>
```

</Arguments>

Rezultati pretvorbe za posameznega uporabnika so prikazani v naslednji tabeli.

Uporabnik	»distinguishedName«
test4	uid=test4,ou=Userji,dc=my-domain,dc=com
test5	uid=test5,ou=Userji,dc=my-domain,dc=com
test6	uid=test6,ou=Userji,dc=my-domain,dc=com

Tabela 49: Rezultati pretvorbe (Primer 3)

**Primer 4:** Konfiguraciji iz prejšnjega primera spremenimo preslikavo za »sys:dir:UUID« tako, da uporabimo »EXPRESSION«, ki ga sestavimo iz »distinguishedName«, »sys:dir:Description« ter »uidNumber« (povezuje jih pomišljaj). Ker »uidNumber« ne moremo direktno naslavljati, določimo novo preslikavo z unikatnim ključem (npr. »uid-stevilka«), tak ključ pa nato uporabimo v definiciji izraza.

<Arguments>

```
<Field key="sys:dir:Account" type="string">cn</Field>
<Field key="sys:dir:Description" type="string">homeDirectory</Field>
<Field key="distinguishedName" type="DISTINGUISHED_NAME"/>
<Field key="uid-stevilka" type="string">uidNumber</Field>
<Field key="sys:dir:UUID" type="expression">%distinguishedName%-%sys:dir:Description%-%uid-
stevilka%</Field>
<Field key="sys:dir:Email" type="string">telephoneNumber</Field>
<Field key="sys:dir:LastName" type="string">postalCode</Field>
```

</Arguments>

Rezultati pretvorbe za posameznega uporabnika so prikazani v naslednji tabeli.

Uporabnik	»sys:dir:UUID«
test4	uid=test4,ou=Userji,dc=my-domain,dc=com-/home/test4-6666
test5	uid=test5,ou=Userji,dc=my-domain,dc=com-/home/test5-63361
test6	uid=test6,ou=Userji,dc=my-domain,dc=com-/home/test6-62784

Tabela 50: Rezultati pretvorbe (Primer 4)

*Primer 5:* Uporabnike, ki imajo »homeDirectory« na ldap strežniku nastavljene na »/home/test4« ali »/home/test5« bi radi onemogočili. Konfiguraciji iz prejšnjega primera dodamo preslikavo za »sys:dir:Flags:Enabled«, kjer navedemo željene vrednosti, končni rezultat pa negiramo.

<Arguments>

<Field key="sys:dir:Account" type="string">cn</Field>

<Field key="sys:dir:Description" type="string">homeDirectory</Field>

<Field key="distinguishedName" type="DISTINGUISHED\_NAME"/>

<Field key="uid-stevilka" type="string">uidNumber</Field>

<Field key="sys:dir:UUID" type="expression">%distinguishedName%- %sys:dir:Description%- %uid-stevilka%</Field>

<Field key="sys:dir:Email" type="string">telephoneNumber</Field>

<Field key="sys:dir:LastName" type="string">postalCode</Field>

<Field key="sys:dir:Flags:Enabled" type="boolean"

typeExt="VAL=/home/test4#/home/test5,NEG=true">homeDirectory</Field>

</Arguments>

*Primer 6:* Uporabnikom iz prejšnjega primera dodamo sinonime tako, da dodamo preslikavo za »sys:dir:Aliases«. Če želimo več sinonimov, potem preslikavo določimo kot »EXPRESSION«, kjer mu v »typeExt« določimo ločitveni znak (DEL). Tak izraz se bo najprej razdelil na pod-izraze glede na ločitveni znak, nato pa se bo vsak pod-izraz ovrednotil. Pogoji za uspešno ovrednotenje celotnega izraza je ta, da ima vsak pod-izraz enako število rezultatov.

<Arguments>

<Field key="sys:dir:Account" type="string">cn</Field>

<Field key="sys:dir:Description" type="string">homeDirectory</Field>

<Field key="distinguishedName" type="DISTINGUISHED\_NAME"/>

<Field key="uid-stevilka" type="string">uidNumber</Field>

<Field key="sys:dir:UUID" type="expression">%distinguishedName%-%sys:dir:Description%-%uid-stevilka%</Field>

<Field key="sys:dir:Email" type="string">telephoneNumber</Field>

<Field key="sys:dir:LastName" type="string">postalCode</Field>

<Field key="sys:dir:Flags:Enabled" type="boolean"

typeExt="VAL=/home/test4#/home/test5,NEG=true">homeDirectory</Field>

<Field key="sys:dir:Aliases" type="expression"

typeExt="DEL=#">%sys:dir:DistinguishedName%#%sys:dir:Description%#%uid-stevilka%</Field>

</Arguments>

*Primer 7:* Prikazan je primer konfiguracije za sinhronizacijo uporabnikov in skupin z Microsoft Active Directory.

<Arguments>

<Field key="sys:dir:Account" type="string">sAMAccountName</Field>

<Field key="sys:dir:FirstName" type="string">givenName</Field>

<Field key="sys:dir:LastName" type="string">sn</Field>

<Field key="sys:dir:Description" type="string">description</Field>

<Field key="sys:dir:Email" type="string">mail</Field>

<Field key="sys:dir:UUID" type="binary">objectGUID</Field>

<Field key="sys:dir:DistinguishedName" type="string">distinguishedName</Field>

<Field key="sys:dir:Flags:Enabled" type="bitfield"

typeExt="OFF=1,NEG=true">userAccountControl</Field>

<Field key="sys:dir:Flags:Locked" type="boolean" typeExt="VAL=0,NEG=true"

scope="user">lockoutTime</Field>

<Field key="sys:dir:Aliases" type="string">userPrincipalName</Field>

<Field key="sys:dir:GroupMembers" type="string" scope="group">member</Field>

</Arguments>

**Primer 8:** Prikazan je primer konfiguracije za sinhronizacijo uporabnikov in skupin s testno implementacijo generičnega SOAP odjemalca.

```

<Arguments>
  <Class>com.imis.imisarc.server.aaa.impl.GenericSoapConnector</Class>
  <SoapClient>com.imis.imisarc.server.aaa.impl.soap.client.TestniSoapOdjemalec</SoapClient>
  <Field key="sys:dir:Account" type="expression"
scope="user">%sys:dir:FirstName%_%sys:dir:LastName%</Field>
  <Field key="sys:dir:Account" type="string" scope="group">ROLE_NAME</Field>
  <Field key="sys:dir:FirstName" type="string" scope="user">FIRST_NAME</Field>
  <Field key="sys:dir:LastName" type="string" scope="user">LAST_NAME</Field>
  <Field key="sys:dir:Email" type="string" typeExt="remempty=true,trim=true"
scope="user">EMAIL</Field>
  <Field key="sys:dir:Flags:Enabled" type="string">IS_ACTIVE</Field>
  <Field key="sys:dir:Aliases" type="string" typeExt="REMEMPTY=true,trim=true"
scope="user">EMAIL</Field>
  <Field key="sys:dir:GroupMembers" type="string" scope="group">ROLE_MEMBERSHIP</Field>
  <Property key="endpoint">http://localhost/testniSoapStreznik</Property>
  <PropertyArray key="user_fieldName">firstName</PropertyArray>
  <PropertyArray key="user_fieldValue">User1</PropertyArray>
  <PropertyArray key="user_fieldValue">User2</PropertyArray>
  <PropertyArray key="user_fieldValue">User3</PropertyArray>
  <PropertyArray key="group_fieldName">roleName</PropertyArray>
  <PropertyArray key="group_fieldValue">administrators</PropertyArray>
  <PropertyArray key="group_fieldValue">Users</PropertyArray>
  <Property key="method_query_user">getUsers</Property>
  <Property key="method_query_group">getGroups</Property>
</Arguments>

```

**Primer 9:** Prikazan je primer izseka konfiguracije za sinhronizacijo uporabnikov, kjer se LDAP vrednosti »sAMAccountName« polja doda pripona z vrednostjo »test«:

```
<Arguments>
...
<Field key="ad:accountName" type="string" scope="user">sAMAccountName</Field>
<Field key="sys:dir:Account" type="expression" scope="user" preScript="var tmp =
sys_dir_Account[0]; tmp += ' test'; tmp;">%ad:accountName%</Field>
...
</Arguments>
```

**Primer 10:** Prikazan je primer izseka konfiguracije za sinhronizacijo uporabnikov, kjer se iz LDAP vrednosti »sAMAccountName« in »sAMAccountType« sestavi unikatni identifikator, kodiran kot Base64:

```
<Arguments>
...
<Field key="sys:dir:Account" type="string">sAMAccountName</Field>
<Field key="ad:sAMAccountType" type="string">sAMAccountType</Field>
<Field key="sys:dir:UUID" type="expression" scope="user" script="var tmp = sys_dir_Account[0]; tmp
+= ad_sAMAccountType[0]; var b64encode = java.util.Base64.encoder.encodeToString(tmp.bytes);
b64encode;">%sys:dir:Account%</Field>
...
</Arguments>
```

### 3.9 Varnostno kopiranje in obnovitev podatkov

Za učinkovito varovanje podatkov je potrebno zagotoviti redno izdelavo varnostnih kopij.

Pomembno je, da varnostne kopije ne pridejo v roke nepooblaščenim osebam in da v primeru nesreče ostanejo nepoškodovane. Varnostno kopiranje zmanjšuje tveganje izgube podatkov zaradi tehnične okvare nosilca zapisa, napake v programu, naravne nesreče, nepooblaščenega dostopa, človeškega faktorja, ...

Omogoča obnovitev podatkov in povrnitev prejšnjega stanja.

Strežnik IMiS®/ARChive Server omogoča varnostno kopiranje in obnavljanje:

- Dokumentarnega gradiva.
- Načrta razvrščanja gradiva v celoti ali samo izbranih razredov, zadev in dokumentov.
- Metapodatkov.
- Revizijske sledi.
- Digitalnih potrdil.
- Liste dostopnih pravic.
- Strežniškega imenika.

Spodnja tabela prikazuje tabele v bazi z opisom vsebine za varnostno kopiranje in obnavljanje.

<b>Tabela</b>	<b>Opis</b>
ACLENTRY	Vnosi za listo dostopnih pravic.
ACLENTRYVALIDITY	Časovne omejitve dostopnih pravic.
ATTRIBUTE	Atributi, ki so določeni na strežniku IMiS®/ARChive Server.
ATTRIBUTEVALUE	Povezovalna tabela med atributom, vrednostjo in entiteto, kateri vrednost pripada.
ATTRIBUTEVALUEBINARY	Tabela vsebuje binarne vrednosti atributov.
ATTRIBUTEVALUEDATETIME	Tabela vsebuje datumske vrednosti s časovno komponento.
ATTRIBUTEVALUEDOUBLE	Tabela vsebuje realna (racionalna) števila v plavajoči vejici z dvojno natančnostjo.
ATTRIBUTEVALUEFILE	Tabela vsebuje vrednosti o datotekah.
ATTRIBUTEVALUEINT32	Tabela vsebuje predznačena 32 bitna cela števila.
ATTRIBUTEVALUEINT64	Tabela vsebuje predznačena 64 bitna cela števila.
ATTRIBUTEVALUEINT128	Tabela vsebuje predznačena 128 bitna cela števila.
ATTRIBUTEVALUEINT128IDX	Tabela vsebuje indeksirana predznačena 128 bitna cela števila.
ATTRIBUTEVALUESTRING	Tabela vsebuje neomejene nize UTF-8 znakov (omejeni so z možnostjo platforme).

ATTRIBUTEVALUESTRING10	Tabela vsebuje nize UTF-8 znakov, dolgih 10 bajtov.
ATTRIBUTEVALUESTRING20	Tabela vsebuje nize UTF-8 znakov, dolgih 20 bajtov.
ATTRIBUTEVALUESTRING30	Tabela vsebuje nize UTF-8 znakov, dolgih 30 bajtov.
ATTRIBUTEVALUESTRING40	Tabela vsebuje nize UTF-8 znakov, dolgih 40 bajtov.
ATTRIBUTEVALUESTRING50	Tabela vsebuje nize UTF-8 znakov, dolgih 50 bajtov.
ATTRIBUTEVALUESTRING100	Tabela vsebuje nize UTF-8 znakov, dolgih 100 bajtov.
ATTRIBUTEVALUESTRING200	Tabela vsebuje nize UTF-8 znakov, dolgih 200 bajtov.
ATTRIBUTEVALUESTRING20IDX	Tabela vsebuje indeksirane nize UTF-8 znakov, dolgih 20 bajtov.
ATTRIBUTEVALUESTRING30IDX	Tabela vsebuje indeksirane nize UTF-8 znakov, dolgih 30 bajtov.
ATTRIBUTEVALUESTRING40IDX	Tabela vsebuje indeksirane nize UTF-8 znakov, dolgih 40 bajtov.
ATTRIBUTEVALUESTRING50IDX	Tabela vsebuje indeksirane nize UTF-8 znakov, dolgih 50 bajtov.
ATTRIBUTEVALUESTRING100IDX	Tabela vsebuje indeksirane nize UTF-8 znakov, dolgih 100 bajtov.
ATTRIBUTEVALUESTRING200IDX	Tabela vsebuje indeksirane nize UTF-8 znakov, dolgih 200 bajtov.
ATTRIBUTEVALUEUINT32	Tabela vsebuje ne-predznačena 32 bitna cela števila.
ATTRIBUTEVALUEUINT64	Tabela vsebuje ne-predznačena 64 bitna cela števila.
ATTRIBUTEVALUEUINT128	Tabela vsebuje ne-predznačena 128 bitna cela števila.
ATTRIBUTEVALUEUINT128IDX	Tabela vsebuje indeksirana ne-predznačena 128 bitna cela števila.
DIGITALCERTIFICATE	Tabela vsebuje digitalna potrdila, ki se nahajajo v strežniški shrambi digitalnih potrdil.
COUNTER	Tabela vsebuje vrednosti števcov za avtomatsko generiranje klasifikacijskih kod.
DIGITALSIGNATURE	Tabela vsebuje digitalne podpise.

DIRECTORYENTRY	Tabela vsebuje entitete (uporabnike ali uporabniške skupine) v strežniškem imeniku.
DIRECTORYENTRYALIAS	Tabela vsebuje sinonime entitet v strežniškem imeniku.
DIRECTORYENTRYGROUP	Tabela vsebuje podatke o članih uporabniških skupin.
ENTITY	Tabela vsebuje podatke o strežniških entitetah (razredih, zadevah, dokumentih).
ENTITYCLASS	Tabela vsebuje podatke o razredih na strežniku.
ENTITYDOCUMENT	Tabela vsebuje podatke o dokumentih na strežniku.
ENTITYFOLDER	Tabela vsebuje podatke o zadevah na strežniku.
PROFILE	Tabela vsebuje podatke o HSM profilih.
PROPERTY	Generična tabela nastavitvev.
TEMPLATE	Tabela vsebuje strežniške predloge.
TEMPLATEATTRIBUTE	Tabela vsebuje povezave med strežniškimi predlogami in atributi, ki jim pripadajo.
TEMPLATEBIND	Tabela vsebuje podatke o povezavah med strežniškimi predlogami.
ARCHIVALINFORMATIONPACKAGE	Tabela vsebuje arhivske informacijske pakete (AIP).
ARCHIVALINFORMATIONPACKAGEQUEUE	Tabela predstavlja čakalno vrsto za AIP.
CREATEAIPQUEUE	Tabela predstavlja čakalno vrsto za ustvarjanje AIP.
AIPJOBTIMESTAMP	Tabela vsebuje podatke o postopku časovnega žigosanja.
REVOCATIONDATA	Tabela vsebuje informacije o preklicih digitalnih potrdil.
CONTENTPROCESSINGQUEUE	Tabela vsebuje informacije za indeksiranje in pretvorbo vsebin.
CONTENTPROCESSINGERROR	Tabela vsebuje informacije vsebinah, nad katerimi se je neuspešno izvršilo indeksiranje ali pretvorba.
TIMESTAMP	Tabela vsebuje časovne žige.
VOLUME	Tabela vsebuje podatke o HSM volumnih.
LOOKUPTABLE	Tabela vsebuje statuse, pomembnost ter stopnje tajnosti entitet. Poleg tega vsebuje še prioritete dostave elektronske pošte ter status fizičnega gradiva.
HASH128	Tabela vsebuje prstne odtise dolžine 128 bitov.
HASH160	Tabela vsebuje prstne odtise dolžine 160 bitov.
HASH224	Tabela vsebuje prstne odtise dolžine 224 bitov.



HASH256	Tabela vsebuje prstne odtise dolžine 256 bitov.
HASH384	Tabela vsebuje prstne odtise dolžine 384 bitov.
HASH512	Tabela vsebuje prstne odtise dolžine 512 bitov.
REVOCATIONDATATIMESTAMP	Tabela vsebuje povezave med informacijami o preklicih digitalnih potrdil in časovnimi žigi, katerim pripadajo.
REVOCATIONDATADIGITALSIGNATURE	Tabela vsebuje povezave med informacijami o preklicih digitalnih potrdil in elektronskimi podpisimi, katerim pripadajo.
ENTITYRETENTIONDISPOSITIONSCHEDULE	Tabela vsebuje informacije o povezavah med roki hrambe ter entitetami.
TIMESTAMPARCHIVALINFORMATIONPACKAGE	Tabela vsebuje arhivske informacijske pakete za časovne žige.
CERTIFICATEBODY	Tabela vsebuje binarne ali Base64 kodirane podatke, ki predstavljajo digitalno potrdilo.
FILEDESCRIPTION	Tabela vsebuje opise digitalnih vsebin.
ATTRIBUTEVALUENULL	Tabela vsebuje entitete z atributi, katerih vrednosti so »null«.
REVIEWQUEUE	Tabela vsebuje preglede odbiranja in izločanja, ki so v postopku izdelave ali v postopku izvajanja.
CONTENTBIND	Tabela vsebuje informacije o odvisnosti vsebin v entiteti.
DIRECTORYENTRYDELEGATE	Tabela vsebuje seznam povezav med uporabniki in njihovimi delegati.
TOKEN4	Tabela vsebuje besede (ali dele besed) do velikosti 4 bajtov.
TOKEN8	Tabela vsebuje besede (ali dele besed) do velikosti 8 bajtov.
TOKENMAX	Tabela vsebuje besede (ali dele besed) do velikost 30 bajtov
SYSEVENT	Tabela vsebuje strežniške dogodke.

Tabela 51: Tabele z opisom podatkov za varnostno kopiranje in obnavljanje

Strežnik IMiS®/ARChive Server dodatno omogoča samodejno izdelavo varnostnih kopij vseh, za delovanje in konsistentnost, pomembnih datotek. Te obsegajo podatkovno zbirko, kjer strežnik IMiS®/ARChive Server hrani metapodatke o gradivih, podatke revizijske sledi, konfiguracijo, ... in datoteke arhiviranih gradiv.

Kot izdelovalec programske opreme strankam priporočamo, da področje varnostnega kopiranja in obnovitve (angl. Backup/ Restore) arhivskega strežnika uredijo s profesionalnim orodjem tipa odjemalec/strežnik (npr. IBM Tivoli Storage Manager, HP Data Protector, CA ARCserve, ...).

### 3.9.1 Varnostno kopiranje

Za izvedbo varnostnega kopiranja moramo na IMiS®/ARChive Server namestiti odjemalca za varnostno shranjevanje datotek. Lokacija odjemalca je odvisna od tega, katero orodje tipa odjemalec/strežnik uporabimo.

#### 3.9.1.1 Nastavitve varnostnega kopiranja

Nastavitve varnostnega kopiranja so odvisne od tega, katero orodje za varnostno kopiranje uporabimo. V večini primerov se opis nastavitve nahaja v njihovi dokumentaciji.

V osnovi pa lahko varnostno kopiranje ločimo na naslednje tipe:

- Popolno varnostno kopiranje (angl. Full backup), ki obsega kopiranje vseh podatkov.
- Prirastno varnostno kopiranje (angl. Incremental backup), ki obsega kopiranje podatkov, ki so se spremenili od časa zadnjega varnostnega kopiranja.
- Diferencialna varnostna kopija (angl. Differential backup), ki obsega kopiranje podatkov, ki so se spremenili od časa zadnjega popolnega varnostnega kopiranja.

V kombinaciji z orodjem `dbtool` se za IMiS®/ARChive Server lahko uporabi katerikoli tip varnostnega kopiranja.

### 3.9.2 Obnovitev podatkov

Obnovitev arhiviranih dokumentov na strežniku IMiS®/ARChive Server je odvisna od stanja strežnika in zelenega rezultata po obnovitvi podatkov strežnika.

V primeru negotovosti glede uporabnosti podatkov, ki so ostali na diskih, ali če obstaja možnost restavriranja stanja pred odpovedjo diskov, vam svetujemo, da se obrnete na našo tehnično podporo preko e-pošte: [podpora@imis.si](mailto:podpora@imis.si).

Pri obnovitvi podatkov iz varnostne kopije je zagotovljena celovitost podatkov, kar velja tudi za revizijsko sled. Obnovitev podatkov strežnika IMiS®/ARChive Server je odvisna od stanja strežnika in zelenega rezultata po obnovitvi podatkov.

Za uspešno obnovitev podatkov mora strežnik opravilo varnostnega kopiranja shraniti najmanj za:

- Bazo strežnika (privzeta lokacija je v imeniku `/iarc/db`).
- Volumne strežnika z vso vsebino, rekurzivno (privzeta lokacija je v imeniku `/iarc/vol`).
- Nastavitveno datoteko strežnika `iarc.conf` (privzeta lokacija je v imeniku `/etc`).

Popolno kopijo pri varnostnem kopiranju dosežemo, če opravilo varnostnega kopiranja poleg minimalnih zahtev shrani še:

- Imenik `/iarc/webadmin` z vso vsebino, rekurzivno.
- Imenik `/opt/IS/imisar` z vso vsebino, rekurzivno.
- Datoteko `/etc/init.d/iarc`.
- Imenik `/var/log/iarc` z vso vsebino.

### 3.9.2.1 Nastavitve obnovitve podatkov

Pri postopku obnovitve podatkov najprej pridobimo zadnje shranjene tekstovne datoteke s podatki iz baze ter vsebino volumnov strežnika. Pri tem je potrebno paziti na pravilne nastavitve dostopnih pravic za uporabnika, v imenu katerega se strežnik zaganja (privzet uporabnik je `iarc`, za spreminjanje lastniških pravic pa lahko uporabimo orodja kot sta `chown` ali `chmod`).

Postopek obnovitev volumnov je naslednji:

- če vsebina starih volumnov obstaja (privzeta lokacija se nahaja v imeniku `/iarc/vol`) se izbriše;
- objekte volumnov iz varnostne kopije uporabnik kopira na volumne strežnika;
- za kopirane objekte je potrebno nastaviti dostopne pravice (pravice branja in pisanja).

Postopek obnovitve strežniške baze je naslednji:

- Prazno strežniško bazo se uporabnik kopira na strežniško lokacijo (privzeta lokacija je v imeniku `/iarc/db`).
- Na strežniški bazi se nastavi pravice branja in pisanja.
- Tekstovne datoteke baze iz varnostne kopije se kopirajo na začasno lokacijo na disku.
- Tekstovnim datotekam nastavimo pravice branja.

- Strežniško bazo obnovimo z uporabo orodja dbtool . Pri tem lahko obnavljamo posamezne tabele z uporabo parametra `-t` ali pa uporabimo parameter `-a`, ki uvozi podatke v vse tabele, za katere tekstovne datoteke obstajajo. Za več informacij glej poglavje [Konfiguriranje](#).

### 3.9.3 Primer

Pri izdelavi varnostnih kopij podatkov strežnika IMiS®/ARChive Server je potrebno upoštevati tudi možnost izgube ali delne okvare podatkov na sami varnostni kopiji in možnost uničenja medija. Dobra praksa vključuje izdelavo kopij varnostnih kopij in hranjenje dvojnikov na oddaljeni lokaciji. Varnostne kopije in njih kopije hranimo na ustrezno varovanem ognjevarnem mestu. Možnost popolne izgube podatkov zmanjšamo tudi z ustreznim načrtom izdelave in hranjenja varnostnih kopij za daljše obdobje.

*Primer:* Varnostne kopije strežnika IMiS®/ARChive Server izdelujemo dnevno.

*Izvirne varnostne kopije hranimo v ognjevarni omari na lokaciji strežnika, kopije varnostnih kopij pa v sefu na oddaljeni lokaciji. Varnostne kopije, narejene ob koncu tedna, ob koncu meseca in ob koncu leta, hranimo v sefu še primerno dolgo, glede na trajanje medija in uporabnost varnostno kopiranih vsebin.*

Uporabnost varnostnih kopij je potrebno tudi periodično preverjati. Podatke iz varnostne kopije restavriramo na drugo lokacijo in jih primerjamo z izvornimi podatki s strežnika IMiS®/ARChive Server.

Načrt izdelave in hranjenja varnostnih kopij je potrebno periodično preverjati vsaj ob bistvenih spremembah, kot so zamenjave strežnikov, medijev ali infrastrukture, ki neposredno vpliva na dogodke povezane s strežnikom IMiS®/ARChive Server. Načrt praviloma preveri revizor informacijskih sistemov, ki se do njega tudi opredeli.

### 3.9.4 Težave pri obnovitvi podatkov

V primeru negotovosti glede uporabnosti podatkov, ki so ostali na diskih ali če obstaja možnost restavriranja stanja pred odpovedjo diskov vam svetujemo, da se obrnete na tehnično osebje proizvajalca strežnika IMiS®/ARChive Server.

Primeri v nadaljevanju prikazujejo težave, ki se lahko zgodijo pri postopku obnovitve podatkov.

### Opis težave #1

Pri postopku obnovitve podatkov pri uvozu z orodjem `dbtool` dobimo naslednjo napako (ime tekstovne datoteke je lahko drugačno in je odvisno od tega, katero tabelo v bazi obnavljamo):

*Using 'sl\_SI.UTF-8' locale settings.*

*Document Root: /iarc/db/*

*Port: 21553*

*attribute.txt file, open error 13: Permission denied.*

*Import command completed with 1 error(s).*

**Rešitev težave #1:** Dostopne pravice za tekstovne datoteke niso pravilno nastavljene.

Uporabniku, v imenu katerega se bo izvajal strežnik (privzet uporabnik je `iarc`) nima bralnih pravic na tekstovnih datotekah. Rešitev je nastavitev pravih dostopnih pravic tekstovnih datotek in ponovitev postopka obnavljanja podatkov.

### Opis težave #2

V postopku obnovitve podatkov pri uvozu z orodjem `dbtool` dobimo naslednjo napako:

*Using 'sl\_SI.UTF-8' locale settings.*

*Document Root: /iarc/db/*

*Port: 21553*

*Error; Unable to move to requested record (dberr#-940) while going backwards! (file = RaimaKeyIterator.cpp, func = moveTo, line = 200)*

**Rešitev težave #2:** Dostopne pravice za strežniško bazo niso pravilno nastavljene.

Rešitev je nastavitev dostopnih pravic branja in pisanja na strežniški bazi za uporabnika, v imenu katerega se bo IMiS®/ARChive Server zaganjal. Sledi postopek obnavljanja podatkov.

### Opis težave #3

V postopku obnovitve podatkov pri uvozu z orodjem `dbtool` dobimo naslednjo napako (ime tekstovne datoteke in vrednost tabele je lahko drugačno in je odvisno od tega, katero tabelo v bazi obnavljamo):

*Using 'sl\_SI.UTF-8' locale settings.*

*Document Root: /iarc/db/*

*Port: 21553*

*Importing attribute.txt (3194 bytes) to ATTRIBUTE ... Error; Tried to insert duplicate key into table 10008! (file = RaimaDataSet.cpp, func = InsertObject, line = 207)*

Rešitev težave #3: Strežniška baza v katero želimo uvoziti že vsebuje podatke, ki so podvojeni s podatki v tekstovnih datotekah. Rešitev za takšen tip napak je več:

- Strežniško bazo zamenjamo s prazno ter ponovimo postopek uvoza podatkov.
- Posamezno tabelo, pri kateri dobimo v postopku uvoza podatkov zgoraj opisano napako najprej izbrišemo (uporabimo ukaz `init` v `dbtool-u`), ter ponovimo postopek uvoza podatkov za to tabelo (to ne velja za revizijsko sled, saj se le-te ne da izbrisati).
- Pri uvozu podatkov z orodjem `dbtool` uporabimo možnost `-o`, ki morebitne obstoječe podatke v bazi prepíše s podatki iz tekstovnih datotek.

*Primer:* ukaz za uvoz vseh tekstovnih datotek z možnostjo prepisa:

```
su - iarc -s /bin/bash -c "cd /opt/IS/imisarc && ./dbtool -f /etc/iarc.conf -w /iarc/db/ -o -a imp"
```

## 3.10 Skladiščenje vsebine

Vsebina entitet se shranjuje na HSM (angl. Hierarchical Storage Management) profilih in volumnih. HSM je hierarhično zasnovan sistem za shranjevanje podatkov, kjer se vsebina, do katere se pogosto dostopa, shranjuje na hitrejših nosilcih, vsebina z malo dostopi pa se hrani na počasnejših nosilcih (za več informacij glej:

[https://en.wikipedia.org/wiki/Hierarchical\\_storage\\_management](https://en.wikipedia.org/wiki/Hierarchical_storage_management)).

Profili predstavljajo logično zaključeno HSM celoto, kjer so posamezni volumni razporejeni po nivojih glede na hitrost (od najhitrejših do najpočasnejših). Volumni predstavljajo nosilce podatkov, s katerimi IMiS®/ARChive Server operira.

### 3.10.1 Profili

Profili predstavljajo logično zaključeno HSM celoto. Poleg osnovnih informacij (ime, opis), profil vsebuje še skupno velikost vseh volumnov, ki pripadajo profilu, skupen zaseden prostor, skupno število vsebin na vseh volumnih ter naslednje lastnosti, ki pogojujejo delovanje profila:

- »ReadOnly« – vsebin na volumnih, ki pripadajo profilu se ne more urejati.
- »WORM« (angl. write once read many) – vsebine se na volumnih, ki pripadajo profilu lahko ustvarja, urejati se jih ne more.
- »StopAddingObjects« - vsebine na volumnih se lahko bere in ureja, novih vsebin se ne more dodajati.

Profilu lahko določimo razred in s tem omejimo vsebine, ki se bodo shranjevale na volumne profila. Če ima profil določen razred, potem se bodo na volumne shranjevale samo vsebine entitet, ki so vsebovane entitete nastavljenega razreda. Če razred ni določen, profil velja za celoten arhiv. Zaporedje volumnov na profilu (znotraj istega nivoja) se lahko spreminja. S tem lahko administrator nadzira zasedenost volumnov na profilu.

Primer konfiguracije profila:

```
<ns1:Profile xsi:type="ns1:StorageProfile">
  <ns1:Name xsi:type="xsd:string">Dokumenti</ns1:Name>
  <ns1:Objects xsi:type="xsd:unsignedInt">1095174</ns1:Objects>
  <ns1:Size xsi:type="xsd:unsignedLong">51539607552</ns1:Size>
  <ns1:Used xsi:type="xsd:unsignedLong">44696233984</ns1:Used>
  <ns1:ReadOnly xsi:type="xsd:boolean">>false</ns1:ReadOnly>
  <ns1:WORM xsi:type="xsd:boolean">>false</ns1:WORM>
  <ns1:StopAddingObjects xsi:type="xsd:boolean">>false</ns1:StopAddingObjects>
  <ns1:Volume level="0">vol20</ns1:Volume>
  <ns1:Volume level="0">vol06</ns1:Volume>
  <ns1:Volume level="0">vol05</ns1:Volume>
  <ns1:Volume level="0">vol00</ns1:Volume>
  <ns1:Volume level="0">vol01</ns1:Volume>
  <ns1:Volume level="0">vol02</ns1:Volume>
  <ns1:Class xsi:type="ns1:EntityId" type="ClassificationCode"/>
</ns1:Profile>
```

**Etiketa »Name«:** Vsebina etiketa vsebuje ime profila.

**Etiketa »Objects«:** Vsebina etikete vsebuje število vsebin na vseh volumnih na profilu.

**Etiketa »Size«:** Vsebina etikete vsebuje skupno velikost vseh volumnov na profilu (v bajtih).

**Etiketa »Used«:** Vsebina etikete vsebuje skupno velikost zasedenega prostora na vseh volumnih na profilu (v bajtih).

**Etiketa »ReadOnly«:** Vrednost »True« predstavlja profil, ki omogoča samo branje vsebine. Vrednost »False« omogoča tudi ustvarjanje in urejanje vsebine (odvisno je od drugih lastnosti profila).

**Etiketa »WORM«:** Vrednost »True« predstavlja profil, ki omogoča samo ustvarjanje in branje vsebin. Vrednost »False« omogoča tudi urejanje vsebine (odvisno je od drugih lastnosti profila).

**Etiketa »StopAddingObjects«:** Vrednost »True« onemogoči ustvarjanje novih vsebin na volumnih profila. Vrednost »False« omogoča ustvarjanje novih vsebin (odvisno je od drugih lastnosti profila).

**Etikete »Volume«:** Vrednost etikete predstavlja ime volumna, ki je dodeljen profilu. Atribut »level« predstavlja HSM nivo volumna, zaporedje etiket pa predstavlja zaporedje volumnov na profilu.

**Etiketa »Class«:** Vrednost etikete predstavlja identifikator razreda, kateremu je profil dodeljen. Atribut »type« predstavlja tip identifikatorja.



### 3.10.2 Volumni

Volumni predstavljajo nosilce podatkov, s katerimi strežnik operira. Vsak volumen vsebuje definicijo, to je absolutna pot do datotečnega sistema, kamor se bo vsebina fizično shranila. Poleg tega volumni vsebujejo še informacije o njihovi velikosti, profilu, številu vsebin na volumnu, zaseden prostor, »ReadOnly«, »WORM« in »StopAddingObjects« nastavitve (njihov pomen je enak kot na profilu), ter informacijo, ali je volumen vpet (angl. mounted) ali ne. Če volumen ni vpet, potem so zahteve za dostop do vsebine na takem volumnu zavrnjene. Volumen se lahko menja med profili, vendar samo če je prazen. Naslednji zapis prikazuje primer konfiguracije volumna.

```
<ns1:Volume xsi:type="ns1:StorageVolume">
  <ns1:Name xsi:type="xsd:string">vol05</ns1:Name>
  <ns1:Definition xsi:type="xsd:string">/iarc/vol/vol05</ns1:Definition>
  <ns1:Profile xsi:type="ns1:StorageVolumeProfile">
    <ns1:Name xsi:type="xsd:string">Dokumenti</ns1:Name>
    <ns1:Level xsi:type="xsd:unsignedByte">0</ns1:Level>
    <ns1:Sequence xsi:type="xsd:unsignedInt">2</ns1:Sequence>
  </ns1:Profile>
  <ns1:Objects xsi:type="xsd:unsignedInt">37212</ns1:Objects>
  <ns1:Size xsi:type="xsd:unsignedLong">8589934592</ns1:Size>
  <ns1:Used xsi:type="xsd:unsignedLong">8411480064</ns1:Used>
  <ns1:ReadOnly xsi:type="xsd:boolean">>false</ns1:ReadOnly>
  <ns1:WORM xsi:type="xsd:boolean">>false</ns1:WORM>
  <ns1:StopAddingObjects xsi:type="xsd:boolean">>false</ns1:StopAddingObjects>
  <ns1:Mounted xsi:type="xsd:boolean">>true</ns1:Mounted>
</ns1:Volume>
```

**Etiketa »Name«:** Vrednost etikete predstavlja ime volumna.

**Etiketa »Definition«:** Vrednost etikete predstavlja absolutno pot na datotečne sistemu, kamor se bo vsebina fizično shranjevala.

**Etiketa »Profile«:** Etiketa vsebuje ime profila, HSM nivo ter zaporedje v profilu, kjer se volumen nahaja.

**Etiketa »Objects«:** Vrednost predstavlja število vsebin na volumnu.

**Etiketa »Size«:** Vrednost predstavlja velikost volumna (v bajtih).

**Etiketa »Used«:** Vrednost predstavlja zaseden prostor na volumnu (v bajtih).

**Etiketa »ReadOnly«:** Vrednost »True« predstavlja volumen »samo za branje«. Vrednost »False« pomeni, da administrator lahko ustvarja in ureja vsebine na volumnu (odvisno od drugih lastnosti volumna).

**Etiketa »WORM«:** Vrednost »True« predstavlja volumen, ki omogoča samo ustvarjanje in branje vsebin. Vrednost »false« omogoča tudi urejanje vsebine (odvisno od drugih lastnosti volumna).

**Etiketa »StopAddingObjects«:** Vrednost »True« onemogoča ustvarjanje novih vsebin na volumnu. Vrednost »False« omogoča ustvarjanje novih vsebin (odvisno od drugih lastnosti volumna).

**Etiketa »Mounted«:** Vrednost »True« pomeni, da je volumen vpet in da omogoča serviranje shranjene vsebine. Vrednost »False« pomeni, da dostop do vsebine ni možen. Prav tako ni možno ustvarjanje nove vsebine.

### 3.11 Verzioniranje

Verzioniranje je proces, skozi katerega se ustvarjajo nove vrednosti atributov na entiteti.

Slednje velja, če je atribut na predlogi označen kot »verzionabilen«.

Za več informacij glej poglavje [Predloge](#).

Strežnik IMiS®/ARChive Server omogoča verzioniranje vrednosti atributov na dokumentih.

Verzionabilnim atributom se vrednosti spreminjajo glede na verzijo, medtem ko vrednosti atributov, ki niso verzionabilni ostajajo čez vse verzije enake.

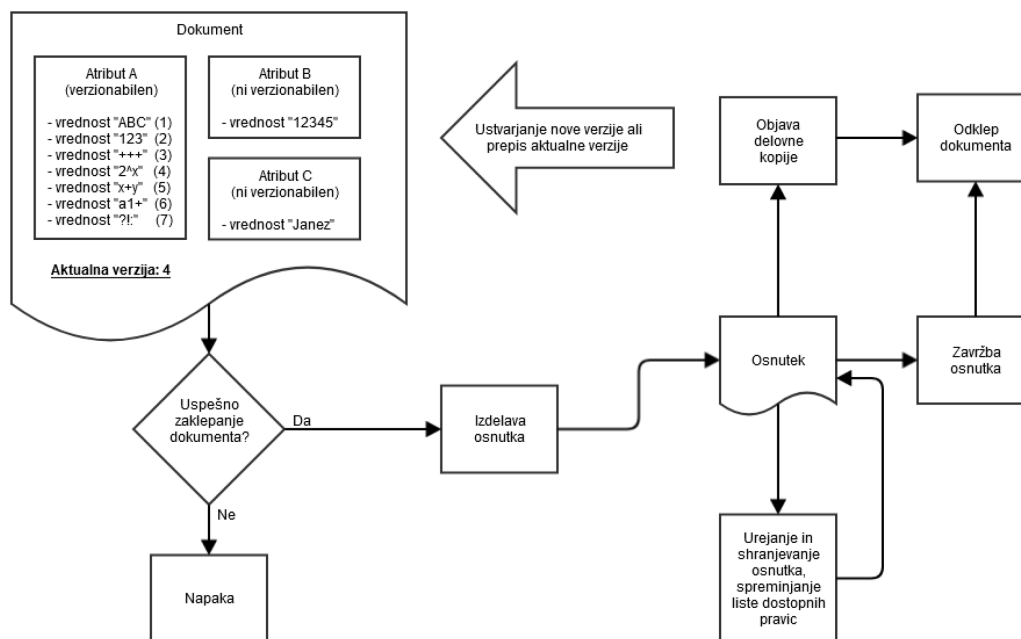
Ob ustvarjanju nove verzije se vrednostim verzionabilnih atributov dodeli nova zaporedna številka, ki predstavlja verzijo (angl. Version sequence). Največje število verzij za posamezen dokument je omejeno na 65535. Aktualna verzija dokumenta predstavlja zaporedno številko verzije, katere atributi so bili spremenjeni ob zadnji shranitvi dokumenta.

Proces verzioniranja je sestavljeno iz treh operacij:

- Izdelava osnutka (angl. Check-out).
- Vložitev osnutka (angl. Check-in).
- Zavrženje osnutka (angl. Discard).

Osnutek je kopija originalnega dokumenta, ki je viden samo lastniku (uporabniku ali skupini uporabnikov, ki so navedeni v atributu 'sys:Owner') ter uporabniku s pravicami (administratorju), ki ima vlogo »ManageDraft«. Ti uporabniki lahko izvajajo operacije vložitve (angl. Check in) ali zavrženja osnutka (angl. Discard). Na osnutku je mogoče izvajati še operacije urejanja in shranjevanja ter spreminjati listo dostopnih pravic. Vse ostale operacije niso dovoljene. Ob izdelavi osnutka se izvorni dokument zaklene za urejanje ter ostane zaklenjen, dokler se osnutek bodisi ne vloži ali zavrže. Vložitev osnutka omogoča ustvarjanje nove verzije, ali pa prepis trenutno aktualne verzije, zavrženje osnutka pa osnutek izbriše.

Celoten proces verzioniranja prikazuje naslednja slika.



Slika 35: Proces verzioniranja

## 4 SISTEMSKE ZAHTEVE

### 4.1 Strojna oprema

Strežniki, ki jih lahko danes kupimo na tržišču, večinoma zadoščajo zahtevam strežnika IMiS®/ARChive Server saj potrebuje malo virov in zato brez težav deluje tudi v virtualnih okoljih. Pozornost je potrebno posvetiti ustrezni arhitekturi strežnika in jo uskladiti z eno izmed podprtih arhitektur produkta, večinoma gre za Intel x86 platforme v 32 in 64 bitnih izvedbah.

#### 4.1.1 Načrtovanje procesorske moči strežnika

Pri izbiri procesorske moči je potrebno posvetiti pozornost predvidenim obremenitvam strežnika (število odjemalcev, število vzporednih uporabniških sej, povprečne velikosti arhiviranih vsebin, uporaba revizijske sledi, ...).

Glede na trenutne funkcionalne lastnosti produkta, je na trgu zadovoljiva količina različnih procesorjev srednjih ali višjih zmogljivosti, ki omogoča kvalitetno obratovalno okolje.

Navadno se pri izbiri procesorske moči lahko orientiramo glede na priporočene zahteve samega operacijskega sistema.

Za namišljen sistem 500 uporabnikov s povprečno 200 vpogledi na dan pri povprečni velikosti arhivirane vsebine 100KB, bi tudi v primeru sočasne uporabe vseh uporabnikov s transakcijami v istem časovnem obdobju zadostoval 1x procesor tehnologij Xeon QuadCore srednje frekvenčne zmogljivosti ali 1x procesor družine Intel Core i5/i7 srednje frekvenčne zmogljivosti.

#### 4.1.2 Načrtovanje pomnilniških kapacitet strežnika

Pri načrtovanju velikosti pomnilnika strežnika IMiS®/ARChive Server je potrebno upoštevati:

- Zahteve operacijskega sistema.
- Osnovne zahteve strežnika, ki za samo delovanje potrebuje približno 512 MB.
- Število hkratnih uporabnikov; vsaka povezava bo potrebovala približno 256 KB.
- Minimalna priporočena velikost pomnilnika je enaka seštevku 512MB in minimalne velikosti pomnilnika, ki je zahtevan s strani proizvajalca operacijskega sistema.

Priporočena velikost pomnilnika je enaka seštevku potrebe po pomnilniku s strani servisov samega operacijskega sistema in 1024MB (1GB) za delovanje samega strežnika IMiS®/ARChive Server.

### 4.1.3 Načrtovanje diskovnih kapacitet strežnika

Pri načrtovanju diskovnih kapacitet strežnika je potrebno upoštevati naslednje:

- Zahteve operacijskega sistema.
- Predviden povprečen dnevni prirastek objektov.
- Predviden prirast objektov na račun pretvorbe starega papirnega arhiva v elektronsko.
- Velikost povprečnega objekta.
- Predvideni čas uporabe strežnika (npr. 5 let).

Objekti, ki jih hrani strežnik IMiS®/ARChive Server na svojih volumnih so lahko različnih tipov in lahko izvirajo iz različnih računalniških okolij.

Objekti, skenirani z IMiS®/Scan pri ločljivosti 300pik/inčo, v črno-beli tehniki (barvna globina 1 bit) pri uporabi privzete metode za zgoščevanje (CCITT G4 T6) zavzamejo povprečno 45KB na skenirano stran.

Z uporabo drugih zgoščevalnih metod, barvne globine in ločljivosti se velikost praviloma poveča (glej tabelo v nadaljevanju).

Barvna globina	Črno/belo (1 bit)	Svinsko (8 bit)	Barvno (24 bit)
<b>Brez</b>	605 KB	5 MB	15 MB
<b>CCITT G3</b>	85 KB	x	X
<b>CCITT G4 T6</b>	45 KB	x	X
<b>JBIG</b>	36 KB	x	x
<b>JBIG 2bit</b>	x	84 KB	x
<b>JBIG 3bit</b>	x	165 KB	x
<b>JBIG 4bit</b>	x	420 KB	x
<b>Packed bits</b>	109 KB	5 MB	15 MB
<b>LZW</b>	75 KB	3,2 MB	x
<b>Packed bits 8 bit</b>	x	x	x
<b>Packed bits 24 bit</b>	x	x	x
<b>ZIP</b>	56 KB	3 MB	9 MB
<b>Wang JPEG</b>	x	315 KB	363 KB
<b>Sekvenčni JPEG</b>	x	315 KB	360 KB
<b>Progresivni JPEG</b>	x	310 KB	334 KB

Tabela 52: Povprečne velikosti skeniranega dokumenta glede na metode stiskanja

Pri izbiri ustrezne metode za zgoščevanje je potrebno upoštevati, da prenos večjih objektov preko računalniške mreže, zahteva večjo pasovno širino in lahko vpliva tudi na odzivnost računalniške mreže.

Odsvetujemo skeniranje v sivinah ali barvah, saj danes večina skenerjev, ki so namenjeni zajemu dokumentov uporablja napredne metode in filtre za grafično obdelavo, kar zagotavlja optimalno kvaliteto skeniranih dokumentov.

Priporočamo uporabo diskovnih kapacitet z ustreznim varovanjem podatkov in razširljivostjo. Priporočamo uporabo sodobnih diskovnih krmilnikov, ki omogočajo predpomnjenje branja in pisanja. Predpomnilnik naj ima avtonomno podporo napajanja ali pa izveden s tehnologijo »Flash Memory« (EEPROM tehnologija), ki lahko hrani podatke brez pomoči električne energije, kot to zahteva statičen RAM, s katerim so opremljeni starejši RAID krmilniki.

Diski naj bodo združeni v redundantno diskovno polje. Zaradi izkoristka priporočamo diskovno polje tipa RAID5 z dodatnim rezervnim diskom.

Odsvetujemo diskovne kapacitete, ki bi bilo strežniku IMiS®/ARChive Server dostopno preko lokalne mreže, npr. NAS (angl. Network Attached Storage) ali diskovne kapacitete, ki se nahaja na drugem strežniku in je strežniku IMiS®/ARChive Server dano v souporabo preko protokolov kot so CIFS, NSF, ...

#### **4.1.4 Komunikacijske poti**

IMiS® odjemalci komunicirajo s strežnikom IMiS®/ARChive Server preko omrežnih vrat številka 16807, v kolikor v nastavitveni datoteki `/etc/iarc.conf` ni nastavljeno drugače.

Potrebno je poskrbeti, da je komunikacija preko teh vrat omogočena, pri čemer naj pravila na požarnih zidovih ali drugi aktivni omrežni opremi dovoljujejo vzpostavitev povezave odjemalec-strežnik s strani IMiS® odjemalca, medtem ko vzpostavitev povezave strežnik-odjemalec s strani strežnika ni predvidena/potrebna.

#### **4.1.5 Priklop na mrežno opremo**

Priporočamo podvojene povezave in priklop na hrbtenico lokalne mreže s čim manj posredniki. Najbolje je, če je strežnik priklopljen na glavno mrežno stikalo.

Omrežni protokol med odjemalcem IMiS® in strežnikom IMiS®/ARChive Server je optimiziran za pakete v velikosti 32KB v primeru podatkovnih paketov (branje/pisanje arhivirane vsebine) in manjše v primeru ukaznih paketov.

Posamezen omrežni paket lahko izjemoma preseže 32KB v kolikor zahtevk ali odgovor na zahtevk to zahteva (večji obseg podatkov enega zahtevka).

Vsa komunikacija med strežnikom in odjemalcem je zgoščena po GZIP in je iz tega vidika propustnost največja. Testi med razvojem in pri opazovanju velikih produkcijskih sistemov kažejo na ozko grlo prav v širini komunikacijskih poti in strojne opreme.

#### **4.1.6 Administratorske pravice**

Pravice, ki jih administrator strežnika IMiS®/ARChive Server pri svojem delu potrebuje, so ekvivalentne korenskemu uporabniku `root`. Pravice navadno dodeli administrator strežnika in morajo zadoščati za namestitvev, nadgradnjo in administriranje strežnika.

Za svoje delovanje ne potrebuje posebnih pravic.

Namestitvena skripta strežnika IMiS®/ARChive Server pri namestitvi ustvari uporabniški račun `iarc` in skupino `iarc` s katerim so zagnani vsi procesi strežnika.

V primeru napada preko morebitne napake v aplikacijski kodi strežnika je s tem onemogočen kakršen koli prevzem pravic korenskega uporabnika.

#### **4.1.7 Nadzor delovanja strojne opreme**

Večina proizvajalcev strojne strežniške opreme ob nakupu strežnika priloži tudi sistem za nadzor strojne opreme (npr. IBM Tivoli, HP Insight Systems Manager, Dell OpenManage).

Uporaba takega sistema je zelo priporočljiva, ko pride do težav pri delovanju opreme ali v primeru, ko nadzorniki sistema potrebujejo podatke o delovanju strežnikov.

Priporočljivo je tudi, če nadzorni sistem omogoča sporočanje napak pri delovanju sistemov preko mobilnih telefonov ali elektronske pošte.

#### **4.1.8 Minimalne zahteve**

Minimalne zahteve za strojno opremo za delovanje strežnika:

- Strežnik z Intel Pentium x86 ali x86\_64 procesorjem 800Mhz ali drugim kompatibilnim procesorjem z x86 arhitekturo (glej minimalne zahteve namestitvene platforme – operacijskega sistema).
- 1GB RAM (glej minimalne zahteve namestitvene platforme – operacijskega sistema in prištej 512 MB).

- Ustrezna diskovna kapaciteta za pričakovan obseg arhiviranih vsebin, minimalno 1GB za delovanje strežnika.
- Dostop do omrežja po TCP/IP protokolu (IPv4 ali IPv6).
- Katerakoli strojna oprema, ki nudi podporo izvajanju Linux operacijskega sistema z navedenimi podprtimi distribucijami v omrežnem načinu.

#### 4.1.9 Priporočene zahteve

Priporočene zahteve za strojno opremo za delovanje strežnika:

- Strežnik z več-jedrnim Intel Xeon E5/E7 ali Xeon 5xxx/6xxx/7xxx (x86\_64) procesorjem 2GHz (ali zmogljivejšim).
- 4GB SDRAM (DDR3/DDR4) visokih frekvenc ali več.
- Hitra matična plošča z Front Side Bus-om višjih frekvenc (1GHz ali hitreje).
- Volumni na RAID5 logičnih diskih/particijah (vnaprej predvideni 3-5 letni prirast prostora na diskih).
- SCSI/SAS kontrolerji z write-back cache zmožnostmi (do 40% boljša učinkovitost), priporočljivo je 128MB cache ali več s podporo baterijskemu napajanju ali flash spominu v primeru prekinitve napajanja \*.
- Hitri SCSI/SAS diski (10k/15k RPM) z ustreznim predpomnjenjem \*.
- Redundantno napajanje z vzpostavljenim sistemom hlajenja.
- Redundantni omrežni priklon 1Gbps ali več z IPv4 ali IPv6 protokolom.

*\* diskovni podsistem lahko zamenjamo z ustreznimi omrežnimi SAN volumni, ki so performančno primerljivi priporočenim lokalnim diskovnim kapacitetam.*

*\* Produkt normalno deluje tudi v svetovno priznanih virtualizacijskih okoljih kot so VMware ESX/ESXi, Microsoft Hyper-V, Oracle VM ipd. v kolikor so mu zagotovljeni ustrezni virtualni resursi, ki omogočajo podobno performančno okolje, kot ga dosegamo z zgornjo priporočeno strojno opremo.*



## 4.2 Programska oprema

### 4.2.1 Operacijski sistemi

Strežnik IMiS®/ARChive Server deluje na operacijskem sistemu x86/x86\_64, na distribucijah Red Hat in SuSE z naslednjimi derivati:

- RHEL 4.x
- RHEL 5.x
- RHEL 6.x
- CentOS 4.x
- CentOS 5.x
- CentOS 6.x
- SLES 11.x
- SLES 12.x
- OpenSuSE 11.x
- OpenSuSE 12.x.

### 4.2.2 Minimalne zahteve

Minimalne zahteve za delovanje strežnika:

Operacijski sistem Linux (RedHat EL/Fedora, SuSE SLES/OpenSuSE). Zasnovan mora biti na kateremkoli 2.6.x jedru.

Minimalne zahteve za delovanje spletnega administracijskega vmesnika:

Deluje v vseh priljubljenih brskalnikih na Windows, MacOS in drugih operacijskih sistemih.

Storitev administracijskega vmesnika:

- Java 8 Runtime Environment verzije 1.8.0\_172,
- Apache Tomcat 9.0.x
- Podprti operacijski sistemi:\*
- Solaris 11.x, 10 update 9;
  - Windows 10; Windows 8.x; Windows 7 SP1; Windows Vista SP2;
  - Windows server 2012 R2 (64-bit); Windows server 2012 (64-bit); Windows server 2008 R2 SP1 (64-bit);
  - Oracle Linux 7.x (64-bit), 6.x, 5.5+;
  - Red Hat Enterprise Linux 7.x (64-bit), 6.x, 5.5+;
  - Suse Linux Enterprise Linux 12.x (64-bit), 11.x, 10 SP2;
  - Ubuntu Linux 15.10, 15.04, 14.x, 13.x, 12.04 - LTS;
  - OS X 10.9 in novejši (64-bit), 10.8.3+ (64-bit).

Za svoje delovanje potrebuje malo virov.

- Brskalniki:
  - Chrome ≥ 66.0.3359
  - Firefox ≥ 60.0.1
  - Edge ≥ 42.17134
  - Safari ≥ 11.1
  - Internet Explorer 11 ≥ 11.0.10240.16384.
- Velikost delovnega spomina naj bo cca 512 MB večja od zahteve po spominu operacijskega sistema.
- Dostop do omrežja po TCP/IP protokolu (IPv4 ali IPv6).

### 4.2.3 Priporočene zahteve

Priporočene zahteve za delovanje strežnika:

Operacijski sistem Linux (RedHat EL/Fedora, SuSE SLES/OpenSuSE). Zasnovan mora biti na kateremkoli 2.6.x jedru.

Pri namestitvi in delovanju strežnika IMiS®/ARChive Server mora operacijski sistem zagotoviti orodja in knjižnice operacijskega sistema Linux, ki so lahko sestavni del različnih namestitvenih paketov operacijskega sistema. Za več informacij glej poglavje [Seznam obveznih sistemskih orodij](#) in [Seznam obveznih sistemskih knjižnic](#).

Priporočene zahteve za delovanje spletnega administracijskega vmesnika:

- Brskalniki:
  - Chrome ≥ 66.0.3359
  - Firefox ≥ 60.0.1
  - Edge ≥ 42.17134
  - Safari ≥ 11.1
  - Internet Explorer ≥ 7.
- Velikost delovnega spomina naj bo cca 1 GB večja od zahteve po spominu operacijskega sistema.
- Dostop do omrežja po TCP/IP protokolu (IPv4 ali IPv6).

#### 4.2.4 Seznam obveznih sistemskih orodij

bash	(več na: <a href="http://www.linuxmanpages.com/man1/bash.1.php">http://www.linuxmanpages.com/man1/bash.1.php</a> )
chmod	(več na: <a href="http://www.linuxmanpages.com/man1/chmod.1.php">http://www.linuxmanpages.com/man1/chmod.1.php</a> )
chown	(več na: <a href="http://www.linuxmanpages.com/man1/chown.1.php">http://www.linuxmanpages.com/man1/chown.1.php</a> )
cp	(več na: <a href="http://www.linuxmanpages.com/man1/cp.1.php">http://www.linuxmanpages.com/man1/cp.1.php</a> )
echo	(več na: <a href="http://www.linuxmanpages.com/man1/echo.1.php">http://www.linuxmanpages.com/man1/echo.1.php</a> )
grep	(več na: <a href="http://www.linuxmanpages.com/man1/grep.1.php">http://www.linuxmanpages.com/man1/grep.1.php</a> )
mv	(več na: <a href="http://www.linuxmanpages.com/man1/mv.1.php">http://www.linuxmanpages.com/man1/mv.1.php</a> )
ps	(več na: <a href="http://www.linuxmanpages.com/man1/ps.1.php">http://www.linuxmanpages.com/man1/ps.1.php</a> )
pwd	(več na: <a href="http://www.linuxmanpages.com/man1/pwd.1.php">http://www.linuxmanpages.com/man1/pwd.1.php</a> )
rm	(več na: <a href="http://www.linuxmanpages.com/man1/rm.1.php">http://www.linuxmanpages.com/man1/rm.1.php</a> )
rmdir	(več na: <a href="http://www.linuxmanpages.com/man1/rmdir.1.php">http://www.linuxmanpages.com/man1/rmdir.1.php</a> )
rpm	(več na: <a href="http://www.linuxmanpages.com/man8/rpm.8.php">http://www.linuxmanpages.com/man8/rpm.8.php</a> )
sed	(več na: <a href="http://www.linuxmanpages.com/man1/sed.1.php">http://www.linuxmanpages.com/man1/sed.1.php</a> )
sh	(več na: <a href="http://www.linuxmanpages.com/man1/sh.1.php">http://www.linuxmanpages.com/man1/sh.1.php</a> )
su	(več na: <a href="http://www.linuxmanpages.com/man1/su.1.php">http://www.linuxmanpages.com/man1/su.1.php</a> )
touch	(več na: <a href="http://www.linuxmanpages.com/man1/touch.1.php">http://www.linuxmanpages.com/man1/touch.1.php</a> )
ip	(več na: <a href="http://www.linuxmanpages.com/man7/ip.7.php">http://www.linuxmanpages.com/man7/ip.7.php</a> )
ldconfig	(več na: <a href="http://www.linuxmanpages.com/man1/ps.1.php">http://www.linuxmanpages.com/man1/ps.1.php</a> )
awk	(več na: <a href="http://www.linuxmanpages.com/man1/awk.1.php">http://www.linuxmanpages.com/man1/awk.1.php</a> )
find	(več na: <a href="http://www.linuxmanpages.com/man1/find.1.php">http://www.linuxmanpages.com/man1/find.1.php</a> )
id	(več na: <a href="http://www.linuxmanpages.com/man1/id.1.php">http://www.linuxmanpages.com/man1/id.1.php</a> )
ipcrm	(več na: <a href="http://www.linuxmanpages.com/man8/ipcrm.8.php">http://www.linuxmanpages.com/man8/ipcrm.8.php</a> )
ipcs	(več na: <a href="http://www.linuxmanpages.com/man8/ipcs.8.php">http://www.linuxmanpages.com/man8/ipcs.8.php</a> )
killall	(več na: <a href="http://www.linuxmanpages.com/man1/killall.1.php">http://www.linuxmanpages.com/man1/killall.1.php</a> )
setsid	(več na: <a href="http://www.linuxmanpages.com/man2/setsid.2.php">http://www.linuxmanpages.com/man2/setsid.2.php</a> )
groupadd	(več na: <a href="http://www.linuxmanpages.com/man8/groupadd.8.php">http://www.linuxmanpages.com/man8/groupadd.8.php</a> )
useradd	(več na: <a href="http://www.linuxmanpages.com/man8/useradd.8.php">http://www.linuxmanpages.com/man8/useradd.8.php</a> )

#### 4.2.5 Seznam obveznih sistemskih knjižnic

libc.so.6  
libm.so.6  
libpthread.so.0  
libstdc++.so.6  
libdl.so.2  
libgcc\_s.so.1  
librt.so.1  
libbz2.so.1  
libz.so.1  
rpmli

## 5 NAMESTITEV

V nadaljevanju je opisan postopek namestitve strežnika IMiS®/ARChive Server in spletnega administracijskega vmesnika.

### 5.1 Postopek namestitve

Namestitev strežnika IMiS®/ARChive Server lahko opravi korenski uporabnik (`root`) ali uporabnik z ekvivalentnimi pravicami (`sudo`) s pomočjo konzolnih orodij.

Mogoče ga je opraviti le v okolju, ki izpolnjuje vsaj minimalne zahteve za namestitev ene od podprtih Linux distribucij. Minimalne zahteve nadgradimo v skladu s predvidenimi potrebami.

Za več informacij glej poglavje [Strojna oprema](#) in [Programska oprema](#).

Postopek poteka po korakih in je enoten za vse ciljne skupine oseb, ki strežnik nameščajo.

#### Korak 1

V konzolo operacijskega sistema se prijavimo kot `root` uporabnik ali ukaze izvajamo z ekvivalentom `root` uporabnika preko orodja `sudo`. Diskovni pogoni, ki so predvideni za uporabo strežnika IMiS®/ARChive Server, naj bodo predhodno pripravljene in dostopne v datotečnem sistemu. Lokacija `/iarc` je privzeta za večino datotek strežnika (podatkovna baza, datoteke dokumentov, ...). Namestitev opravimo z orodjem `rpm`, ki je sestavni del podprtih Linux distribucij.

#### Korak 2

Izvedemo ukaz `rpm` za namestitev namestitvenega paketa:

```
[user1@iarc ~]# sudo rpm -ivh imisarc.10.3.2210-750.0001.el8.x86_64.rpm
```

Ime paketa za namestitev je lahko tudi drugačno. Odvisno je od Linux distribucije in verzije strežnika IMiS®/ARChive Server.

#### Korak 3

Ob uspešni namestitvi se izpiše naslednje (izpis se lahko spreminja glede na uporabljeno Linux distribucijo):

```
Preparing      ##### [100%]
1:imisarc      ##### [100%]
Performing POSTINSTALLATION Actions
POSTINSTALLATION Actions Done
```

#### Korak 4

Postopek namestitve ustvari naslednje imenike in datoteke:

/iarc/db in	
/iarc/db/iarc	Imenika, ki vsebujeta datoteke podatkovne baze strežnika.
/iarc/fti	Imenik, ki vsebuje podatkovno bazo sistema za iskanje po polnem besedilu dokumentov.
/iarc/vol	Imenik, ki vsebuje volumne, kamor strežnik IMiS®/ARChive Server shranjuje datoteke dokumentov.
/iarc/wcache	Imenik, ki ga strežnik uporablja za predpomnenje datotek dokumentov pri nastajanju ali urejanju.
/iarc/rcache	Imenik za predpomnenje datotek dokumentov, za katere uporabniki podajo zahtevo za pregledovanje.
/iarc/work	Imenik, v katerem strežnik shranjuje datoteke začasne narave pri posameznih procesih.
/opt/IS/imisarcd	Vsebuje izvajalne datoteke in knjižnice, ki jih strežnik potrebuje za svoje delovanje.
/etc/iarc.conf	Konfiguracijska datoteka strežnika.
/etc/init.d/iarc	Zagonska skripta strežnika.

Namestitev spletnega administracijskega vmesnika lahko izvede uporabnik z ustreznimi pravicami na strežniku, kamor ga namešča (administrator). Pred pričetkom namestitve mora administrator zaustaviti Apache Tomcat strežnik.

V nadaljevanju je opisan postopek namestitve po korakih:

1. Namesti podatkovno bazo (podprte so PostgreSQL, Apache Derby in SQLite).
2. Namesti Tomcat strežnik.
3. Doda knjižnico podatkovne baze v Tomcat .../lib.
4. Razširi WAR datoteko v direktorij .../webapps/<project name>.
5. Doda projekt v .../conf/server.xml datoteko.
6. Nastavi konfiguracijo storitve .../webapps/<project name>/WEB-INF/web.xml.
7. Razširi namestitveni paket spletnega vmesnika v imenik na strežniku.
8. Nastavi settings.json spletnega vmesnika.
9. Zažene Apache Tomcat strežnik.

**Konfiguracijska datoteka storitve administracijskega vmesnika web.xml**

com.imis.archive.admin.service.database.url	String	Naslov podatkovne baze. Podprte začetne vrednosti: - jdbc:postgresql, - jdbc:derby, - jdbc:sqlite.  Primer: jdbc:postgresql://localhost:5432/i aa_dev
com.imis.archive.admin.service.database.username	String	Uporabniško ime.
com.imis.archive.admin.service.database.password	String	Geslo.
com.imis.archive.admin.service.database.provider	String	Vrednost določa knjižnico, ki se bo uporabljala za dostop do baze (opcijsko).  Primer: org.sqlite.JDBC

**Primer konfiguracije datoteke web.xml**

```

<web-app ...>

...

<context-param>
  <param-name>com.imis.archive.admin.service.database.url</param-name>
  <param-value>/etc/isc/config.xml</param-value>
</context-param>
<context-param>
  <param-name>com.imis.archive.admin.service.database.username</param-name>
  <param-value>user</param-value>
</context-param>
<context-param>
  <param-name>com.imis.archive.admin.service.database.password</param-name>
  <param-value>password</param-value>
</context-param>

...

</web-app>

```

**Konfiguracijska datoteka spletnega administracijskega vmesnika settings.json**

url	String	Naslov storitve administracijskega vmesnika.  Primer: https://apps.imis.si/isc/iaaservice/
-----	--------	---

**Primer konfiguracije datoteke spletnega vmesnika settings.json**

```
{
  "url": "https://apps.imis.si/isc/iaaservice/"
}
```

**5.2 Ponamestitveni postopki**

Po-namestitvene postopke strežnika IMiS®/ARChive Server lahko opravi korenski uporabnik ali uporabnik z ekvivalentnimi pravicami (administrator, tehnično osebje, ...).

**5.2.1 Nastavitev števila hkrati odprtih datotek**

Vsak proces na Linux operacijskem sistemu potrebuje za delovanje določene pravice.

To dosežemo tako, da proces teče s privilegiji določenega uporabniškega računa, kateremu dodelimo ustrezne pravice. Poleg namestitve datotek postopek namestitve ustvari tudi uporabniški račun z imenom `iarc`.

Po namestitvi je potrebno ročno nastaviti še največje število hkrati odprtih datotek za uporabniški račun strežnika IMiS®/ARChive Server. Priporočena vrednost je največ 4096 hkrati odprtih datotek.

Nastavitev uredimo v datoteki `/etc/security/limits.conf` tako, da vpišemo naslednji dve vrstici:

```
iarc          soft          nofile        4096
iarc          hard          nofile        4096
```

Pravice lahko nastavimo tudi za vse uporabnike, ki pripadajo skupini `iarc`, čeprav to eksplicitno ni potrebno:

```
@iarc        soft          nofile        4096
@iarc        hard          nofile        4096
```

Enak učinek je možno doseči tudi z zaustavitvijo datoteke `/etc/security/limits.d/iarc.conf`, v katero vnesemo zgornji dve vrstici, za uporabnika ali skupino.

Odločitev za en ali drug pristop naj temelji na:

- notranjih pravilih izvajanja systemske administracije strežnika, kamor se strežnik IMiS®/ARChive Server namešča;
- osebni preferenci glavnega systemskega administratorja – skrbnika.

`pam_limits` modul PAM arhitekture (Pluggable Authentication Modules for Linux, [http://en.wikipedia.org/wiki/Linux\\_PAM](http://en.wikipedia.org/wiki/Linux_PAM)) namreč upošteva vse nastavitvene ukaze iz direktorija `/etc/security/limits.d/`, kot tudi samo nastavitveno datoteko `/etc/security/limits.conf`.

## 5.2.2 Nastavitev samodejnega zagona

Ob namestitvi je strežnik IMiS®/ARChive Server nastavljen na samodejni zagon.

Samodejni zagon strežnika ob zagonu operacijskega sistema lahko nastavimo tudi ročno:

- za RHEL in CentOS distribucije z ukazom: **`chkconfig iarc on`**;
- za SLES in OpenSuSE distribucije z ukazom: **`chkconfig iarc on`** ali **`yast`** (`yast`: standardno nastavitveno orodje v SLES in OpenSuSE distribucijah).

Nastavitev samodejnega zagona strežniške storitve lahko preverimo:

- za RHEL in CentOS distribucije z ukazom: **`chkconfig iarc --list`**;  
(izpiše na katerih nivojih se servis samodejno zažene).
- za SLES in OpenSuSE distribucije z ukazom: **`chkconfig iarc --list`** ali **`yast`**.

Pomembno je, da se servis zažene na nivoju 3 in 5 kar potrjuje naslednji izpis:

```
[user1@iarc ~]# sudo chkconfig iarc --list  
iarc    0:off 1:off 2:on 3:on 4:on 5:on 6:off
```



## 5.3 Preizkušanje namestitve in nastavitvev

Preizkus uspešnosti namestitve lahko opravimo v nekaj korakih:

### Korak 1

V nastavitveni datoteki `/etc/iarc.conf`, v sekciji [Log], nastavimo parameter `LogLevel` na vrednost 7 in zaženemo IMiS®/ARChive Server strežniško storitev.

Izpiše se sporočilo:

```
[user1@iarc ~]# sudo service iarc start
Starting IMiS/ARChive HSM Storage Server:      [ OK ]
```

### Korak 2

Z ukazom `ps tree -G` preverimo stanje delujočih procesov in njihovih niti.

Izpiše se seznam, katerega del je tudi (izpis se lahko spreminja glede na distribucijo):

```
[user1@iarc ~]# sudo ps tree -G
```

```
init ──┬─ ...
...
├─ iarcd ── 50*[{iarcd}]
```

Izpis predstavlja glavni proces »iarcd« s 50 nitmi.

### Korak 3

Z ukazom `netstat -tan` preverimo ali povezovalni in administrativni proces strežnika IMiS®/ARChive Server na TCP vratih, določenih v `iarc.conf` pričakujeta zahteveke.

V primeru, da so nastavljena privzeta TCP vrata, izpis vsebuje:

```
[user1@iarc ~]# netstat -tan
Proto Recv-Q Send-Q Local Address Foreign Address  State
...
tcp    0      0 *.16807      *.*          LISTEN
tcp    0      0 *.16808      *.*          LISTEN
```

## 6 NADGRADNJA

Nadgradnjo strežnika IMiS®/ARChive Server lahko opravi korenski uporabnik ali uporabnik z ekvivalentnimi pravicami (administrator, tehnično osebje, ...).

Ob nadgradnji je potrebno izvesti nekatere izmed postopkov opisanih v nadaljevanju.

V kolikor je preskok verzije strežnika večji (npr. ob nadgradnji na višjo glavno verzijo), je potrebno izvesti vse navedene postopke:

- Preverjanje konsistentnosti interne baze podatkov strežnika.
- Izvoz interne baze podatkov strežnika.
- Nadgradnja izvajalnih programov.
- Nadgradnja knjižnic (opsijsko).
- Razširitev sheme baze podatkov strežnika.
- Uvoz baze podatkov strežnika potem, ko je bila shema razširjena.
- Ureditev pravic in lastništva na datotekah strežnika.

### 6.1 Postopek nadgradnje

Nadgradnjo strežnika IMiS®/ARChive Server lahko izvede administrator po naslednjem postopku:

#### Korak 1

Pred nadgradnjo je potrebno opraviti izvoz baze strežnika IMiS®/ARChive Server in narediti varnostno kopijo po postopku, kot je opisan v različnih poglavjih te dokumentacije.

#### Korak 2

Nadgradnja je lahko precej dolgotrajna, kar je odvisno predvsem od števila objektov, ki jih hrani strežnik IMiS®/ARChive Server. Nadgradimo ga z ukazom:

```
luser1@iarc ~]# sudo rpm -Uvh imisarc.10.3.2210-750.0001.el8.x86_64.rpm
```

Ob pravilnem delovanju proces nadgradnje izpiše vsebino, podobno spodnji (variacije so odvisne od distribucije Linux sistema):

```
Shutting down IMiS/ARChive HSM Storage Server:      [ OK ]
Verifying IMiS/ARChive HSM Storage Server Database (BDB edition) integrity (this may take a while depending
on your object store size)...
Database is consistent!
Exporting IMiS/ARChive HSM Storage Server Database (this may take a while depending on your object store
size)...
Database Export succesfull! Upgrade can proceed.
Performing POSTINSTALLATION Actions
Importing exported database files (this may take a while depending on your object store size)...
Done.
```

### Korak 3

Po nadgradnji je smiselno preveriti uspešnost prenosa obstoječega stanja interne baze podatkov strežnika IMiS®/ARChive Server z izvozom baze podatkov in verifikacijo smiselnosti vpisov v tekstovne datoteke baze, preverjanjem lastništva datotek in imenikov volumnov in vsebine datoteke `/etc/iarc.conf`.

Pred pričetkom nadgradnje spletnega administracijskega vmesnika mora administrator zaustaviti Apache Tomcat strežnik.

Postopek nadgradnje izvede po naslednjih korakih:

1. Naredi kopijo trenutne konfiguracije, ki se nahaja na `.../webapps/<project name>/WEB-INF/web.xml` v začasen direktorij (izven `.../webapps/<project name>/`).
2. Izbriše direktorij `.../webapps/<project name>`.
3. Razširi `.war` datoteko v direktorij `.../webapps/<project name>`.
4. Zamenja `.../webapps/<project name>/WEB-INF/web.xml` s prejšnjo datoteko (iz koraka 1).
5. Naredi kopijo trenutnih nastavitev spletnega vmesnika »`assets/settings.json`« v začasen imenik.
6. Izbriše imenik spletnega vmesnika, kjer se nahajajo datoteke spletnega administracijskega vmesnika.
7. Razširi namestitveni paket spletnega vmesnika v imenik.
8. Zamenja `settings.json` spletnega vmesnika iz začasnega imenika.
9. Zažene Tomcat strežnik.

## 6.2 Možni zapleti pri nadgradnji

### Opis pogostega zapleta 1

Ob poizkusu nadgradnje se pojavi napaka:

```
error: can't create transaction lock on /var/lib/rpm/.rpm.lock (Permission denied)
```

### Razlog zapleta 1

Uporabnik, ki izvaja nadgradnjo, nima ustreznih pravic.

### Rešitev zapleta 1

Za nadgradnjo se je potrebno prijaviti kot korenski uporabnik ali pa mora uporabnik uporabljati pripomočke, ki mu zagotovijo pravice ekvivalentne korenskemu (sudo).

### Opis pogostega zapleta 2

Ob poizkusu nadgradnje se pojavi opozorilo:

```
Changing ownership of volume mountpoint "/iarc/vol/vol00" recursively to iarc:iarc (this may take a while).  
WARNING: Operation failed. You will need to grant access to directories and objects for user iarc group iarc  
manually.
```

### Razlog zapleta 2

Ob urejanju pravic volumen na lokaciji /iarc/vol/vol00 ni bil dosegljiv ali obstaja nek drug razlog, ki preprečuje korenskemu uporabniku spremembo lastništva datotek in imenikov volumna.

### Rešitev zapleta 2

Potrebno je povezati diskovne pogone, kjer se nahajajo manjkajoči volumni (v našem primeru je med njimi /iarc/vol/vol00) in ročno nastaviti lastništvo nad imeniki in datotekami z ukazom:

```
[user1@iarc ~]# sudo chown <iarc uporabnik>:<iarc skupina><pot> -R
```

V našem primeru:

```
[user1@iarc ~]# sudo chown iarc:iarc /iarc/vol/vol00 -R
```

### Opis pogostega zapleta 3

Ob poizkusu nadgradnje se pojavi napaka:

```
ERROR: IMiS/ARChive Storage Server BDB Database consistency check reported an error in one of the
database entities. Manually run '/opt/IS/imisarc/dbtool -a check' from directory /iarc/db to get extended error
information. IMiS/ARChive upgrade can proceed only when database is consistent. You need to manually verify
and remove any inconsistency of the database. UPGRADE ABORTED!
```

### Razlog zapleta 3

Interna baza strežnika IMiS®/ARChive Server ni dostopna ali pa je okvarjena.

### Rešitev zapleta 3

Preverimo ali imenik, kjer se nahaja podatkovna baza strežnika obstaja. Preverimo tudi, da imenik ni prazen ter da so v njem urejene pravice uporabnika, ki izvaja procese strežnika.

Nato zaženemo ukaz:

```
[user1@iarc ~]# sudo su - iarc -s /bin/bash -c "cd /opt/IS/imisarc && ./dbtool -f <pot do strežniške
konfiguracijske datoteke> -h <pot do interne baze> -w <pot do interne baze> -a check
```

V našem primeru:

```
[user1@iarc ~]# sudo su - iarc -s /bin/bash -c "cd /opt/IS/imisarc && ./dbtool -f /etc/iarc.conf -h
/iarc/db -w /iarc/db -a check
```

Ukaz nam bo izpisal več podatkov o okvari baze. V primeru, da napaka presega obseg znanj administratorja, ki upravlja s produktom, lahko uporabi poti, ki jih določa sklenjena vzdrževalna pogodba ali drug dogovor in napako po nasvetu s strani proizvajalca odpravi s pomočjo vzdrževalnega osebja proizvajalca.

## 7 ODSTRANITEV

Postopek odstranitve strežnika IMiS®/ARChive Server lahko izvede korenski uporabnik ali uporabnik z ekvivalentnimi pravicami (administrator, tehnično osebje, ...).

### 7.1 Postopek odstranitve

#### Korak 1

V `rpm` bazi preverimo verzijo nameščenega strežnika IMiS®/ARChive Server (izpis se lahko spreminja v odvisnosti od uporabljene distribucije):

```
[user1@iarc ~]#.sudo rpm -q imisarc
imisarc.10.3.2210-750.0001.el8.x86_64.rpm
[user1@iarc ~]#
```

#### Korak 2

Ustavimo IMiS®/ARChive Server strežniško storitev.

To dejanje implicitno izvede sicer tudi dejanje odstranitve v primeru, da zazna delujočo in zagnano storitev.

#### Korak 3

Z `rpm` ukazom izvedemo de-instalacijo namestitvenega paketa strežnika IMiS®/ARChive Server. Potrebno je vpisati celoten naziv iz `rpm` baze, kot je to razvidno iz Koraka 1:

```
[user1@iarc ~]# sudo rpm -e imisarc.10.3.2210-750.0001.el8.x86_64.rpm
```

This uninstall action WILL NOT:

- \* remove IMiS/ARChive configuration file (e.g.: `/etc/iarc.conf`)
- \* remove IMiS/ARChive database files
- \* remove IMiS/ARChive log files (location set in `/etc/iarc.conf`)
- \* remove IMiS/ARChive pid file (location in `/var/run/iarc` or overridden in `/etc/iarc.conf`)
- \* remove IMiS/ARChive stored objects (on all your volume mountpoints)
- \* remove IMiS/ARChive process user (`iarc`) and group (`iarc`) accounts from `/etc/passwd` and `/etc/group`

Above actions should be performed manually if required!

Uninstall complete.

```
[user1@iarc ~]#
```

Pred pričetkom odstranitve spletnega vmesnika administracije mora administrator zaustaviti Apache Tomcat strežnik.

Postopek odstranitve izvede po naslednjih korakih:

1. Izbriše imenik `.../webapps/<project name>`.
2. Izbriše imenik spletnega vmesnika, kjer se nahajajo datoteke spletnega administracijskega vmesnika.
3. Odstrani podatkovno bazo.
4. Zažene Apache Tomcat strežnik.

## 8 UPRAVLJANJE PRODUKTA

S strežnikom IMiS®/ARChive Server lahko upravlja korenski uporabnik ali uporabnik z ustreznimi pravicami (administrator, tehnično osebje, ...).

Zaradi enostavnosti uporabe lahko določene nastavitve upravlja preko spletnega administracijskega vmesnika ali spletnega odjemalca IMiS®/wClient :

- Pravice dostopa uporabnikov in skupin do entitet in uporabniško določenih atributov.
- Uporabniško določeni atributi.
- Nabor vrednosti atributov.
- Globine drevesa entitet v načrtu razvrščanja gradiva in načina zapisa klasifikacijske oznake za posamezno vrsto entitete na določenem nivoju.
- Uporabniki in skupine s pripadajočimi podatki o uporabniku, avtentikaciji, vlogah in članstvu v skupinah.
- Predloge z uporabniško določenimi atributi.
- Profili strežnika.
- Volumni strežnika.

Podrobnejše informacije so na voljo v poglavju [Konfiguracija strežnika v uporabniškem priročniku IMiS®/Client](#).

### 8.1 Postopek zagona in zaustavitve

Za zagon in zaustavitev strežnika IMiS®/ARChive Server uporabimo zagonsko skripto.

Skripta `iarcd` se v primeru uporabe distribucije RHEL ali CentOS nahaja v imeniku `/etc/rc.d/init.d`, v primeru SLES ali OpenSuSE pa v imeniku `/etc/init.d`.

Zagonsko skripto uporabimo z orodjem `service` na naslednji način:

```
[user1@iarc ~]# sudo service iarcd <ukaz>
```

Veljavne vrednosti opcije `<ukaz>` zagonske skripte so:

`start` Ukaz zažene strežnik IMiS®/ARChive Server.

V primeru uspešnega zagona skripta izpiše:

```
Starting IMiS/ARChive HSM Storage Server: [ OK ],
```

v primeru neuspešnega zagona pa:

```
Starting IMiS/ARChive HSM Storage Server: [FAILED].
```



- stop** Ukaz zaustavi delovanje strežnika IMiS®/ARChive Server.  
V primeru uspešne zaustavitve skripta izpiše:  
Shutting down IMiS/ARChive HSM Storage Server: [ OK ],  
v primeru neuspešne zaustavitve pa:  
Shutting down IMiS/ARChive HSM Storage Server: [FAILED].
- restart** Ukaz izvede ponovni zagon (angl. Restart) strežnika IMiS®/ARChive Server.  
Dejansko gre za sosledje ukazov `start` in `stop` zato so tudi izpisi na konzolo enaki, kot če bi zaporedno izvedli oba ukaza.
- status** Ukaz izpiše stanje servisa strežnika IMiS®/ARChive Server.  
V primeru, da ta deluje izpiše tudi identifikacijski številki procesa:  
Status of IMiS/ARChive HSM Storage Server: iarcd (pid 6222 6216) is running ...  
v primeru, da je servis ustavljen pa:  
Status of IMiS/ARChive HSM Storage Server: iarcd is stopped

Več informacij o morebitnih težavah pri zagonu strežnika IMiS®/ARChive Server je na voljo v poglavju [Odpravljanje težav](#).

## 8.2 Konfiguriranje

Konfiguriranje opravi korenski uporabnik `root` ali uporabnik s pravicami ekvivalentnimi korenskemu uporabniku preko orodja `sudo` tako, da se izvajajo s poverilnicami uporabniškega računa strežnika IMiS®/ARChive Server, saj lahko v nasprotnem primeru pride do okvare interne baze.

## 8.2.1 Predvidena opravila

Konzolna orodja za delo z interno bazo strežnika IMiS®/ARChive Server so:

**dbtool** Orodje administratorju strežnika omogoča upravljanje z interno bazo podatkov. Proces izvažanja baze lahko izvajamo pri delujočem strežniku. Proces uvažanja baze pa se lahko izvaja le, ko strežnik ne deluje.

### Sintaksa:

usage: dbtool [-f db\_config\_file] [-q(quiet)] [-w working\_dir] [-v version] [-o override][-a | -t tables[:name],...] exp | imp | init | del

### Tables:

acle - acl entry table  
 aclv - acl entry validity table  
 at - attribute table  
 ag - attribute group table  
 av - attribute value table  
 ab - attribute binary table  
 dt - attribute date-time table  
 db - attribute double table  
 fi - attribute file table  
 i4 - attribute int32 table  
 i8 - attribute int64 table  
 i16 - attribute int128 table  
 i16i - attribute int128 index table  
 sm - attribute max string table  
 s10 - attribute value string 10  
 s20 - attribute value string 20  
 s30 - attribute value string 30  
 s40 - attribute value string 40  
 s50 - attribute value string 50  
 s100 - attribute value string 100  
 s200 - attribute value string 200  
 s20i - attribute value string 20 index  
 s30i - attribute value string 30 index  
 s40i - attribute value string 40 index  
 s50i - attribute value string 50 index  
 s100i - attribute value string 100 index  
 s200i - attribute value string 200 index  
 u4 - attribute value uint32  
 u8 - attribute value uint64  
 u16 - attribute value uint128  
 u16i - attribute value uint128 index  
 au - audit  
 cx - compression  
 mi - content type  
 cnt - counter table  
 dsc - digital certificate

cbdy - certificate body  
ajts - aip job timestamp  
dsi - digital signature  
de - directory entry  
dea - directory entry alias  
dg - directory entry group  
ent - entity  
cl - entity class  
do - entity document  
fl - entity folder  
lo - lookup table  
h128 - 128 bit hash table  
h160 - 160 bit hash table  
h224 - 224 bit hash table  
h256 - 256 bit hash table  
h384 - 384 bit hash table  
h512 - 512 bit hash table  
rets - revocation data/timestamp bind table  
resig - revocation data/digital signature bind table  
tsaip - timestamp/aip bind table  
cxl - compression library  
pr - profile  
prop - property  
sd - storage driver  
tm - template  
ta - template attribute  
tb - template bind  
aip - archival information package  
aipq - archival information package queue  
caq - create aip queue  
revo - revocation data  
fti - full text indexing queue record  
ts - timestamp  
tsr - timestamp rule  
vo - volume  
fd - file description  
null - attribute value null value  
revq - review queue  
cb - content bind  
t4 - tokens up to 4 bytes in length  
t8 - tokens up to 8 bytes in length  
tmax - tokens up to 30 bytes in length  
se - server events and stats

GetStorageInfo Orodje za konfiguracijo profilov in volumnov ter podatke o zasedenosti.

**Sintaksa:**

usage: GetStorageInfo [ path-to-iarc.conf]

(skupaj s potjo, če se ta ne nahaja na privzeti lokaciji – /etc .])

### 8.3 Beleženje dogodkov delovanja

Beleženje dogodkov je namenjeno preverjanju delovanja, ki jo občasno, oziroma po potrebi izvaja administrator strežnika ali administrator strežnika IMiS®/ARChive Server. IMiS®/ARChive Server beleži dogodke glede na nastavitev nivoja beleženja v nastavitveni datoteki `/etc/iarc.conf`. Privzeta lokacija dnevnikov je v imeniku `/var/log/iarc`. Aktivni dnevnik, v katerega IMiS®/ARChive Server beleži trenutne dogodke, se nahaja na lokaciji `/var/log/iarc/iarc.log`. Starejši dogodki so shranjeni v arhivskih datotekah dnevnika, ki se v odvisnosti od nastavitve ustvarjajo po potrebi z naslovno shemo `/var/log/iarc/iarc.XX.log` (XX = sekvenca arhivske datoteke, večja številka predstavlja dogodke, ki so se zgodili dlje v zgodovini). Beleženje v dnevnike IMiS®/ARChive Server izvaja po FILO principu »FILO – first in/last out« (prvi notri – zadnji ven).

Število arhivskih dnevnikov in njihovo velikost nastavimo v nastavitveni datoteki `/etc/iarc.conf`, v razdelku `[Log]`. Čas, ko informacija iz dnevnika izpade, prilagajamo z nastavitvijo števila in velikosti dnevnikov glede na količino vpisov. Dobra praksa narekuje nastavitve, ki omogočajo hranjenje informacij nivoja 6 najmanj tri mesece.

Nivojev beleženja je 7. Vsak nivo pomeni stopnjo podrobnosti informacij, ki jih strežnik IMiS®/ARChive Server beleži v dnevnik.

### Nivo 0 – Emergency

Zapisi t.i. "nultege" nivoja so napake, ki onemogočajo nadaljnje delovanje strežnika IMiS®/ARChive Server. Pomenijo težko napako ob verjetno okrnjeni celovitosti podatkov strežnika, zato se slednji ob nastanku takšne napake sam takoj zaustavi in nadaljevanje ni mogoče brez posega administratorja strežnika.

Vzroki za te napake so navadno zunanje narave npr. odpoved ključnih delov strojne opreme strežnika.

### Nivo 1 – Alert

Zapisi prvega nivoja so napake pri katerih ni nujno, da strežnik IMiS®/ARChive Server preneha delovati. Delovati preneha, če bi ob nadaljevanju lahko prišlo do okvare na interni bazi strežnika ali objektih.

Vzrok za tako napako je lahko odpoved strojne opreme, zaznano nepravilno delovanje funkcij operacijskega sistema, preobremenitev strežnika ali poseganje drugega programa v okolje strežnika IMiS®/ARChive Server ali nepravilen poizkus konfiguriranja profilov in volumnov.

### Nivo 2 – Critical

Zapisi drugega nivoja so napake pri katerih IMiS®/ARChive Server preneha delovati, saj bi lahko ob nadaljevanju prišlo do okvare na interni bazi strežnika ali objektih. Vzrok za tako napako je lahko zaznano nepravilno delovanje funkcij operacijskega sistema, pomanjkanje virov operacijskega sistema, preobremenitev strežnika ali zaznana napaka v delovanju strežnika.

### Nivo 3 – Error

Zapisi tretjega nivoja so napake pri katerih je strežnik IMiS®/ARChive Server zaznal napako pri delovanju, ki pa ni kritična napaka in ne pomeni možnosti okvare podatkov. Vzroki za tako napako so lahko na strani odjemalca, posledica uporabe napačnih ali neprimernih nastavitvenih parametrov strežnika ali posledica napačnih vpisov v bazo.

### Nivo 4 – Warning

Zapisi četrtega nivoja so opozorila pri katerih je strežnik IMiS®/ARChive Server zaznal nepravilnost, ki pa bistveno ne vpliva na delovanje strežnika in so največkrat posledica neregularnih zahtevkov odjemalcev, redkeje posledica napačnih vpisov v bazo strežnika ali nastavitveno datoteko.

### Nivo 5 – Notice

Zapisi petega nivoja so zapisi o pomembnih regularnih (normalnih) dogodkih na strežniku IMiS®/ARChive Server, ki bi utegnile zanimati administratorsko osebje.

### Nivo 6 – Info

Zapisi šestega nivoja so zapisi o manj pomembnih regularnih (normalnih) dogodkih na strežniku IMiS®/ARChive Server, ki bi utegnile zanimati administratorsko osebje.

### Nivo 7 – Debug

Zapisi sedmega nivoja so razširjeni zapisi o vseh dogodkih na strežniku IMiS®/ARChive Server, ki jih uporabljamo pri zbiranju natančnejših podatkov o delovanju strežnika kadar vzroki za napako ali opozorilo niso evidentni.

Administrator strežnika IMiS®/ARChive Server mora biti pozoren na pojavljanje sporočil nivojev 4 do 0, saj ti lahko odkrivajo težave pri delovanju strežnika in delovanju strežnika ter komunikaciji z odjemalci.

## **8.3.1 Postopki konfiguriranja s konzolnimi orodji**

Izvoz interne baze strežnika opravimo z ukazom (izpis je odvisen od konfiguracije strežnika):

```
[user1@iarc ~]# sudo su - iarc -s /bin/bash -c "cd /opt/IS/imisarc && ./dbtool -f /etc/iarc.conf -w /iarc/db/ -a exp"
```

Using 'sl\_SI.UTF-8' locale settings.

Document Root: /iarc/db/

Port: 21553

```
Exporting ACLENTY (33 records) to acleentry.txt ... OK.
Exporting ACLENTYVALIDITY (2 records) to acleentryvalidity.txt ... OK.
Exporting ATTRIBUTE (84 records) to attribute.txt ... OK.
Exporting ATTRIBUTEGROUP (0 records) to attributegroup.txt ... OK.
Exporting ATTRIBUTEVALUE (4569935 records) to attributevalue.txt ... OK.
Exporting ATTRIBUTEVALUEBINARY (1 records) to attributevaluebinary.txt ... OK.
```

Exporting ATTRIBUTEVALUEDATETIME (1232675 records) to attributevaluedt.txt ... OK.  
Exporting ATTRIBUTEVALUEDOUBLE (0 records) to attributevaluedouble.txt ... OK.  
Exporting ATTRIBUTEVALUEFILE (1310789 records) to attributevaluefile.txt ... OK.  
Exporting ATTRIBUTEVALUEINT32 (820991 records) to attributevalueint32.txt ... OK.  
Exporting ATTRIBUTEVALUEINT64 (821009 records) to attributevalueint64.txt ... OK.  
Exporting ATTRIBUTEVALUEINT128 (1 records) to attributevalueint128.txt ... OK.  
Exporting ATTRIBUTEVALUEINT128IDX (1 records) to attributevalueint128idx.txt ... OK.  
Exporting ATTRIBUTEVALUESTRING (242028 records) to attributevaluemaxstring.txt ... OK.  
Exporting ATTRIBUTEVALUESTRING10 (0 records) to attvalstr10.txt ... OK.  
Exporting ATTRIBUTEVALUESTRING20 (1 records) to attvalstr20.txt ... OK.  
Exporting ATTRIBUTEVALUESTRING30 (1 records) to attvalstr30.txt ... OK.  
Exporting ATTRIBUTEVALUESTRING40 (1 records) to attvalstr40.txt ... OK.  
Exporting ATTRIBUTEVALUESTRING50 (619562 records) to attvalstr50.txt ... OK.  
Exporting ATTRIBUTEVALUESTRING100 (39 records) to attvalstr100.txt ... OK.  
Exporting ATTRIBUTEVALUESTRING200 (649035 records) to attvalstr200.txt ... OK.  
Exporting ATTRIBUTEVALUESTRING20IDX (1 records) to attvalstr20idx.txt ... OK.  
Exporting ATTRIBUTEVALUESTRING30IDX (8 records) to attvalstr30idx.txt ... OK.  
Exporting ATTRIBUTEVALUESTRING40IDX (1 records) to attvalstr40idx.txt ... OK.  
Exporting ATTRIBUTEVALUESTRING50IDX (1 records) to attvalstr50idx.txt ... OK.  
Exporting ATTRIBUTEVALUESTRING100IDX (68 records) to attvalstr100idx.txt ... OK.  
Exporting ATTRIBUTEVALUESTRING200IDX (31426 records) to attvalstr200idx.txt ... OK.  
Exporting ATTRIBUTEVALUEUINT32 (2565834 records) to attvaluint32.txt ... OK.  
Exporting ATTRIBUTEVALUEUINT64 (30944 records) to attvaluint64.txt ... OK.  
Exporting ATTRIBUTEVALUEUINT128 (1 records) to attvaluint128.txt ... OK.  
Exporting ATTRIBUTEVALUEUINT128IDX (1 records) to attvaluint128idx.txt ... OK.  
Exporting audit log data (9544057 records) to auditlog.bin ... OK.  
Exporting DIGITALCERTIFICATE (40 records) to digitalcert.txt ... OK.  
Exporting COUNTER (4756 records) to counter.txt ... OK.  
Exporting DIGITALSIGNATURE (476 records) to digitalsig.txt ... OK.  
Exporting DIRECTORYENTRY (89 records) to direntry.txt ... OK.  
  
Exporting DIRECTORYENTRYALIAS (42 records) to direntryalias.txt ... OK.  
Exporting DIRECTORYENTRYGROUP (80 records) to direntrygroup.txt ... OK.  
  
Exporting ENTITY (1245268 records) to entity.txt ... OK.  
Exporting ENTITYCLASS (127 records) to entityclass.txt ... OK.  
Exporting ENTITYDOCUMENT (1237320 records) to entitydocument.txt ... OK.  
Exporting ENTITYFOLDER (7787 records) to entityfolder.txt ... OK.  
Exporting PROFILE (4 records) to profile.txt ... OK.  
Exporting PROPERTY (15 records) to property.txt ... OK.  
Exporting TEMPLATE (33 records) to template.txt ... OK.  
Exporting TEMPLATEATTRIBUTE (142 records) to templateatt.txt ... OK.  
Exporting TEMPLATEBIND (22 records) to templatebind.txt ... OK.  
Exporting ARCHIVALINFORMATIONPACKAGE (589815 records) to aip.txt ... OK.  
Exporting ARCHIVALINFORMATIONPACKAGEQUEUE (0 records) to aipq.txt ... OK.  
Exporting CREATEAIPQUEUE (0 records) to createaipqueue.txt ... OK.  
Exporting AIPJOBTIMESTAMP (0 records) to aipjobts.txt ... OK.  
Exporting REVOCATIONDATA (1034 records) to revodata.txt ... OK.  
Exporting CONTENTPROCESSINGQUEUE (0 records) to cpqueue.txt ... OK.  
Exporting CONTENTPROCESSINGERROR (1 records) to cperror.txt ... OK.

Exporting TIMESTAMP (476 records) to timestamp.txt ... OK.  
Exporting VOLUME (12 records) to volume.txt ... OK.  
Exporting LOOKUPTABLE (12 records) to lookup.txt ... OK.  
Exporting HASH128 (1 records) to hash128.txt ... OK.  
Exporting HASH160 (524494 records) to hash160.txt ... OK.  
Exporting HASH224 (1 records) to hash224.txt ... OK.  
Exporting HASH256 (65322 records) to hash256.txt ... OK.  
Exporting HASH384 (1 records) to hash384.txt ... OK.  
Exporting HASH512 (1 records) to hash512.txt ... OK.  
Exporting REVOCATIONDATATIMESTAMP (657 records) to revodatats.txt ... OK.  
Exporting REVOCATIONDATADIGITALSIGNATURE (0 records) to revodatadsig.txt ... OK.  
Exporting ENTITYRETENTIONDISPOSITIONSCHEDULE (86 records) to rds.txt ... OK.  
Exporting TIMESTAMPARCHIVALINFORMATIONPACKAGE (589814 records) to tsaip.txt ... OK.  
Exporting CERTIFICATEBODY (14302 records) to certbody.txt ... OK.  
Exporting FILEDESCRIPTION (348 records) to filedesc.txt ... OK.  
Exporting ATTRIBUTEVALUENULL (124334 records) to attvalnull.txt ... OK.  
Exporting REVIEWQUEUE (0 records) to reviewqueue.txt ... OK.  
Exporting CONTENTBIND (31 records) to contentbind.txt ... OK.  
Exporting TOKEN4 (0 records) to token4.txt ... OK.  
Exporting TOKEN8 (7 records) to token8.txt ... OK.  
Exporting TOKENMAX (3 records) to tokenmax.txt ... OK.  
Exporting SYSEVENT (0 records) to sysevent.txt ... OK.  
Export command completed with no errors.

*Opomba: Številke (XX records) pri vsaki vrstici se lahko spreminjajo, odvisno od števila zapisov.*



Rezultat so tekstovne datoteke, ki predstavljajo posamezne tabele v bazi, binarna datoteka, ki predstavlja revizijsko sled ter dodatni podatki (shranjeni v datotekah brez končnic, datoteke se začnejo s črko, kateri sledi zaporedna številka – primer: »p0« za blob iz PROPERTY tabele), ki vsebujejo del interne baze strežnika IMiS®/ARChive Server.

## 8.4 Administracija

Administracijska opravila lahko bistveno vplivajo na delovanje strežnika IMiS®/ARChive Server. Pravilna namestitev in konfiguracija sistema lahko zagotovi stabilno in pričakovano delovanje strežnika z malo ali nič vzdrževalnimi posegi. V primeru napačne ali neskladne konfiguracije pa strežnik lahko kompromitira in postane nestabilen, počasi delujoč ali varnostno ranljiv. Zato morajo biti posegi v administracijo strežnika omejeni na izkušene administratorje, ki so v podrobnosti seznanjeni z navodili izdelovalca programske opreme in splošnimi dobrimi praksami pri načrtovanju in vzdrževanju informacijskih sistemov.

Ob nakupu svetujemo vzpostavitev vzdrževalne pogodbe z izdelovalcem programske opreme, ki zagotavlja brezhibno in neprekinjeno delovanje ključnega sistema (angl. mission-critical), kar naj bi arhivski sistem predstavljal.

Administrator strežnika IMiS®/ARChive Server nastavlja parametre v nastavitveni datoteki glede na porabo virov strežnika, ki jih spremlja s periodičnim pregledovanjem stanja strežnika, zapisov v dnevnikih in zahtev aplikacijskega okolja.

Administrator po navodilih izdelovalca programske opreme upravlja z nastavitvenimi parametri strežnika, ki vplivajo na načrt razvrščanja gradiva, predloge entitet, metapodatkovne sheme atributov, nastavitve vtičnikov za različne podporne storitve sistema, itd. Ti posegi se izvajajo s pomočjo spletnega administracijskega vmesnika ali v okviru spletnega odjemalca IMiS®/wClient.

Administratorjem uporabnikov nudimo izobraževanja za upravljanje s strežnikom, strankam pa svetujemo sklenitev vzdrževalne pogodbe. Profesionalne storitve upravljanja s strežnikom, ki jih izvajamo, zagotavljajo nemoteno delovanje strežnika skozi daljše obdobje.

Pred vsakim posegom je smiselno poskrbeti za varnostno kopijo interne baze strežnika in nastavitvene datoteke v primeru potrebe po restavraciji starih nastavitvev zaradi nepravilne prilagoditve nastavitvev in/ali baze.

### 8.4.1 Konfiguracijska datoteka iarc.conf

Nastavitveni parametri strežnika IMiS®/ARChive Server so nastavljivi v datoteki `/etc/iarc.conf`.

Za spodnje opise so uporabljene privzete vrednosti.

Parametri so razvrščeni v sekcije po namembnosti in jih podrobneje obravnavamo v nadaljevanju, kjer so razdeljene po principu:

Ključ:	Opis (opsijsko nabor veljavnih, minimalnih, maksimalnih, priporočenih vrednosti)
--------	--

#### **Sekcija [Server]**

Path:	Označuje absolutno pot do izvajalnih datotek (programov) in knjižnic strežnika. Privzeta vrednost je <code>/opt/IS/imisarc</code>
ReqThreads:	Označuje število niti, ki izvajajo zahteve. Privzeta vrednost je <code>7</code> in navzgor ni omejena. Priporočena vrednost znaša dvakratnik števila niti, ki jih je strežnikov procesor zmožen izvajati hkrati in je odvisen od števila procesorskih jeder.
ClientTimeout:	Označuje čas neaktivnosti prijavljenega odjemalca v sekundah, ki mora preteči preden strežnik prekine sejo. Privzeta vrednost je <code>3600</code> sekund. Najmanjša možna vrednost je <code>1</code> in največja <code>2147483647</code> .
SocketTimeout	Označuje čas neaktivnosti vtičnice, ki mora preteči, preden strežnik vtičnico zapre. Privzeta vrednost je <code>3600</code> sekund. Najmanjša možna vrednost je <code>1</code> in največja <code>2147483647</code> .
NoAuthClientTimeout:	Označuje čas neaktivnosti neprijavljenega (anonimnega) odjemalca v sekundah, ki mora preteči preden strežnik prekine sejo. Privzeta vrednost je <code>10</code> sekund. Najmanjša možna vrednost je <code>1</code> in največja <code>2147483647</code> . Skozi anonimne seje je možno s strežnikom izmenjati le najosnovnejše in neobčutljive informacije (naziv arhiva, opis, ipd.).
IdentPassword:	Označuje šifrirano zgoščeno vrednost gesla, ki ga strežnik uporablja pri delovanju v procesih šifriranja. V kolikor trajno hranimo notranje identifikatorje za entitete v drugih sistemih, vrednosti ne smemo spreminjati po arhiviranju prve entitete, saj vrednost vpliva na šifrirni algoritem za generiranje notranjih identifikatorjev entitet.
Port:	Označuje številko TCP vrat, na katerih povezovalni proces strežnika pričakuje zahteve odjemalcev. Privzeta vrednost je <code>16807</code> .

Listen:	<p>Označuje omrežni naslov na katerega strežnik veže TCP vrata na katerih pričakuje zahteveke odjemalcev. Vrednosti so lahko le v skladu IPv4 ali IPv6 naslovno shemo.</p> <p>Primeri veljavnih vrednosti:</p> <p>192.168.92.32</p> <p>fd00:192:168:92::32</p> <p>192.168.92.32:16807</p> <p>[fd00:192:168:92::32]:16807</p> <p>[fd00:192:168:92:2340:efa1:1244:32]</p> <p>fd00:192:168:92:2340:efa1:1244:32</p> <p>[fd00:192:168:92:2340:efa1:1244:32]:12345</p> <p>::ffff:192.168.92.12]</p> <p>::ffff:192.168.92.12</p> <p>::ffff:192.168.92.12]:65743</p> <p>localhost</p> <p>[::]</p>
CXLib:	<p>Označuje relativno pot do knjižnic, ki vsebujejo kompresijske metode za različne platforme odjemalcev, znotraj poti, ki jo označuje vrednost parametra <code>DataPath</code> opisanega spodaj.</p>
PartialTimeout:	<p>Označuje čas v sekundah, v katerem se mora odjemalec odzvati na zahtevek strežnika. Po preteku tega časa strežnik zaključi sejo. Najmanjša vrednost je 1, največja je 2147483647 in priporočena 5.</p>
PidPath:	<p>Označuje pot do identifikacijske datoteke glavnega procesa strežnika. Privzeta vrednost je <code>/var/run/iarc</code>.</p>

CountryLanguage:	<p>Označuje regionalne nastavitve v POSIX formatu: <code>xx_YY[.CHARSET[@variant]]</code>; prvi dve črki <code>xx</code> predstavljata kodo jezika po standardu ISO-639, drugi dve črki predstavljata kodo države po standardu ISO-3166, <code>CHARSET</code> podatek (opcijski) določa kodno tabelo oziroma kodni razpored (seznam dostopen v imeniku <code>/usr/share/i18n/charsets</code>), podatek <code>variant</code> (opcijski) pa določa nacionalne posebnosti jezika. Seznam možnih nastavitvev je možno pridobiti preko izpisa ukaza <code>"locale -a"</code>. Vrednost določa nabor pravil s katerimi naj strežnik izvaja vse operacije z znakovnimi nizi, ki so lahko "občutljivi" na različne nacionalne znake (sortiranje, prevajanje, zlaganje, itd).</p> <p>Privzeta vrednost je <code>"</code>, kar efektivno določa sistemsko nastavljena pravila (glej sistemski ukaz <code>"locale"</code></p> <p><i>Posebnost: Zaradi zagotavljanja prenosljivosti shranjenih podatkov v notranji bazi storitev, ne glede na določene regionalne nastavitve, interno uporablja UTF-8 kot notranjo kodno tabelo. Ostale regionalne nastavitve ohrani (jezik, država, jezikovna posebnost).</i></p>
DataPath:	<p>Označuje področje na disku, kjer strežnik hrani trajne podatke, povezane z arhivom kot so statistični podatki transakcij, ipd.</p> <p>Privzeta vrednost je <code>/iarc/db</code>.</p>
MaxRequestSize:	<p>Določa največji možen enkratni zahtevek odjemalca.</p> <p>Privzeta vrednost je <code>3276800</code> bajtov. Najmanjša možna vrednost je <code>32768</code> in največja <code>32768000</code>.</p>
JVMHome:	<p>Označuje absolutno pot do javanskega okolja. Privzeta vrednost je <code>/opt/IS/imisarc/jvm</code>.</p>
JVMOptions:	<p>Označuje konfiguracijske parametre za javansko okolje.</p>
Mode:	<p>Določa način, kako lahko odjemalec komunicira s strežnikom. Vrednosti so naslednje: <code>0</code> – komunikacija poteka po nezaščitenem kanalu, <code>1</code> - strežnik omogoča komunikacijo tako po nezaščitenem kakor tudi po zaščitenem kanalu, <code>2</code> – komunikacija poteka samo po zaščitenem kanalu. Privzeta vrednost je <code>0</code>.</p>
SecureListen:	<p>Označuje omrežni naslov na katerega strežnik veže TCP vrata, na katerih pričakuje zahteve odjemalcev (zaščiten komunikacijski kanal). Za podrobnosti glej opis pod ključem <code>Listen</code>.</p>
SecurePort:	<p>Označuje številko TCP vrat, na katerih povezovalni proces strežnika pričakuje zahteve odjemalcev (zaščiten komunikacijski kanal).</p>

SecureCertKeyFile:	Označuje absolutno pot do ključa digitalnega potrdila, ki se uporablja v procesu vzpostavitve zaščitene komunikacijskega kanala. Privzeta vrednost je /opt/IS/imisarc/cert.key.
SecureCertFile:	Označuje absolutno pot do digitalnega potrdila, ki se uporablja v procesu vzpostavitve zaščitene komunikacijskega kanala. Privzeta vrednost je /opt/IS/imisarc/cert.crt.
SecureCertChainFile:	Označuje absolutno pot do datoteke, ki vsebuje zaupanja vredno verigo digitalnih potrdil, ki se preverjajo v procesu vzpostavitve zaščitene komunikacijskega kanala.
SecureProtocol:	Označuje kriptografski protokol, ki se uporablja za zaščito komunikacijskega kanala. Privzeta vrednost je TLSv1.
SecureCiphers:	Označuje omogočene kriptografske algoritme za šifriranje podatkov.
SecureVerifyClientMode:	Določa način preverjanja odjemalčevega digitalnega potrdila v procesu vzpostavitve zaščitene komunikacijskega kanala. Vrednosti so naslednje: 0 – odjemalčevo digitalno potrdilo ni potrebno, 1 – odjemalčevo digitalno potrdilo je opcijsko (če ga odjemalec posreduje ga strežnik preveri), 2 – odjemalec mora posredovati digitalno potrdilo ki se nato na strežniku preveri.
SecureHandshakeTimeout:	Označuje čas (v sekundah), v katerem morata odjemalec in strežnik vzpostaviti zaščiten komunikacijski kanal. Privzeta vrednost je 60 sekund, najmanjša vrednost je 5 sekund, največja pa 3600.
SecureRevocationCheck:	Določa način preverjanja odjemalčevega digitalnega potrdila v povezavi s preklicnimi listami izdajateljev digitalnih potrdil. Vrednosti so naslednje: 0 – (OFF) preklic odjemalčevega digitalnega potrdila se ne preverja, 1 – (OPTIONAL) preklic odjemalčevega digitalnega potrdila se preveri. V primeru kakršnekoli napake pri tem postopku, strežnik povezavo vseeno dovoli, 2 – (REQUIRED-CACHED) stanje preklic odjemalčevega digitalnega potrdila se obvezno preveri. Strežnik lahko uporabi predhodno pridobljeno informacijo, v kolikor je še veljavna, 3 – (REQUIRED-FRESH) stanje preklic odjemalčevega digitalnega potrdila se obvezno preveri. Strežnik vselej uporabi sveže informacije o preklic.

### **Sekcija [Database]**

ProviderBootstrapFile:	Označuje relativno pot do nastavitvene datoteke vtičnika za servis podatkovne baze. Relativna je glede na vrednost parametra [Server].Path.
------------------------	---

**Sekcija [Cache]**

ReadPath:	Označuje pot do imenika, ki predstavlja medpomnilnik, kjer strežnik IMiS®/ARChive Server odlaga objekte, ko jih je potrebno tja začasno odložiti zaradi hitrejšega posredovanja objektov odjemalcem. Pravice na poti morajo biti urejene tako, da lahko uporabnik, ki izvaja procese strežnika, tam bere in zapisuje datoteke.
ReadSize:	Označuje najmanjšo velikost medpomnilnika. Strežnik to omejitev prilagaja dinamično, glede na potrebe. Spreminjanje vrednosti ni smiselno.
EditPath:	Označuje pot do imenika, ki predstavlja medpomnilnik, kjer strežnik začasno odlaga objekte, ki mu jih posredujejo odjemalci. Pravice na poti morajo biti urejene tako, da lahko uporabnik, ki izvaja procese strežnika, tam lahko bere in zapisuje datoteke.
EditSize:	Označuje najmanjšo velikost medpomnilnika. Strežnik to omejitev prilagaja dinamično, glede na potrebe. Spreminjanje vrednosti ni smiselno.

**Sekcija [Log]**

LogFile:	Označuje osnovno ime dnevniške datoteke, skupaj s potjo, v katero strežnik IMiS®/ARChive Server beleži dogodke. Pravice na poti in datoteki morajo biti urejene tako, da lahko uporabnik, ki izvaja procese strežnika, v njo zapisuje datoteke in po potrebi ustvarja nove datoteke.
MaxSize:	Označuje največjo velikost ene dnevniške datoteke v bajtih. Privzeta in priporočena vrednost je 1000000, najmanjša 65536 in največja 2147483648.
BackupCount:	Označuje število arhivskih dnevniških datotek, znotraj katerega strežnik zapisuje dogodke po algoritmu prvi notri – zadnji ven. Privzeta vrednost je 1, priporočena 9.
LogLevel:	Nivo dogodkov, ki jih strežnik zapisuje v dnevniško datoteko. Za več informacij glej poglavje <a href="#">Beleženje dogodkov delovanja</a> . Najmanjša vrednost je 1, največja 7, priporočena 6.

**Sekcija [AuditLog]**

AuthCryptoModes:	Označuje nabor možnih kriptografskih metod, ki jih strežnik dovoli uporabiti za šifriranje avtentikacijskih sporočil in kasnejše komunikacije z odjemalcem, ki želi izvesti vpogled v revizijsko sled. Identifikator predstavlja kombinacijo algoritma, dolžine ključa in kriptografski način obdelave paketa podatkov. Veljavne vrednosti so: aes-256-cbc aes-256-ecb aes-256-ofb aes-256-cfb aes-192-cbc aes-192-ecb aes-192-ofb aes-192-cfb aes-128-cbc aes-128-ecb aes-128-ofb aes-128-cfb
AuthPreSharedKey:	Predpomnjeni strežniški ključ, ki se uporabi za šifriranje avtentikacijskih sporočil in kasnejše komunikacije z odjemalcem, ki predstavlja pooblaščen osebo za namen vpogleda v revizijsko sled beleženja dogodkov povezanih s sejami in/ali objekti.

**Sekcija [Authentication]**

Methods:	<p>Označuje možen nabor metod za vzpostavitev seje odjemalca IMiS® s strežnikom IMiS®/ARChive Server. Veljaven nabor vrednosti je:</p> <ul style="list-style-type: none"> <li>- basic</li> <li>- advanced</li> <li>- psk</li> <li>- srp6a</li> </ul> <p>Osnovna (basic) predstavlja starejšo metodo vzpostavitve seje s strežnikom, brez posredovanja evidenčnih podatkov o odjemalcu.</p> <p>Pri napredni (advanced) je vključena zapletenejša (HMAC) metoda vzpostavitve seje s strežnikom, ki predvideva obvezne in neobvezne metapodatke o odjemalcu.</p> <p>Pri uporabi deljenega ključa (psk) napredno metodo dodatno zaščitimo s šifrirano izmenjavo omrežnih avtentikacijskih paketov.</p> <p>Uporaba prijavnih podatkov uporabnika »User Credentials« (srp6a) pa omogoča individualno prijavo uporabnikov, kjer se podatki o uporabniku pridobijo na podlagi uspešne avtentikacije uporabnika iz internih virov (imenika).</p>
CryptoModes:	<p>Označuje nabor možnih metod šifriranja, ki jih strežnik uporabi za šifrirano komunikacijo z odjemalcem. Identifikator predstavlja kombinacijo algoritma, dolžine ključa in kriptografski način obdelave paketa podatkov. Veljavne vrednosti so:</p> <ul style="list-style-type: none"> <li>aes-256-cbc</li> <li>aes-256-ecb</li> <li>aes-256-ofb</li> <li>aes-256-cfb</li> <li>aes-192-cbc</li> <li>aes-192-ecb</li> <li>aes-192-ofb</li> <li>aes-192-cfb</li> <li>aes-128-cbc</li> <li>aes-128-ecb</li> <li>aes-128-ofb</li> <li>aes-128-cfb</li> </ul>
PreSharedKey:	<p>Predpomnjeni strežniški ključ, ki se uporabi za šifriranje avtentikacijskih sporočil (prijavna metoda psk) in kasnejše komunikacije z odjemalcem, ki predstavlja navadnega IMiS® odjemalca.</p>



RequiredParams:	<p>Nabor zahtevanih podatkov, ki jih mora posredovati odjemalec pri odpiranju seje ali dogodka. V kolikor manjka en sam zahtevan podatek, strežnik zavrne vzpostavitev seje ali dogodka.</p> <p>Veljaven nabor zahtevanih podatkov lahko vsebuje vsaj enega izmed:</p> <ul style="list-style-type: none"> <li>- username (ime uporabnika, ki izvaja operacijo)</li> <li>- computername (ime računalnika, iz katerega operacija izvira)</li> <li>- message (razlog/sporočilo, ki ga uporabnik vpiše pri izvedbi operacije)</li> </ul> <p>Privzeta nastavitvev je prazno – ne vsebuje nobenega iz nabora.</p>
-----------------	---

### **Sekcija [Admin]**


Enabled:	<p>Označuje vrednost, ki pove ali je administracijskih modul omogočen ali ne. Vrednosti so naslednje: 0 – administracijski modul ni omogočen, 1 – administracijski modul je omogočen. Privzeta vrednost je 0.</p>
IdleTimeout:	<p>Označuje čas v sekundah, po katerem se administracijska seja zaradi nedejavnosti prekine. Privzeta vrednost je 900 sekund.</p>
WebPath:	<p>Označuje relativno pot, ki predstavlja spletni naslov administracijskega vmesnika. Privzeta vrednost je /admin.</p>
Port:	<p>Označuje številko TCP vrat, na katerih povezovalni proces strežnika pričakuje zahteve odjemalcev za administracijo.</p>
Listen:	<p>Označuje omrežni naslov na katerega strežnik veže TCP vrata na katerih pričakuje zahteve odjemalcev za administracijo.</p> <p>Za podrobnosti glej opis v sekciji Server pod ključem Listen.</p>
MaxSessionsPerUser:	<p>Označuje največje število vzporednih administracijskih sej za posameznega uporabnika. Privzeta vrednost je 5 administracijskih sej.</p>
MaxRequestSize:	<p>Določa največji možen enkratni zahtevek odjemalca. Privzeta vrednost je 1048576 bajtov. Najmanjša možna vrednost je 10240 in največja 10485760.</p>
Secure:	<p>Označuje vrednost, ki pove ali komunikacije med odjemalcem in strežnikom poteka po zaščitenem kanalu ali ne. Vrednosti so:</p> <p>0 – komunikacija med odjemalcem in strežnikom poteka po nezaščitenem kanalu, 1 – komunikacija med odjemalcem in strežnikom poteka po zaščitenem kanalu. Privzeta vrednost je 0.</p>
SecureCertKeyFile:	<p>Označuje absolutno pot do ključa digitalnega potrdila, ki se uporablja v procesu vzpostavitve zaščitenega komunikacijskega kanala. Privzeta vrednost je /opt/IS/imisarc/cert.key.</p>

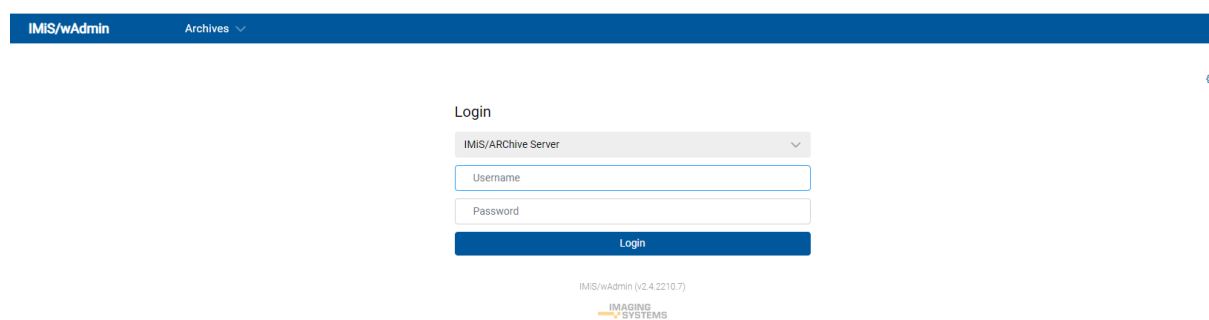
SecureCertKeyPassword:	Označuje geslo za dostop do ključa digitalnega potrdila.
SecureCertFile:	Označuje absolutno pot do digitalnega potrdila, ki se uporablja v procesu vzpostavitve zaščitenega komunikacijskega kanala. Privzeta vrednost je /opt/IS/imisarc/cert.crt.
SecureCertChainFile:	Označuje absolutno pot do datoteke, ki vsebuje zaupanja vredno verigo digitalnih potrdil. Preverjajo se v procesu vzpostavitve zaščitenega komunikacijskega kanala.
SecureProtocol:	Označuje kriptografski protokol, ki se uporablja za zaščito komunikacijskega kanala. Privzeta vrednost je TLSv1.
SecureCiphers:	Označuje omogočene kriptografske algoritme za šifriranje podatkov.
SecureVerifyClientMode:	Določa način preverjanja odjemalčevega digitalnega potrdila v procesu vzpostavitve zaščitenega komunikacijskega kanala. Vrednosti so naslednje: 0 – odjemalčevo digitalno potrdilo ni potrebno, 1 – odjemalčevo digitalno potrdilo je opcijsko (če ga odjemalec posreduje ga strežnik preveri), 2 – odjemalec mora posredovati digitalno potrdilo ki se nato na strežniku preveri.
SecureHandshakeTimeout:	Označuje čas (v sekundah), v katerem morata odjemalec in strežnik vzpostaviti zaščiten komunikacijski kanal. Privzeta vrednost je 60 sekund, najmanjša vrednost je 5 sekund, največja pa 3600.
SecureRevocationCheck:	Določa način preverjanja odjemalčevega digitalnega potrdila v povezavi s preklicnimi listami izdajateljev digitalnih potrdil. Vrednosti so naslednje: 0 – (OFF) preklic odjemalčevega digitalnega potrdila se ne preverja, 1 – (OPTIONAL) preklic odjemalčevega digitalnega potrdila se preveri. V primeru kakršnekoli napake pri tem postopku, strežnik povezavo vseeno dovoli, 2 – (REQUIRED-CACHED) stanje preklic odjemalčevega digitalnega potrdila se obvezno preveri. Strežnik lahko uporabi predhodno pridobljeno informacijo, v kolikor je še veljavna, 3 – (REQUIRED-FRESH) stanje preklic odjemalčevega digitalnega potrdila se obvezno preveri. Strežnik vselej uporabi sveže informacije o preklic.

## 8.5 Administracijski vmesnik

S spletnim administracijskim vmesnikom IMiS®/wAdmin lahko upravlja administrator ali uporabnik z ustreznimi dostopnimi pravicami (prijavljeni uporabnik). Seznanjen mora biti z delovanjem aplikacije in strežnika IMiS®/ARChive Server.

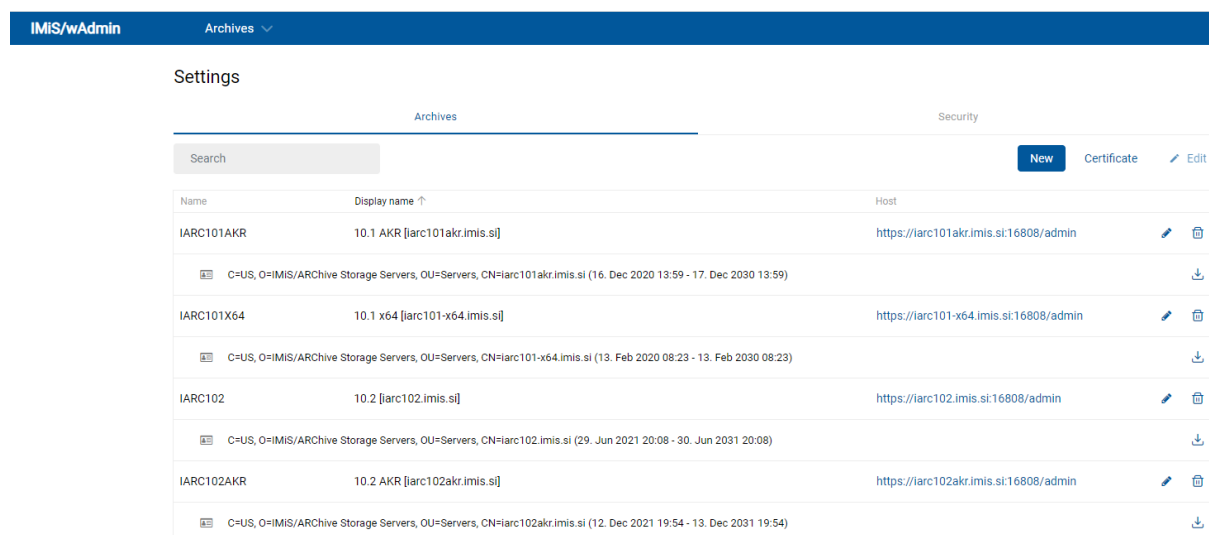
### 8.5.1 Urejanje nastavitev strežnika

Po vpisu ustreznega URL naslova v naslovno vrstico brskalnika se uporabniku prikaže pogovorno okno za prijavo. Z izbiro ikone  v desnem zgornjem kotu je omogočeno urejanje nastavitev arhivskega strežnika.




Slika 36: Prikaz ikone za nastavitve strežnika

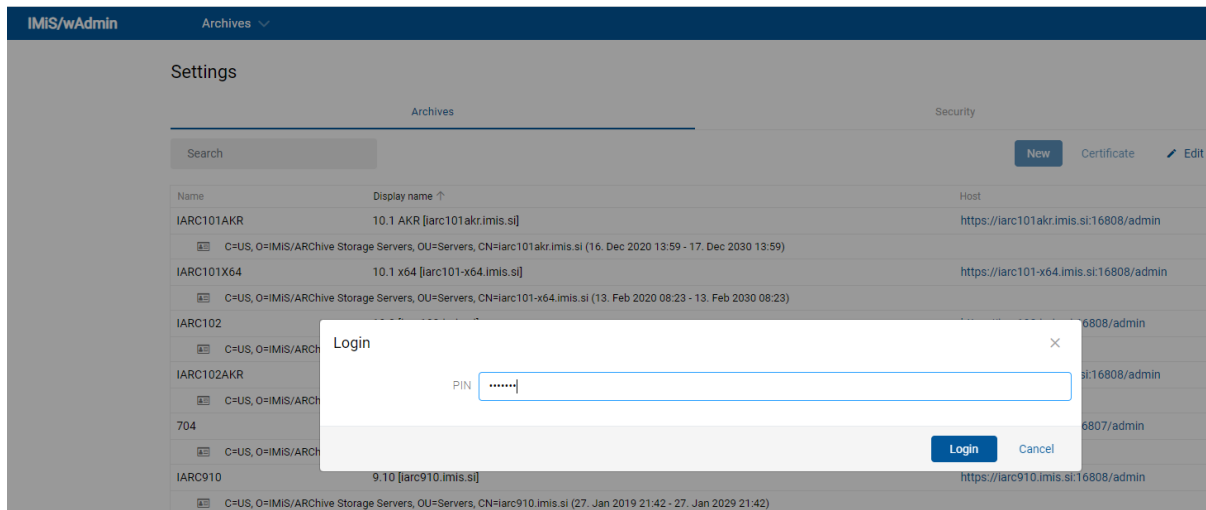
V prikazanem seznamu se nahajajo podatki o arhivskih strežnikih, v kolikor so bili predhodno dodani.



Slika 37: Seznam arhivskih strežnikov v nastavitvah



Prijavljenemu uporabniku je omogočeno iskanje in urejanje arhivskih strežnikov po »Nazivu« (angl. Name) in »Prikazanem imenu« (angl. Display name) v naraščajočem oz. padajočem vrstnem redu.

Za urejanje nastavitev arhivskega strežnika prijavljeni uporabnik najprej izbere »Uredi« (angl. Edit ali ikono ). Dostop do nastavitev je zaščiten z geslom (PIN).



Slika 38: Zaščita nastavitev arhivskega strežnika z geslom

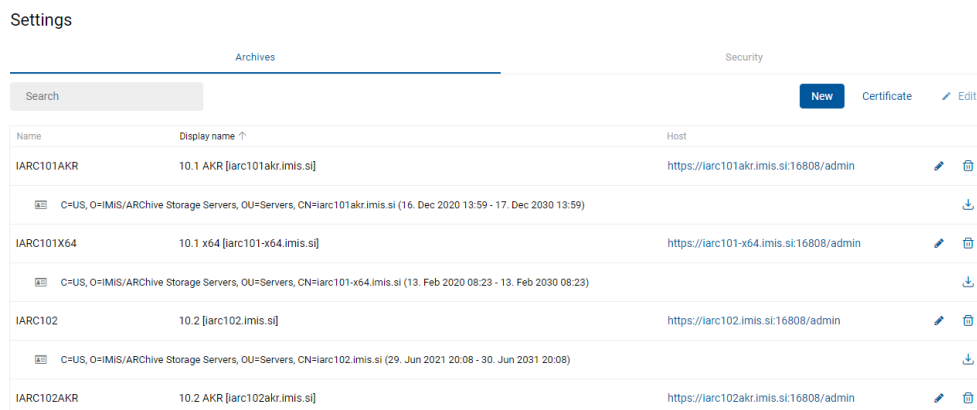
Po vpisu gesla (PIN) je prijavljenemu uporabniku omogočeno izvajanje naslednjih dejanj:

- Dodajanje in odstranjevanje arhivskega strežnika (ikoni  in ).
- Dodajanje in odstranjevanje digitalnih potrdil (angl. Certificate).

*Opomba:* geslo (PIN) za dostop je določeno v datoteki **web.xml** kot ključ **com.imis.archive.admin.service.settings.password** tipa string.





### 8.5.1.1 Dodajanje strežnika

Dodajanje arhivskega strežnika je omogočeno z izbiro dejanja »Nov« (angl. New) v ukazni vrstici v zavihku »Arhivi« (angl. Archives).



Slika 39: Izбира dejanja »Nov« v ukazni vrstici

V pogovornem oknu prijavljeni uporabnik določi naslednje podatke o arhivskem strežniku:

- »Naziv« (angl. Name): ime strežnika.
- »Prikazan naziv« (angl. Display name): prikazano ime strežnika.
- »Strežnik« (angl. Host): pot do strežnika.
- »Dodaj digitalno potrdilo« (angl. Add certificate): dodajanje digitalnega potrdila (ikona ). Iz nabora razpoložljivih datotek (.cer) z digitalnimi potrdili prijavljeni uporabnik izbere ustreznega. Potrdilo odstrani tako, da izbere ikono .
- »Dodaj prstni odtis« (angl. Add fingerprint): dodajanje prstnega odtisa (ikona ). Uporabnik v polje vpiše vrednost prstnega odtisa. Prstni odtis odstrani tako, da izbere ikono .

Slika 40: Dodajanje arhivskega strežnika

**Opomba:** Pri dodajanju arhiva v nastavitvah so za vrednost »Name« dovoljeni samo veljavni URL znaki.

Primer neveljavnih znakov: » / », «, » ; «, » = «, » . «, ...,

Po shranitvi ima prijavljeni uporabnik vpogled v nastavitve strežnika v seznamu.

## Settings

Archives		Security	
10	X	New	Certificate Edit
Name	Display name ↓	Host	
IARC103	IMIS/ARChive Server	https://iarc103.imis.si:16808/admin	
	C=US, O=IMIS/ARChive Storage Servers, OU=Servers, CN=iarc103.imis.si (10. Aug 2022 08:52 - 10. Aug 2032 08:52)		
IARC910R2X64	9.10 R2 x64 [iarc910-r2-x64.imis.si]	https://iarc910-r2-x64.imis.si:16808/admin	
	C=US, O=IMIS/ARChive Storage Servers, OU=Servers, CN=iarc910-r2-x64.imis.si (22. Dec 2019 14:38 - 22. Dec 2029 14:38)		

Slika 41: Prikaz seznama po shranitvi arhivskega strežnika

### 8.5.1.2 Urejanje strežnika

Prijavljeni uporabnik lahko ureja nastavitve arhivskega strežnika tako, da v seznamu izbere ustrezen arhivski strežnik in v ukazni vrstici dejanje »Uredi« (angl. Edit), oziroma ikono .

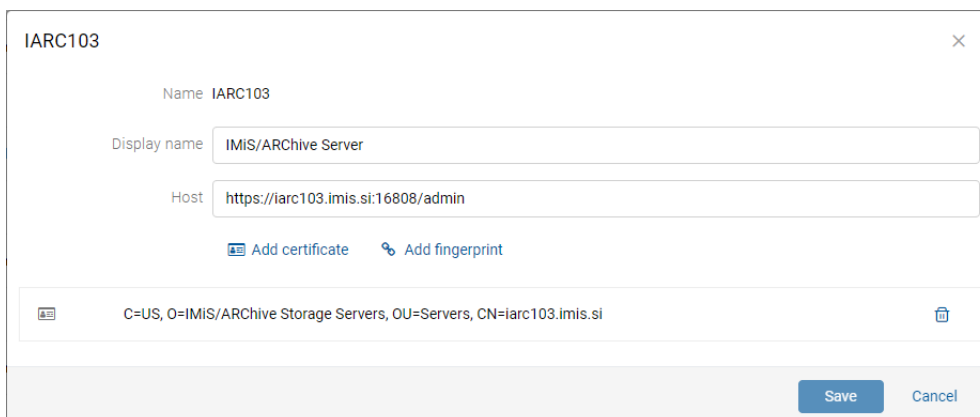
## Settings

Archives		Security	
103	X	New	Certificate Edit
Name	Display name ↓	Host	
IARC103	IMIS/ARChive Server	https://iarc103.imis.si:16808/admin	
	C=US, O=IMIS/ARChive Storage Servers, OU=Servers, CN=iarc103.imis.si (10. Aug 2022 08:52 - 10. Aug 2032 08:52)		

IMIS/wAdmin (v2.4.2210.7)

Slika 42: Izbira arhivskega strežnika v načinu za urejanje

Prikaže se pogovorno okno za urejanje nastavitev arhivskega strežnika.



Slika 43: Pogovorno okno za urejanje nastavitev arhivskega strežnika

Po shranitvi ima prijavljeni uporabnik vpogled v nastavitve strežnika v seznamu.

#### 8.5.1.2.1 Dodajanje in odstranitev digitalnega potrdila za izbrani strežnik


Prijavljeni uporabnik lahko doda digitalno potrdilo za posamezen arhivski strežnik tako, da izbere dejanje »Dodaj digitalno potrdilo« (angl. Add certificate). Odpre se pogovorno okno za izbiro digitalnega potrdila. Po potrditvi izbire se digitalno potrdilo doda v seznam potrdil.

Digitalno potrdilo odstrani z izbiro ikone .

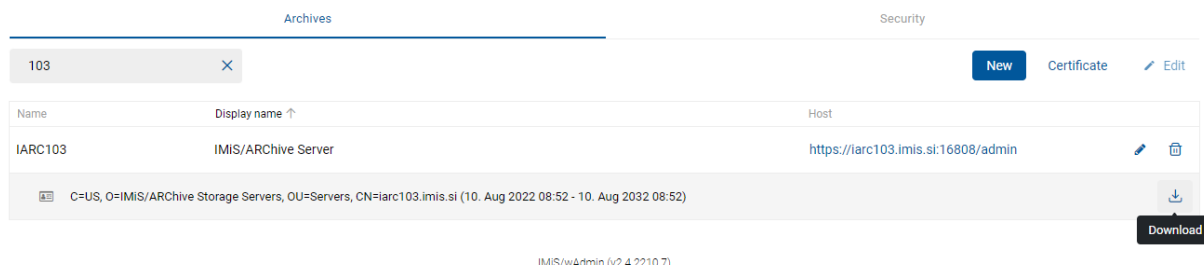


Slika 44: Dodajanje digitalnega potrdila za izbrani arhivski strežnik

### 8.5.1.2.2 Prenos digitalnega potrdila iz izbranega strežnika


Prijavljeni uporabnik lahko prenese (angl. Download) digitalno potrdilo vezano iz izbranega arhivskega strežnika tako, da v seznamu izbere ustrezen arhivski strežnik in ikono .

Settings

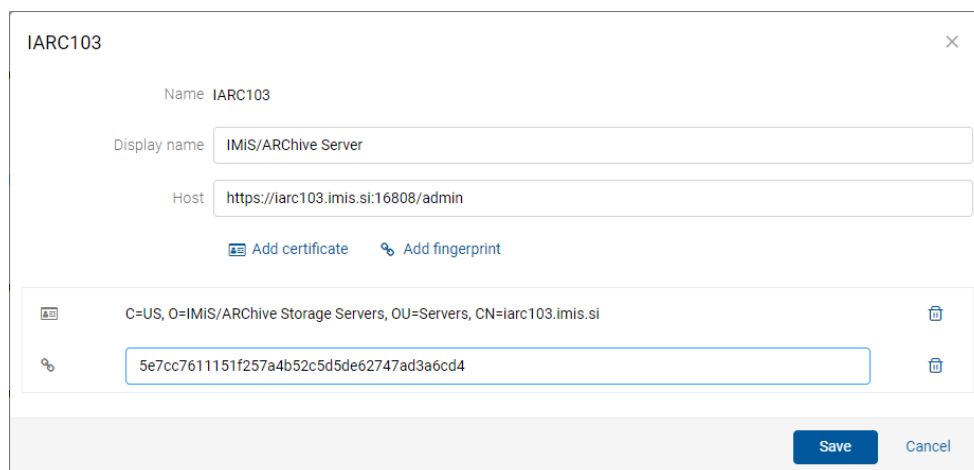


Slika 45: Prenos digitalnega potrdila iz izbranega arhivskega strežnika

### 8.5.1.2.3 Dodajanje in odstranitev prstnega odtisa

Prijavljeni uporabnik doda prstni odtis z izbiro dejanja »Dodaj prstni odtis« (angl. Add fingerprint) poleg ikone . V polje vpiše vrednost ali odloži predhodno zajeti prstni odtis v odložišče.

Prstni odtis odstrani tako, da izbere ikono .

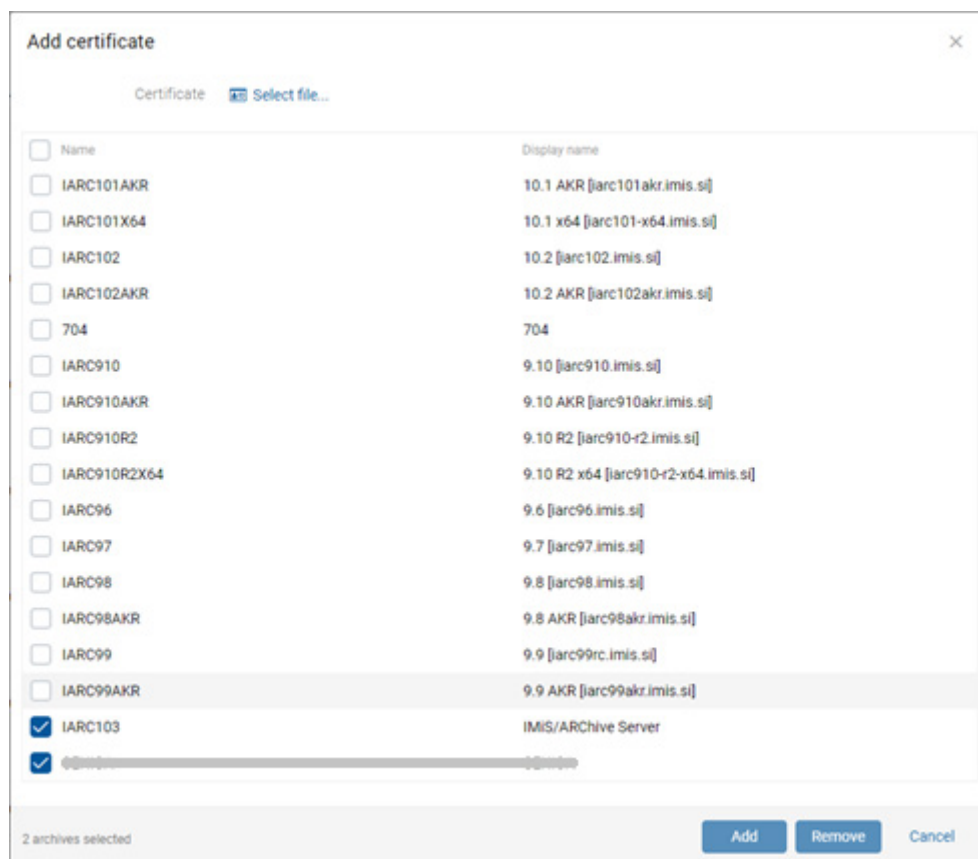


Slika 46: Dodajanje prstnega odtisa za izbrani arhivski strežnik



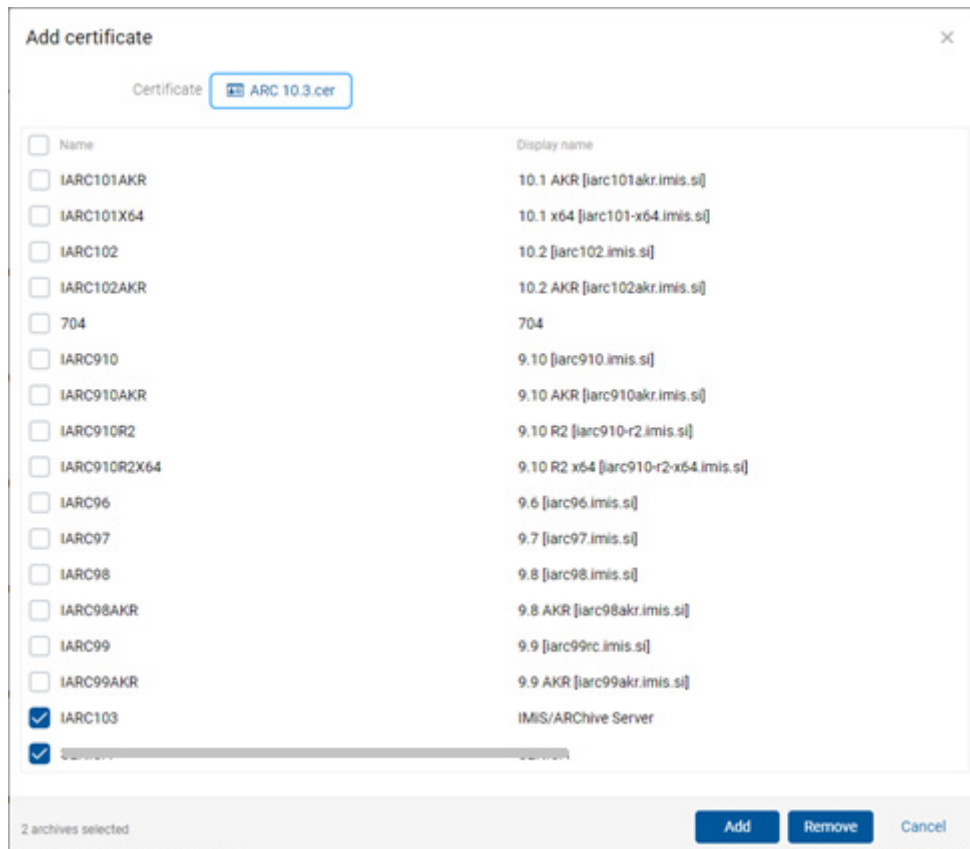
#### 8.5.1.2.4 Dodajanje in odstranitev digitalnega potrdila za izbrane strežnike

Prijavljeni uporabnik lahko doda ali odstrani digitalno potrdilo za več arhivskih strežnikov hkrati z izbiro dejanja »Digitalno potrdilo« (angl. Certificate). Odpre se pogovorno okno, v katerem označi arhivske strežnike in izbere dejanje »Izberi digitalno potrdilo« (angl. Select file).




Slika 47: Izbira digitalnega potrdila za izbrane arhivske strežnike

Po potrditvi izbire datoteke se digitalno potrdilo doda v seznam. Z izbiro dejanja »Dodaj« (angl. Add) se digitalno potrdilo doda k izbranim arhivskim strežnikom. Z izbiro dejanja »Odstrani« (angl. Remove) se digitalno potrdilo odstrani pri izbranih arhivskih strežnikih.

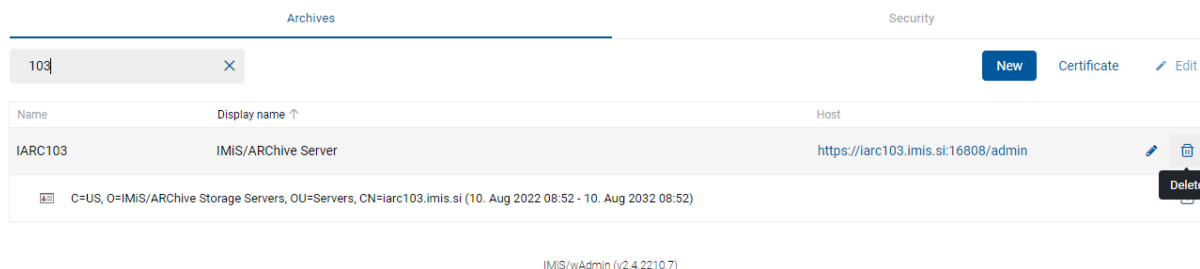


Slika 48: Dodajanje in odstranitev digitalnega potrdila za izbrane arhivske strežnike

### 8.5.1.3 Odstranitev strežnika

Prijavljeni uporabnik lahko odstrani (angl. Delete) nastavitve arhivskega strežnika tako, da v seznamu izbere ustrezen arhivski strežnik in ikono .

Settings



Slika 49: Odstranitev arhivskega strežnika

### 8.5.1.4 Urejanje seznama IP naslovov

Prijavljeni uporabnik lahko ureja seznam dovoljenih in nedovoljenih IP naslovov za dostop do arhivskega strežnika. V zavihku »Varnost« (angl. Security) izbere dejanje »Nov« (angl. New).

Odpre se pogovorno okno za:

- vpis IP naslova;
- določitev ali je naslov dovoljen (angl. Allow) ali nedovoljen (angl. Deny);
- označitev izraza za preverjanje (angl. Regular expression);
- izbiro arhivskih strežnikov, na katere se nastavitve nanaša.

IP address filter



Value: 192.168.100.102

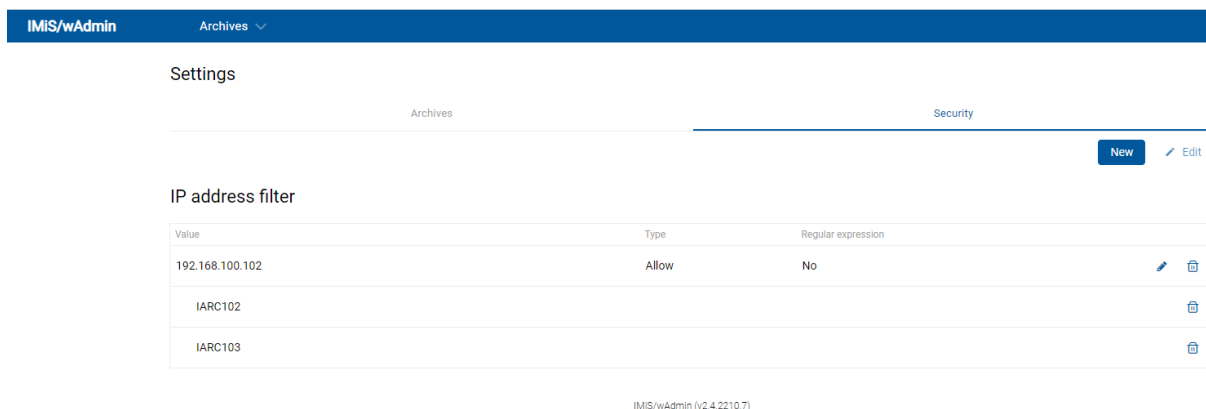
Regular expression

<input type="checkbox"/> Name	Display name
<input type="checkbox"/> IARC101AKR	10.1 AKR [iarc101akr.imis.si]
<input type="checkbox"/> IARC101X64	10.1 x64 [iarc101-x64.imis.si]
<input checked="" type="checkbox"/> IARC102	10.2 [iarc102.imis.si]
<input type="checkbox"/> IARC102AKR	10.2 AKR [iarc102akr.imis.si]
<input type="checkbox"/> 704	704
<input type="checkbox"/> IARC910	9.10 [iarc910.imis.si]
<input type="checkbox"/> IARC910AKR	9.10 AKR [iarc910akr.imis.si]
<input type="checkbox"/> IARC910R2	9.10 R2 [iarc910-r2.imis.si]
<input type="checkbox"/> IARC910R2X64	9.10 R2 x64 [iarc910-r2-x64.imis.si]
<input type="checkbox"/> IARC96	9.6 [iarc96.imis.si]
<input type="checkbox"/> IARC97	9.7 [iarc97.imis.si]
<input type="checkbox"/> IARC98	9.8 [iarc98.imis.si]
<input type="checkbox"/> IARC98AKR	9.8 AKR [iarc98akr.imis.si]
<input type="checkbox"/> IARC99	9.9 [iarc99rc.imis.si]
<input type="checkbox"/> IARC99AKR	9.9 AKR [iarc99akr.imis.si]
<input checked="" type="checkbox"/> IARC103	IMIS/ARChive Server

2 archives selected  Add another

Slika 50: Dodajanje IP naslova za izbrane arhivske strežnike

Po potrditvi izbire (angl. Save), se IP naslov prikaže v seznamu. Uporabnik ga lahko ureja z izbiro ikone , oziroma odstrani z uporabo ikone .







Settings

Archives Security

New Edit


IP address filter

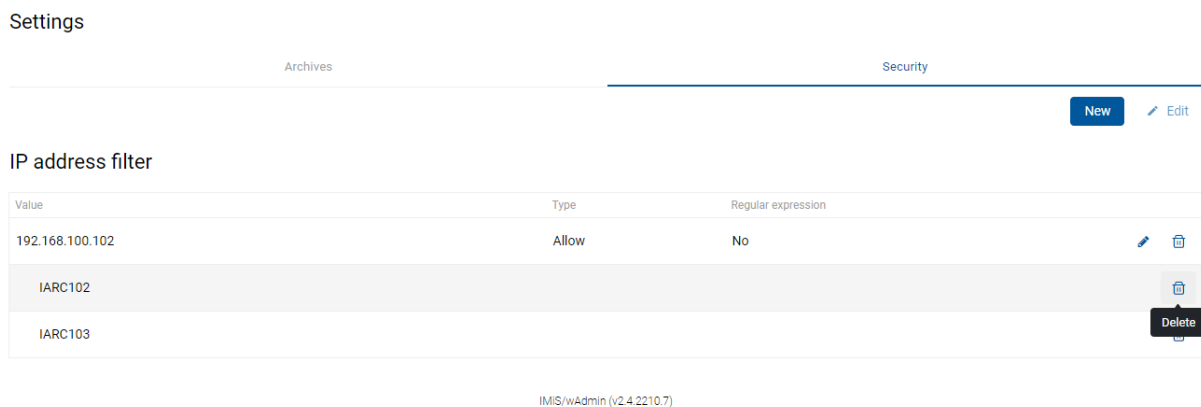
Value	Type	Regular expression	
192.168.100.102	Allow	No	 
IARC102			
IARC103			

IMIS/wAdmin (v2.4.2210.7)

Slika 51: Prikaz nastavitve IP naslova v seznamu

***Opomba:** Nastavitve IP naslovov se shranijo v bazo v novo tabelo `access_filter` (`id: int, value: string, type: int[1=Allow,2=Deny,3=AllowRegEx,4=DenyRegEx]`).*

Prijavljeni uporabnik lahko odstrani IP naslov za dostop do vseh arhivskih strežnikov ali smo za določene. V seznamu izbere ustrezen IP naslov ali arhivski strežnik ter ikono .







Settings

Archives Security

New Edit

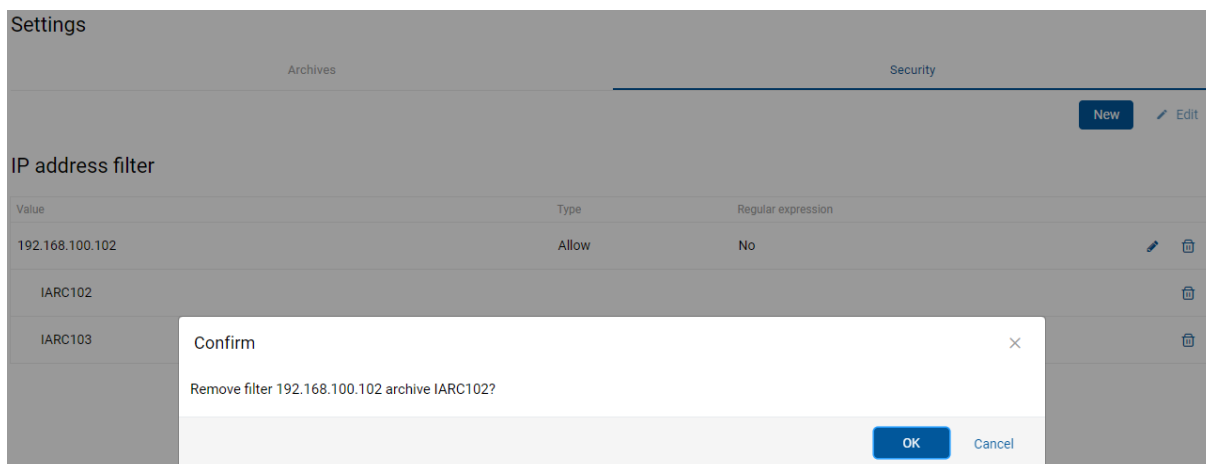
IP address filter

Value	Type	Regular expression	
192.168.100.102	Allow	No	 
IARC102			
IARC103			

IMIS/wAdmin (v2.4.2210.7)

Slika 52: Izbira arhivskega strežnika za odstranitev

Po izbiri ikone za odstranitev arhivskega strežnika se prijavljenemu uporabniku prikaže pogovorno okno za potrditev izbire.



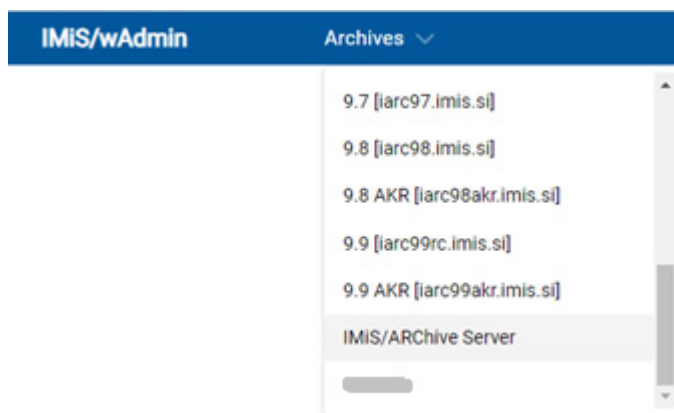
Slika 53: Odstranitev arhivskega strežnika

Po odstranitvi IP naslova za dostop do arhivskega strežnika le-ta ni več viden v seznamu.

### 8.5.2 Prijava in odjava

Prijavljeni uporabnik dostopa do administracijskega vmesnika IMiS®/wAdmin preko spletnega brskalnika (Google Chrome, Mozilla Firefox, MS Edge, ...) tako, da v naslovno vrstico vpiše URL naslov do administracijskega vmesnika. Prikaže se prijavno okno, kjer lahko izvede prijavo v strežnika IMiS®/ARChive Server.

Z izbiro puščice poleg naziva »Arhivi« (angl. Archives) se odpre pojavni meni, kjer izbere ustrezen arhivski strežnik.



Slika 54: Izбира arhiva iz pojavnega menija

Uporabnik se prijavi z izbiro arhivskega strežnika v seznamu in vpisom uporabniškega imena in gesla v prijavno okno.

Login

IMIS/ARChive Server

admin

.....

Login

Slika 55: Vpis uporabniškega imena in gesla v prijavno okno

V razdelku »Arhivi« (angl. Archives) se pod seznamom arhivskih strežnikov nahaja podatek o različici administracijskega vmesnika IMiS®/wAdmin.

IMiS/wAdmin (v2.4.2210.7)



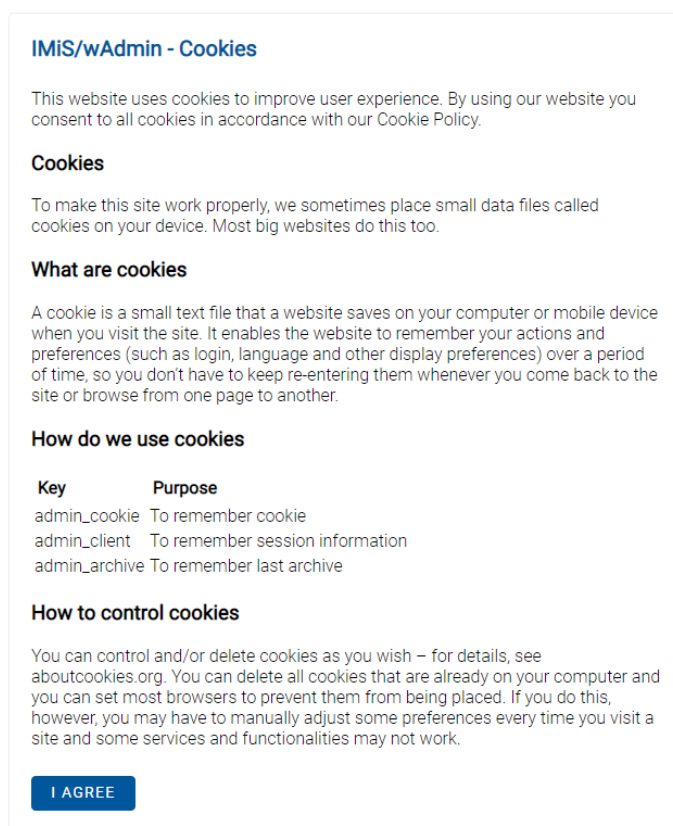
Slika 56: Različica administracijskega vmesnika IMiS®/wAdmin

### 8.5.2.1 Politika piškotkov

Pred prvo prijavo v strežnik in vsako naslednjo v kolikor so bili piškotki odstranjeni, mora prijavljeni uporabnik podati soglasje k uporabi piškotkov.

Za zagotavljanje ustreznega delovanja in boljše uporabniške izkušnje uporablja spletno mesto naslednje piškotke:

- Zapomni si zadnji izbrani strežnik (angl. To remember last selected archive).
- Žeton strežnika (angl. Archive token).
- Potrditev politike (angl. Policy agreed).



**IMiS/wAdmin - Cookies**

This website uses cookies to improve user experience. By using our website you consent to all cookies in accordance with our Cookie Policy.

**Cookies**

To make this site work properly, we sometimes place small data files called cookies on your device. Most big websites do this too.

**What are cookies**

A cookie is a small text file that a website saves on your computer or mobile device when you visit the site. It enables the website to remember your actions and preferences (such as login, language and other display preferences) over a period of time, so you don't have to keep re-entering them whenever you come back to the site or browse from one page to another.

**How do we use cookies**

Key	Purpose
admin_cookie	To remember cookie
admin_client	To remember session information
admin_archive	To remember last archive

**How to control cookies**

You can control and/or delete cookies as you wish – for details, see [aboutcookies.org](http://aboutcookies.org). You can delete all cookies that are already on your computer and you can set most browsers to prevent them from being placed. If you do this, however, you may have to manually adjust some preferences every time you visit a site and some services and functionalities may not work.

**I AGREE**

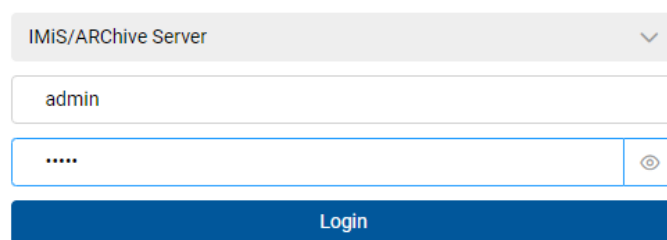
Slika 57: Soglasje k uporabi piškotkov

### 8.5.2.2 Prijava

Uporabnik se prijavi tako, da:

- Izbere arhivski strežnik iz seznama.
- Vpiše uporabniško ime (angl. User name).
- Vpiše geslo (angl. Password).


## Login




IMIS/wAdmin (v2.4.2210.7)



Slika 58: Prijava v strežnik

Po vpisu vsaj enega znaka gesla se prijavljenemu uporabniku prikaže ikona . Z izbiro ikone se uporabniku prikažejo znaki gesla.

Ikona  ob vnosnem polju za vpis gesla omogoča prikaz gesla samo kadar je gumb za prikaz aktiven (angl. mousedown).

Uporabnik se lahko prijavi v več arhivskih strežnikov v več zavihkih brskalnika.

Pri prikazu prijavnne strani po odjavi uporabnika, ostane uporabniška seja še vedno odprta.

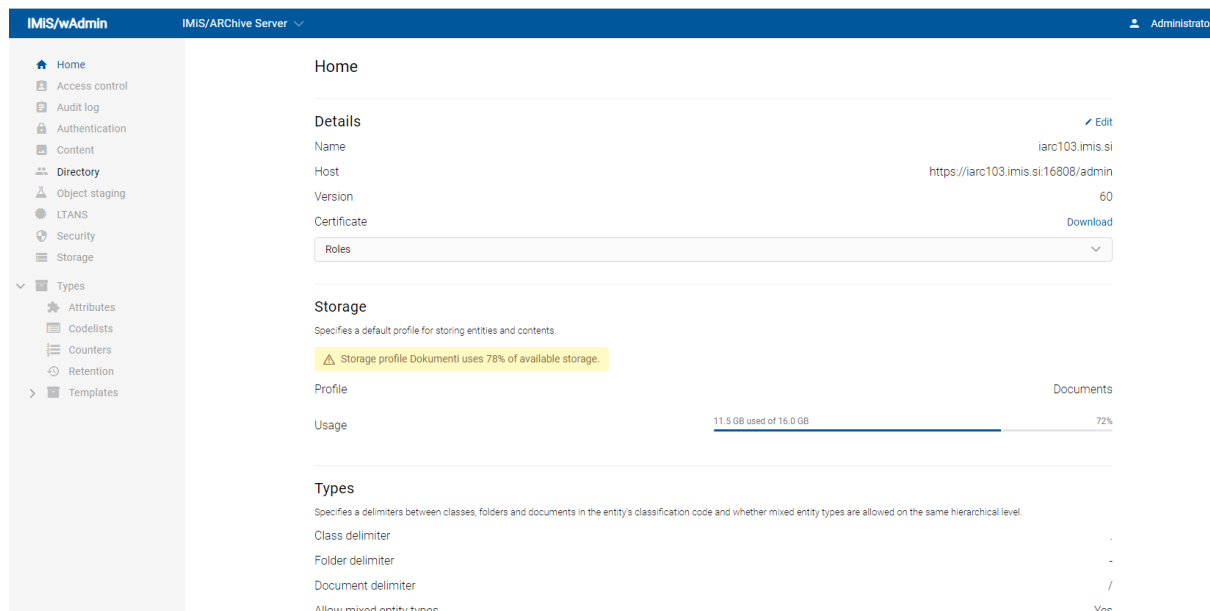
V primeru osvežitve brskalnika ostane uporabnik prijavljen v zadnjem arhivskem strežniku.

V kolikor se po osvežitvi brskalnika identifikator arhiva ne ujema z URL, se prikaže prijavnna stran.



Po uspešni prijavi se uporabniku prikažejo:

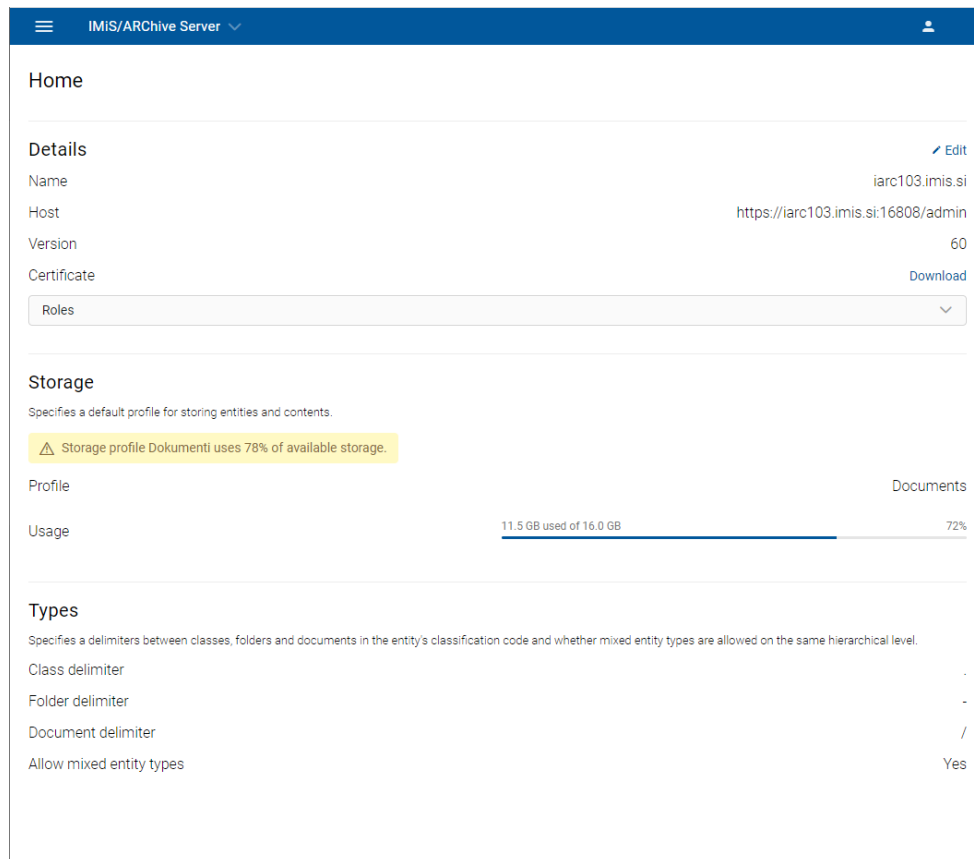
- Konfiguracijske mape v levem prikazu.
- Osnovne nastavitve strežnika ter pregled dostopnih pravic do konfiguracijskih map in vlog za prijavljenega uporabnika v osrednjem prikazu.



The screenshot shows the IMIS/wAdmin interface. The top navigation bar includes 'IMIS/wAdmin', 'IMIS/ARChive Server', and 'Administrator'. The left sidebar contains a menu with categories like 'Home', 'Directory', 'Storage', and 'Types'. The main content area is titled 'Home' and contains three sections: 'Details', 'Storage', and 'Types'. The 'Details' section shows a table with fields: Name (iarc103.imis.si), Host (https://iarc103.imis.si:16808/admin), Version (60), and Certificate (Download). Below this is a 'Roles' dropdown menu. The 'Storage' section has a warning: 'Storage profile Dokumenti uses 78% of available storage.' It shows a profile 'Documents' with a usage bar indicating '11.5 GB used of 16.0 GB' (72%). The 'Types' section lists delimiters: Class delimiter (.), Folder delimiter (-), Document delimiter (/), and Allow mixed entity types (Yes).


Slika 59: Osnovni prikaz po prijavi

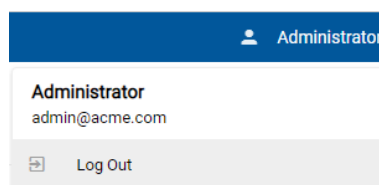
V primeru, da je uporabniku na voljo manjše okno brskalnika (širina je manjša od 800px), lahko osnovni prikaz prilagodi. Konfiguracijske mape v levem prikazu so tako na voljo preko menija, v poljih, kjer se oznake in vrednosti nahajajo ena poleg druge (v eni vrstici), pa se z ožanjem okna vrednosti prikažejo ena pod drugo.



Slika 60: Prilagoditev prikaza manjšemu oknu brskalnika

### 8.5.2.3 Odjava

Odjavo iz strežnika izvede prijavljeni uporabnik preko ikone  in naziva uporabnika. V pojavnem meniju izbere dejanje »Odjava« (angl. Log out).



Slika 61: Odjava uporabnika

### 8.5.3 Konfiguriranje strežnika

Konfiguriranje strežnika IMiS®/ARChive Server je omogočeno prijavljenemu uporabniku, ki ima:

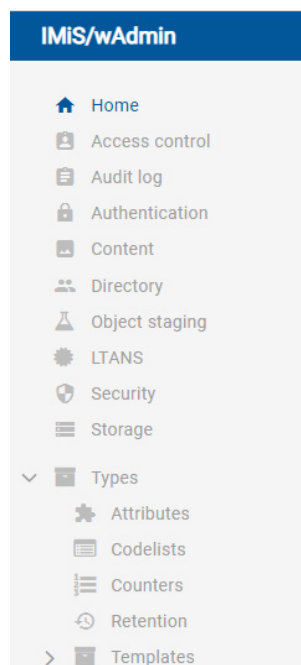
- Pravico spreminjanja posamezne konfiguracijske mape.
- Vključeno HTTP avtentikacijo.
- Ustvarjeno geslo.

Prijavljeni uporabnik ima možnost vpogleda in/ali urejanja nastavitvev v naslednjih konfiguracijskih mapah:

- »Domov« (angl. Home): vsebuje nastavitve strežnika.
- »Nadzor dostopov« (angl. Access Control): vsebuje seznam uporabnikov, skupin in atributov tipa imeniška entiteta, katerim prijavljeni uporabnik določi pravice dostopa do entitet in atributov.
- »Revizijska sled« (angl. Audit log): vsebuje naslednje nastavitve revizijske sledi: obvezne parametre za vzpostavitev povezave s strežnikom (angl. Required), dejanja na vsebini (angl. Content) in entitetami (angl. Entity), ki se beležijo v revizijski sledi.
- »Avtentikacija« (angl. Authentication): vsebuje seznam sistemskih nastavitvev povezav in zunanjih imenikov.
  - »Podrobnosti« (angl. Details): vsebuje nastavitve avtentikacije in avtorizacije.
  - »Priključki« (angl. Connectors): vsebuje seznam vtičnikov (angl. Plugin).
  - »Zunanji imeniki« (angl. External directories): vsebuje seznam zunanjih imenikov.
- »Vsebina« (angl. Content): vsebuje mape z nastavitvami dostopa do vsebin:
  - »Elektronski podpisi« (angl. Digital signatures): vsebuje nastavitve obsega izvajanja elektronskega podpisovanja;
  - »Indeksiranje celotnega besedilu« (angl. Full text index): vsebuje nastavitve indeksiranja celotnega besedila;
  - »Obdelava vsebin« (angl. Processing engine): vsebuje lastnosti dostopa do vsebin v strežniku;
  - »Pretvorniki« (angl. Converters): vsebuje nastavitve pretvornikov vsebin.
  - »Razčlenjevalniki« (angl. Parsers): vsebuje seznam razčlenjevalnikov vezanih na preverjanje elektronskih podpisov in vsebin;
  - »Tipi vsebin« (angl. Content types): vrste vsebin nad katero se izvajajo dejanja.

- »Imenik« (angl. Directory): vsebuje seznam uporabnikov strežnika s pripadajočimi podatki o uporabniku, avtentikaciji, vlogah in pravicah dostopa do konfiguracijskih map.
- »Nestrukturirana hramba« (angl. Object staging): vsebuje mape za nastavitve parametrov nastrukturiranega arhiviranja.
  - »Shranjevalni profili« (angl. Storage profiles): določa nastavitve (predloga, identifikator vsebnika, nazive, opise, ... ipd,.) za vsakokratni strežniški profil, ko se ta uporabi za nestrukturirano arhiviranje;
  - »Vsebniki objektov« (angl. Object containers): določa atribut vsakokratne predloge, ko se ta uporabi za nestrukturirano arhiviranje;
  - »Vrste vsebin« (angl. Content type aliases): vsebuje prevedbeno tabelo vrst vsebin, ki se uporablja za nestrukturirano arhiviranje.
- »Zagotavljanje integritete dolgoročno hranjenih vsebin« (angl. LTANS): vsebuje mape z nastavitvami časovnega žigosanja vsebin.
  - »Podrobnosti« (angl. Details): vsebuje nastavitve lastnosti časovnega žigosanja;
  - »Ponudniki časovnih žigov« (angl. Timestamp providers): vsebuje seznam ponudnikov časovnega žigosanja;
  - »Pravila časovnega žigosanja« (angl. Timestamping rules): vsebuje seznam pravil časovnega žigosanja;
  - »Pravila veriženja časovnih žigov« (angl. Timestamp chaining rules): vsebuje seznam pravil veriženja časovnih žigov.
- »Varnost« (angl. Security): vsebuje mape z nastavitvami varnostnih mehanizmov:
  - »Javni atributi z neomejenim dostopom« (angl. Unrestricted public attributes): vsebuje varnostne nastavitve za javne attribute;
  - »Shramba digitalnih potrdil« (angl. Certificate store): vsebuje mape za dodajanje digitalnih potrdil, omogočanje/onemogočanje digitalnih potrdil, iskanje digitalnih potrdil in iskanje po seznamih preklicanih digitalnih potrdil;
  - »Digitalna potrdila« (angl. Certificates): vsebuje seznam digitalnih potrdil.
- »Arhiv« (angl. Storage): vsebuje mape za profile in volumne določene na strežniku:
  - »Nazivi profilov« (angl. Profile names): vsebuje seznam profilov določenih na strežniku;
  - »Volumni« (angl. Volumes): vsebuje seznam vseh volumnov na strežniku.

- »Tipi« (angl. Types): vsebuje mape z nastavitvami atributov, šifrantov, številčenjem, hrambo in predloge:
  - »Atributi« (angl. Attributes): vsebuje seznam uporabniško nastavljenih in sistemskih atributov, katerim prijavljeni uporabnik določi lastnosti.
  - »Šifranti« (angl. Codelists): vsebuje seznam uporabniško nastavljenih atributov, katerim prijavljeni uporabnik določi nabor vrednosti in sistemskih atributov katerih vrednosti lahko pregleduje.
  - »Številčenje« (angl. Counters): prijavljeni uporabnik določi globino drevesa entitet v načrtu razvrščanja gradiva in način zapisa klasifikacijske oznake za posamezno vrsto entitete na določenem nivoju.
  - »Hramba« (angl. Retention): vsebuje mapi z nastavitvami politik hrambe in zadržanj uničenja:
    - »Politike hrambe« (angl. Retention policies): vsebuje seznam politik hrambe za arhivirano gradivo;
    - »Zadržanje uničenja« (angl. Disposition holds): vsebuje seznam zadržanj uničenja za arhivsko gradivo.
  - »Predloge« (angl. Templates): vsebuje seznam predlog, katerim uporabniki določijo attribute.



Slika 62: Konfiguracijske mape v levem meniju IMiS®/wAdmin

Ovisno od izbrane konfiguracijske mape so prijavljenemu uporabniku na voljo naslednja dejanja:

- »Uredi« (angl. Edit): urejanje nastavitvev.
- »Shrani« (angl. Save): shranitev nastavitvev ali sprememb vrednosti.
- »Opusti« (angl. Cancel): opustitev sprememb.
- »Dodaj« (angl. Add): dodajanje entitet/atributov/volumnov/vsebin iz seznama. Ukaz je na voljo samo za uporabniško nastavljivih entitet/atributov/volumnov/vsebin.
- »Izbris« (angl. Delete): odstranitev izbranih entitet/vsebin/volumnov iz seznama. Ukaz je na voljo samo za uporabniško nastavljive entitete/vsebine, ko je izbrana entiteta odprta v načinu za urejanje (angl. Edit).
- »Vsi« (angl. All): omogoča pregled vseh entitet/vsebin.
- »Prikaz sistemskih atributov/števec/predlog« (angl. Show system attributes/codelists/templates): prikaz sistemskih atributov/števec/predlog.

### 8.5.3.1 Mapa Domov

Mapa »Domov« (angl. Home) vsebuje nastavitve strežnika razvrščene v naslednje razdelke:

- »Osnovne nastavitve« (angl. Details)
- »Shranjevalni profil« (angl. Storage)
- »Vrste prikaza« (angl. Types).

Home

---

**Details** [Edit](#)

Name	iarc102.imis.si
Host	https://iarc102.imis.si:16808/admin
Version	59
Certificate	<a href="#">Download</a>

Roles ▼

---

**Storage**

Specifies a default profile for storing entities and contents.

⚠ Storage profile Dokumenti uses 79% of available storage.

Profile	Documents
Usage	9.3 GB used of 16.0 GB <span style="float: right;">58%</span>

---

**Types**

Specifies a delimiters between classes, folders and documents in the entity's classification code and whether mixed entity types are allowed on the same hierarchical level.

Class delimiter	-
Folder delimiter	-
Document delimiter	/
Allow mixed entity types	Yes

Slika 63: Prikaz osnovnega pregleda v mapi »Domov«

## Osnovne nastavitve

Prijavljeni uporabnik pregleduje ali ureja (angl. Edit) naslednje nastavitve:

- »Naziv« (angl. Name): privzeti naziv strežnika.
- »Strežnik« (angl. Host): pot do strežnika.
- »Različica sheme« (angl. Version): različica WSDL sheme.
- »Digitalno potrdilo« (angl. Certificate): potrdilo strežnika.
- »Vloge« (angl. Roles): sistemske vloge in pravice dostopa do konfiguracijskih map za prijavljenega uporabnika.

**Details** [Edit](#)

Name	iarc103.imis.si
Host	https://iarc103.imis.si:16808/admin
Version	60
Certificate	<a href="#">Download</a>

Roles ▼

Slika 64: Pregled nastavitvev v razdelku »Podrobnosti« v načinu za branje

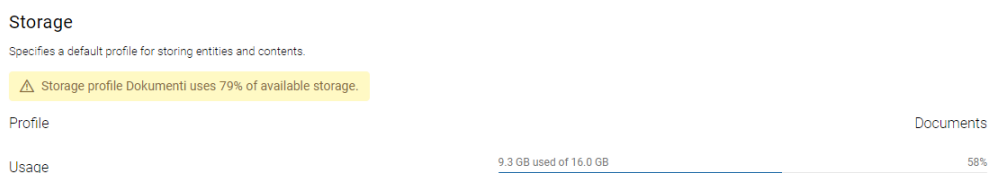
Roles		Access
System		
Audit log query		✓
Import/Export		✓
Content management		✓
Reports		✓
Draft management		✓
Configuration		
	Read	Update
AAA settings	✓	✓
Access control	✓	✓
Archive settings	✓	✓
Attributes	✓	✓
Audit log settings	✓	✓
Codelists	✓	✓
Content settings	✓	✓
Counters	✓	✓
Directory entity	✓	✓
Directory group	✓	✓
Object staging	✓	✓
LTANS settings	✓	✓
Profiles	✓	✓
Retention	✓	✓
Security settings	✓	✓
Templates	✓	✓
Volumes	✓	✓

Slika 65: Pregled sistemskih vlog in pravic dostopa do konfiguracijskih map

## Shranjevalni profil

Prijavljeni uporabnik lahko pregleduje ali ureja (angl. Edit) naslednje nastavitve vrednosti:

- »Profil« (angl. Profile): privzeti profil za shranjevanje entitet in vsebin.
- »Uporabljeno« (angl. Usage): prikazuje velikost zasedenega prostora in odstotek zasedenosti prostora za posamezen profil v giga-bajtih (GB).



Slika 66: Pregled nastavitve v razdelku »Shranjevalni profil« v načinu za urejanje

## Vrste prikaza

Prijavljeni uporabnik lahko pregleduje ali ureja (angl. Edit) naslednje nastavitve vrednosti:

- »Ločilni znak razreda« (angl. Class delimiter): ločilni znak v zapisu klasifikacijske oznake entitete med razredoma.
- »Ločilni znak zadeve« (angl. Folder delimiter): ločilni znak v zapisu klasifikacijske oznake entitete med razredom ali zadevo in zadevo.
- »Ločilni znak dokumenta« (angl. Document delimiter): ločilni znak v zapisu klasifikacijske oznake entitete med razredom ali zadevo in dokumentu.
- »Omogočanje mešanih tipov entitet« (angl. Allow mixed entity types): določa ali so na istem hierarhičnem nivoju dovoljeni mešani tipi entitet.

***Opomba:** V primeru onemogočenja shranjevanja mešanih tipov entitet, ko slednje že obstajajo, določa dovoljen tip entitete tip prve vsebovane entitete po njeni klasifikacijski oznaki.*

*Pri razvrščanju klasifikacijskih oznak je prva vsebovana entiteta tista, katere klasifikacijska oznaka je »najmanjša«.*

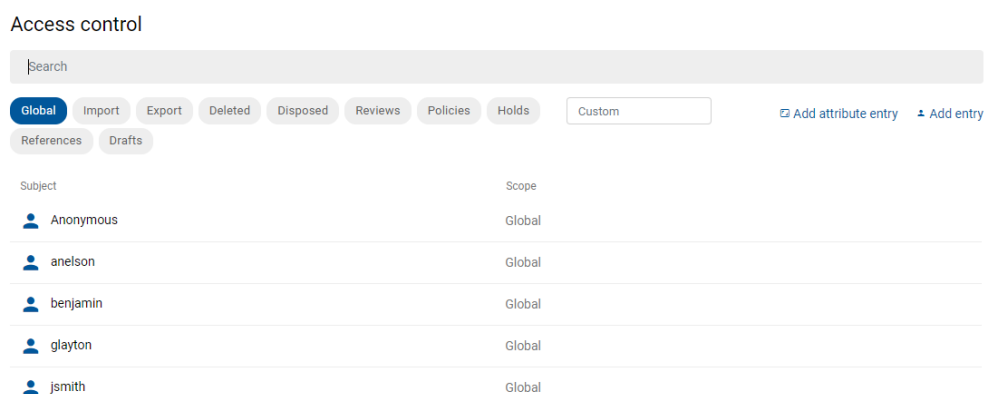
Slika 67: Pregled nastavitve v razdelku »Vrste prikaza« v načinu za urejanje



### 8.5.3.2 Mapa Nadzor dostopov

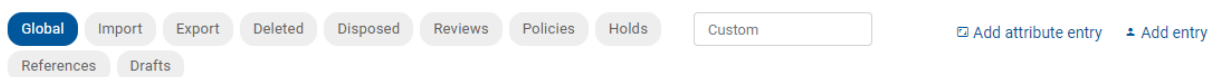
Mapa »Nadzor dostopov« (angl. Access control) vsebuje seznam entitet imenika (uporabnikov, skupin) in atributov tipa imeniška entiteta, katerim prijavljeni uporabnik na nivoju arhivskega strežnika določi dostopne pravice.

V osnovnem pregledu so prikazani nazivi entitet imenika in atributov tipa imeniška entiteta (angl. Subject), konteksti prikaza ter iskalnik.



Slika 68: Prikaz osnovnega pregleda v mapi »Nadzor dostopov«

Prijavljeni uporabnik najprej določi kontekst prikaza. Privzeta vrednost je »Globalno« (angl. Global).



Slika 69: Izbira konteksta v konfiguracijski mapi »Nadzor dostopov«

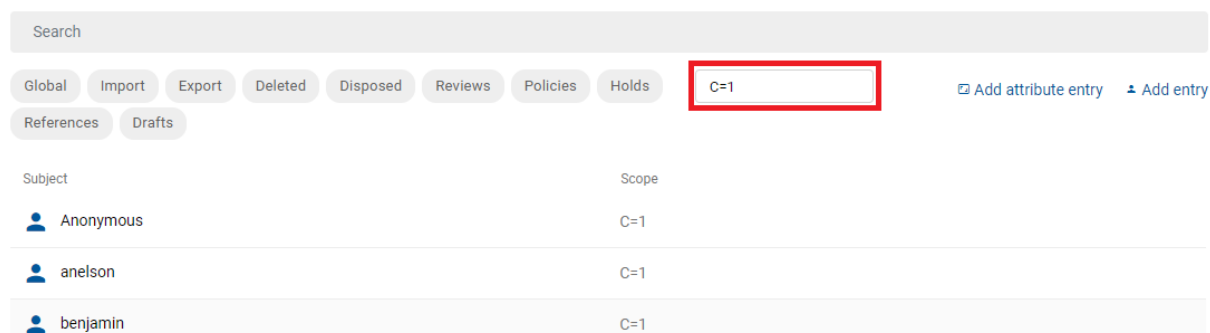
V seznamu lahko izbira med naslednjimi konteksti:

- »Globalno« (angl. Global): pravice dostopa do entitet in atributov na nivoju celotnega arhiva.
- »Uvoz« (angl. Import): pravice dostopa do entitet in atributov v administracijski mapi »Uvoz«.
- »Izvoz« (angl. Export): pravice dostopa do entitet in atributov v administracijski mapi »Izvoz«.




- »Izbrisani« (angl. Deleted): pravice dostopa do entitet in atributov v administracijski mapi »Izbrisani«.
- »Uničeni« (angl. Disposed): pravice dostopa do entitet in atributov v administracijski mapi »Uničeni«.
- »Pregledi« (angl. Reviews): pravice dostopa do entitet in atributov v administracijski mapi »Reviews«.
- »Politike« (angl. Policies): pravice dostopa do entitet in atributov v administracijski mapi »Politike«.
- »Zadržanja« (angl. Holds): pravice dostopa do entitet in atributov v administracijski mapi »Zadržanja«.
- »Reference« (angl. References): pravice ustvarjanja referenc na entitete v načrtu razvrščanja gradiva.
- »Osnutki« (angl. Drafts): pravice dostopa do osnutkov dokumentov.

Poleg navedenih kontekstov prikaza je omogočeno tudi določanje konteksta prikaza po meri. V vpisom konteksta prikaza v polje »Kontekst po meri« (angl. Custom), se v seznamu prikaže nabor entitet imenika in atributov tipa imeniška entiteta, ki ustrezajo želenemu obsegu iskanja (angl. Scope).

#### Access control



The screenshot shows the 'Access control' interface. At the top is a search bar. Below it are several filter buttons: Global, Import, Export, Deleted, Disposed, Reviews, Policies, Holds, C=1 (highlighted with a red box), Add attribute entry, and Add entry. Below the filters is a table with two columns: Subject and Scope.

Subject	Scope
 Anonymous	C=1
 anelson	C=1
 benjamin	C=1

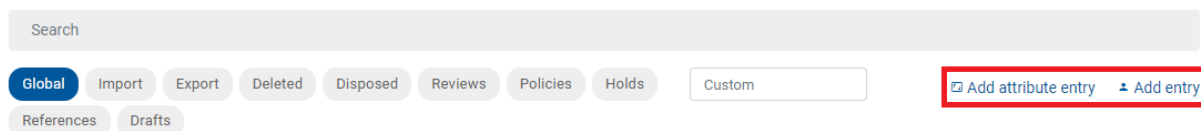
Slika 70: Prikaz osnovnega pregleda v kontekstu prikaza po meri

V naslednjem koraku določi entiteto imenika.

Novo entiteto imenika doda tako, da izbere dejanje »Dodaj entiteto imenika« (angl. Add entry).

Na enak način prijavljeni uporabnik doda nov atribut tipa imeniška entiteta tako, da izbere dejanje »Dodaj atribut tipa imeniška entiteta« (angl. Add attribute entry).

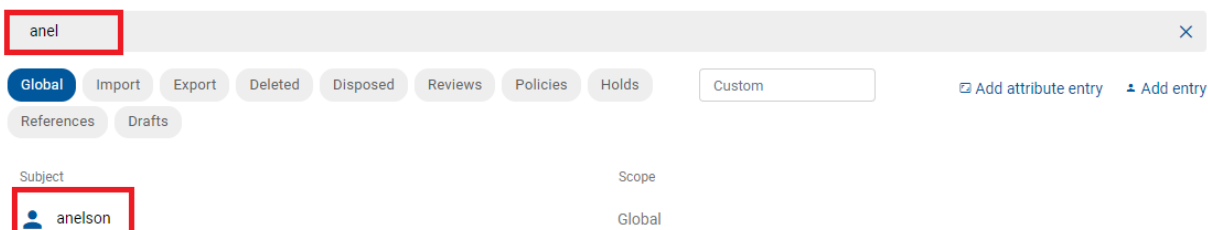
#### Access control



Slika 71: Dodajanje nove imeniške entitete ali atributa tipa imeniška entiteta

V kolikor entiteta imenika ali atribut tipa imeniška entiteta že obstaja v seznamu, jo lahko prijavljeni uporabnik poišče s pomočjo iskalnika. V iskalno polje vpiše iskalni niz in potrdi izbiro.

#### Access control



Slika 72: Vpis iskalnega niza v iskalnik

***Opomba:** Z vpisom znakov iskalnega niza, se ustrezno zoži nabor prikazanih rezultatov iskanja v seznamu. Po vpisu iskalnega niza v iskalnik, lahko prijavljeni uporabnik pregleduje enake rezultate iskanja tudi v ostalih kontekstih prikaza.*

### 8.5.3.2.1 Pravice dostopa do entitet in atributov za entitete imenika

Z izbiro dejanja »Dodaj entiteto imenika« (angl. Add Entry), se prijavljenemu uporabniku prikažeta naslednja razdelka:

- »Osnovne nastavitve« (angl. Details)
- »Lastnosti entitet« (angl. Property).

Access control >

**Details**

Subject

Type

Scope  Global

**Property**

Add permission  Add

Save Cancel

Slika 73: Prikaz razdelkov po izbiri dejanja »Dodaj entiteto imenika«

#### Osnovne nastavitve

Prijavljeni uporabnik izbere entiteto imenika (angl. Subject). Z vpisom iskalnega niza v polje »Izberi entiteto imenika« (angl. Select directory entity) omeji nabor razpoložljivih entitet imenika v spustnem meniju in ustrezno izbere.

Vrednost atributa »Vrsta uporabnika« (angl. Type) se določi samodejno ob izbiri entitete imenika.

Vrednost atributa »Obseg« (angl. Scope) se določi samodejno ob določitvi konteksta prikaza. Omogoča prikaz entitet imenika in njihovih pravic dostopa na nivoju arhivskega strežnika ali samo glede na določene funkcionalnosti strežnika.

V naslednjem koraku za entiteto imenika določi pravice dostopa do entitet (angl. Entity).

V razdelku »Dovoljenje« (angl. Permission) lahko prijavljeni uporabnik za vsako pravico dostopa določi eksplicitno dovoljenje (angl. Allow) ali prepoved (angl. Deny), ki velja na nivoju strežnika ali samo glede na določene funkcionalnosti.

Določijo lahko naslednje dostopne pravice na entiteti:

- »Vse pravice« (angl. Full access): vse pravice dostopa do podatkov o entiteti.
- »Branje« (angl. Read): pravica branja podatkov o entiteti.
- »Pisanje« (angl. Write): pravica urejanja podatkov o entiteti.
- »Premik« (angl. Move): pravica premika entitete znotraj načrta razvrščanja gradiva.
- »Brisanje« (angl. Delete): pravica brisanja podatkov o entiteti.
- »Ustvarjanje entitet« (angl. Create entities): pravica ustvarjanja vsebovanih entitet.
- »Spreminjanje pravic« (angl. Change permissions): pravica spreminjanja eksplicitnih pravic uporabnikov na entiteti.
- »Spreminjanje stopnje tajnosti« (angl. Change security class): pravica spreminjanja stopnje tajnosti entitete.
- »Spreminjanje statusa« (angl. Change Status): pravica spreminjanja statusa entitete.
- »Spreminjanje hrambe« (angl. Change Retention): pravica spreminjanja veljavnosti rokov hrambe entitete.
- »Ustvarjanje referenc« (angl. Create reference): pravica ustvarjanja referenc med entitetami.

V razdelku »Možnosti« (angl. Options) je prijavljenemu uporabniku omogočena izbira dodatnih parametrov za pravice dostopa:

- »Omogočeno za to entiteto« (angl. Enabled for this entity): pravice so omogočene na trenutni entiteti.
- »Omogočeno za vsebovane entitete« (angl. Enabled for subentities): dedovanje pravic je omogočeno na vsebovanih entitetah.
- »Kontekst delegata« (angl. Delegate context): upoštevanje pravic delegata v primeru njegove prijave v imenu uporabnika.

Z določitvijo vsaj ene pravice dostopa, lahko prijavljeni uporabnik v razdelku »Veljavnost« (angl. Validity) določi časovno veljavnost pravic. V koledarju za polja »Velja od« (angl. Valid from) in »Velja do« (Valid to) izbere datum in čas veljavnosti dovoljenja (angl. Allow) ali prepovedi (angl. Deny).

**Details**

Subject

Type User

Scope Global

**Entity**

Permission	Explicit	
Full access	ALLOW	DENY
Read	ALLOW	DENY
Write	ALLOW	DENY
Move	ALLOW	DENY
Delete	ALLOW	DENY
Create entities	ALLOW	DENY
Change permissions	ALLOW	DENY
Change security class	ALLOW	DENY
Change status	ALLOW	DENY
Change retention	ALLOW	DENY
Create references	ALLOW	DENY
<b>Options</b>		
Enabled for this entity	ALLOW	DENY
Enabled for subentities	ALLOW	DENY
Delegate context	ALLOW	DENY

Slika 74: Določanje dostopnih pravic do entitet za imeniško entiteto

### Lastnosti entitet

V razdelku »Lastnosti entitet« (angl. Property) prijavljeni uporabnik v načinu za urejanje izbere polje »Izberi atribut« (angl. Select attribute) in v seznamu ustrezen atribut.

Po potrditvi izbire z dejanjem »Dodaj« (angl. Add) določi še pravice dostopa do atributa.

**Options**

Enabled for this entity

Enabled for subentities

Delegate context

- sys.move:Agent
- sys.move:ClassificationCode
- sys.move:DateTime
- sys.move:Reason
- sys.ObjectEvidence
- sys.Owner

Add

Slika 75: Izbira atributa za določitev dostopnih pravic

Za vsak izbrani atribut lahko določi naslednja dovoljenja (angl. Allow) ali prepovedi (angl. Deny), ki veljajo na nivoju strežnika ali samo glede na določene funkcionalnosti:

- »Branje« (angl. Read): pravica branja vrednosti atributov.
- »Ustvarjanje« (angl. Create): pravica ustvarjanja vrednosti atributov.
- »Pisanje« (angl. Write): pravica pisanja vrednosti atributov.
- »Brisanje« (angl. Delete): pravica brisanja vrednosti atributov.

*Opomba:* Vse navedene pravice lahko naenkrat omogoči z izbiro dovoljenja (angl. Allow) ali onemogoči z izbiro prepovedi (angl. Deny) v nastavitvah parametra »Polni dostop« (angl. Full access).

V razdelku »Možnosti« (angl. Options) je omogočena izbira dodatnih parametrov za pravice dostopa:

- »Omogočeno za to entiteto« (angl. Enabled for this entity): pravice so omogočene na trenutni entiteti.
- »Omogočeno za vsebovane entitete« (angl. Enabled for subentities): dedovanje pravic je omogočeno na vsebovanih entitetah.
- »Kontekst delegata« (angl. Delegate context): upoštevanje pravic delegata v primeru njegove prijave v imenu uporabnika.

V razdelku »Veljavnost« (angl. Validity) prijavljeni uporabnik določi časovno veljavnost pravic. V koledarju za polja »Velja od« (angl. Valid from) in »Velja do« (Valid to) izbere datum in čas veljavnosti dovoljenja (angl. Allow) ali prepovedi (angl. Deny). Časovna veljavnost velja za vsa omogočena dovoljenja ali vse omogočene prepovedi.

Property

Add permission  Add

sys:Owner

Permission	Explicit	
Full access	Allow	Deny
Read	Allow	Deny
Create	Allow	Deny
Write	Allow	Deny
Delete	Allow	Deny

Options

Enabled for this entity	Allow	Deny
Enabled for subtentities	Allow	Deny
Delegate context	Allow	Deny

Validity

Allow between

Valid from  Valid to

Deny between

Valid from  Valid to

Delete this property entry

Save Cancel

Slika 76: Določanje pravic dostopa do atributov za imeniško entiteto

Prijavljeni uporabnik shrani nastavitve z dejanjem »Shrani« (angl. Save).

Pravice dostopa do atributa odstrani iz pregleda tako, da izbere dejanje »Odstrani to lastnost entitete« (angl. Delete this property entry).

### 8.5.3.2.2 Pravice dostopa do entitet za attribute tipa imeniška entiteta

Prijavljeni uporabnik lahko za vsak atribut tipa imeniška entiteta določi pravice dostopa do entitet. Z izbiro dejanja »Dodaj atribut tipa imeniška entiteta« (angl. Add Attribute Entry) v seznamu nastavi parametre za pravice dostopa.

Za več informacij glej poglavje [Pravice dostopa do entitet in atributov za imeniške entitete](#).

Access control > sys:Owner

Details

Subject	sys:Owner
Type	Attribute
Scope	Global

[Delete this entry](#)

Entity

Property

Add permission  Add

SAVE CANCEL

Slika 77: Določanje pravic dostopa za atribut tipa imeniška entiteta



Prijavljeni uporabnik lahko poleg pravic dostopa do entitet za vsak atribut tipa imeniška entiteta, določi tudi pravice dostopa do atributov.

V razdelku »Lastnosti entitet« (angl. Property) prijavljeni uporabnik v načinu za urejanje izbere polje »Izberi atribut« (angl. Select attribute) in v seznamu ustrezen atribut. Po potrditvi izbire z dejanjem »Dodaj« (angl. Add) določi še pravice dostopa do atributa.

Za več informacij glej poglavje [Pravice dostopa do entitet in atributov za imeniške entitete](#).

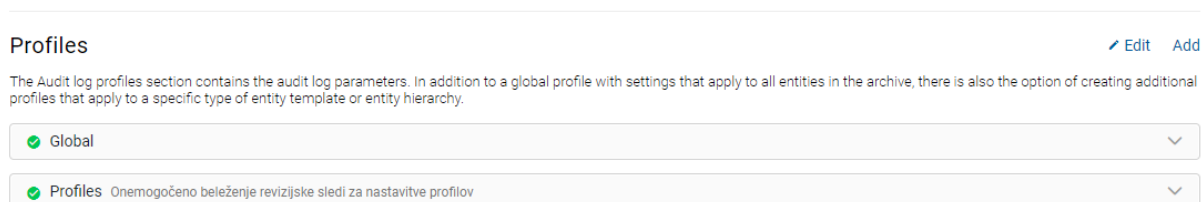
### 8.5.3.3 Mapa Revizijska sled

Mapa »Revizijska sled« (angl. Audit log) vsebuje nastavitve parametrov revizijske sledi.

Poleg globalnega profila z nastavitvami, ki velja za vse entitete v arhivu, ima prijavljeni uporabnik možnost ustvarjanja dodatnih profilov, ki veljajo za določeno vrsto predloge entitete ali hierarhijo entitet.

Za razliko od drugih profilov, se na globalnem profilu ne prikažejo naslednji atributi in njihove vrednosti: »Območje« (angl. Scope), »Predloge« (angl. Templates) in »Identifikator« (angl. Identifier).

#### Audit log



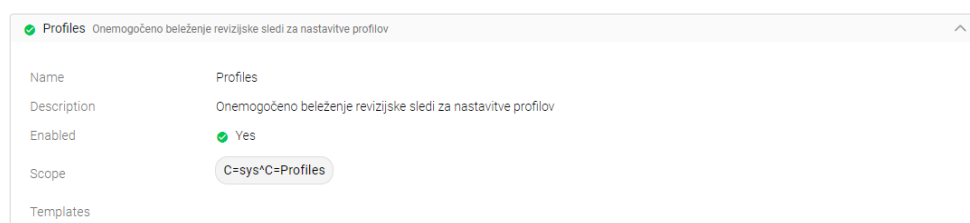
Slika 78: Prikaz osnovnega pregleda v mapi »Revizijska sled«

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi nastavitve novega profila revizijske sledi.

#### Osnovne nastavitve

- »Naziv profila« (angl. Name)
- »Opis profila« (angl. Description)
- »Omogočeno« (angl. Enabled) označitev parametra pomeni, da se nastavitve profila revizijske sledi upoštevajo. Nasprotno, z odznačitvijo prijavljeni uporabnik določi, da profil ni omogočen, oziroma se nastavitve profila ne upoštevajo.

- »Območje« (angl. Scope): določa nad katerim delom klasifikacijskega drevesa je omogočen profil revizijske sledi. Prijavljeni uporabnik lahko pregleduje in/ali spreminja naslednje nastavitve:
  - »Vrsta« (angl. Type): določa vrsto identifikatorja entitete (klasifikacijska oznaka, zunanji ali interni);
  - »Vrednost« (angl. Value): določa vrednost identifikatorja entitete.  
Vrednost označuje, da veljajo nastavitve revizijske sledi za entitete uvrščene pod izbrano in njej vsebovanimi entitetami. Če vrednost ni določena pomeni, da omejitev ni in da se nastavitve revizijske sledi upoštevajo za vse entitete na strežniku.
- »Predloge« (angl. Templates): z izbiro predloge prijavljeni uporabnik določi entitete osnovane na tej predlogi, za katere je omogočen profil revizijske sledi.



Slika 79: Osnovne nastavitve profila

### Obvezni dogodki

V razdelku »Obvezni dogodki« (angl. Required) prijavljeni uporabnik omogoči ali onemogoči obvezne dogodke revizijske sledi na nivoju strežnika.

Določi lahko naslednje vrednosti:

- »Naziv računalnika« (angl. Computer name): v revizijsko sled se obvezno zabeleži naziv računalnika.
- »Razlog« (angl. Reason): v revizijsko sled se obvezno zabeleži razlog za izvedbo dejanja.
- »Naslov računalnika« (angl. Private address): v revizijsko sled se obvezno zabeleži IP naslov računalnika.
- »Uporabniško ime« (angl. Username): v revizijsko sled se obvezno zabeleži uporabniško ime.

Required	<input type="checkbox"/> Check all	<input type="checkbox"/> Private address
	<input type="checkbox"/> Computer name	<input type="checkbox"/> Username
	<input type="checkbox"/> Reason	

Slika 80: Seznam obveznih dogodkov revizijske sledi

### Dogodki na vsebini

V razdelku »Dogodki na vsebini« (angl. Content) se prikažejo naslednje nastavitve vrednosti:

- »Ustvarjanje vsebine« (angl. Content create): v revizijsko sledi se zabeleži dejanje ustvarjanja vsebine.
- »Spreminjanje atributov vsebine« (angl. Content metadata change): v revizijsko sled se zabeleži dejanje spreminjanja vrednosti atributov vsebine.
- »Odpiranje« (angl. Content open read-only): v revizijsko sled se zabeleži dejanje odpiranja entitete v načinu za branje.
- »Shranjevanje« (angl. Content save): v revizijsko sled se zabeleži dejanje shranjevanja sprememb vsebine.
- »Brisanje vsebine« (angl. Content delete): v revizijsko sled se zabeleži dejanje brisanja vsebine.
- »Premik vsebine« (angl. Content move): v revizijsko sled se zabeleži dejanje premika vsebine.
- »Odpiranje« (angl. Content Open read-write): v revizijsko sled se zabeleži dejanje odpiranja entitete v načinu za branje in pisanje.

Content	<input checked="" type="checkbox"/> Check all	<input checked="" type="checkbox"/> Content delete
	<input checked="" type="checkbox"/> Content create	<input checked="" type="checkbox"/> Content move
	<input checked="" type="checkbox"/> Content metadata change	<input checked="" type="checkbox"/> Content open read-write
	<input checked="" type="checkbox"/> Content open read-only	
	<input checked="" type="checkbox"/> Content save	

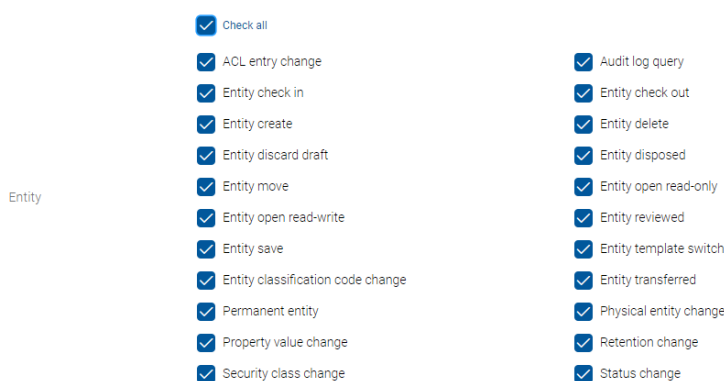
Slika 81: Seznam dogodkov revizijske sledi na vsebini

### Dogodki na entiteti

V razdelku »Dogodki na entiteti« (angl. Entity) so prijavljenemu uporabniku na voljo naslednje nastavitve vrednosti:

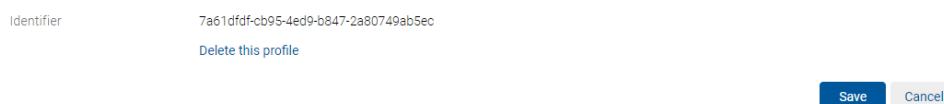
- »Spreminjanje nadzora dostopov do entitete« (angl. ACL entry change): v revizijsko sled se zabeleži dejanje spreminjanja nadzora dostopov.
- »Objava osnutka dokumenta« (angl. Entity check in): v revizijsko sled se zabeleži dejanje objave osnutka dokumenta.
- »Ustvarjanje entitete« (angl. Entity create): v revizijsko sled se zabeleži dejanje ustvarjanja entitete.
- »Zavrženje osnutka dokumenta« (angl. Entity discard draft): v revizijsko sled se zabeleži dejanje zavrženja osnutka dokumenta.
- »Premikanje entitete« (angl. Entity move): v revizijsko sled se zabeleži dejanje premika entitete.
- »Odpiranje entitete v načinu za branje in pisanje« (angl. Entity open read-write): v revizijsko sled se zabeleži dejanje odpiranja entitete v načinu za branje in pisanje.
- »Shranjevanje entitete« (angl. Entity save): v revizijsko sled se zabeleži dejanje shranjevanja entitete.
- »Spreminjanje klasifikacijske oznake« (angl. Entity classification code change): v revizijsko sled se zabeleži dejanje spreminjanja relativnega dela klasifikacijske oznake entitete.
- »Stalnost entitete« (angl. Permanent entity): v revizijsko sled se zabeleži dejanje označevanja entitete za trajno v postopku odbiranja in izločanja.
- »Spreminjanje atributov« (angl. Property value change): v revizijsko sled se zabeleži dejanje spreminjanja vrednosti atributov entitete.
- »Spreminjanje stopnje tajnosti entitete« (angl. Entity security class change): v revizijsko sled se zabeleži dejanje spreminjanja stopnje tajnosti entitete.
- »Revizijska sled« (angl. Audit log query): v revizijsko sled se zabeleži iskanje po revizijski sledi.
- »Izdelava osnutka dokumenta« (angl. Entity check out): v revizijsko sled se zabeleži dejanje izdelave osnutka dokumenta.
- »Brisanje entitete« (angl. Entity delete): v revizijsko sled se zabeleži dejanje brisanja entitete.

- »Uničenje entitete« (angl. Entity disposed): v revizijsko sled se zabeleži dejanje uničenja entitete v postopku odbiranja in izločanja.
- »Odpiranje entitete v načinu za branje« (angl. Entity open read-only): v revizijsko sled se zabeleži dejanje odpiranja entitete v načinu za branje.
- »Pregled entitete« (angl. Entity reviewed): v revizijsko sled se zabeleži dejanje pregleda entitete v postopku odbiranja in izločanja.
- »Zamenjava predloge entitete« (angl. Entity template switch): v revizijsko sled se zabeleži dejanje zamenjave predloge entitete.
- »Prenos entitete« (angl. Entity transferred): v revizijsko sled se zabeleži dejanje prenosa entitete v postopku odbiranja in izločanja.
- »Spreminjanje atributov fizičnega gradiva« (angl. Physical entity change): v revizijsko sled se zabeleži dejanje spreminjanja vrednosti atributov fizičnega gradiva.
- »Spreminjanje roka hrambe« (angl. Retention change): v revizijsko sled se zabeleži dejanje spreminjanja roka hrambe entitete v postopku odbiranja in izločanja.
- »Spreminjanje statusa entitete« (angl. Status change): v revizijsko sled se zabeleži dejanje spreminjanja statusa entitete.



Slika 82: Seznam dogodkov revizijske sledi na entiteti

Prijavljeni uporabnik shrani nastavitve z dejanjem »Shrani« (angl. Save). Po shranitvi je uporabniku na voljo unikatni »Identifikator profila revizijske sledi« (angl. Identifier).



Slika 83: Identifikator profila revizijske sledi

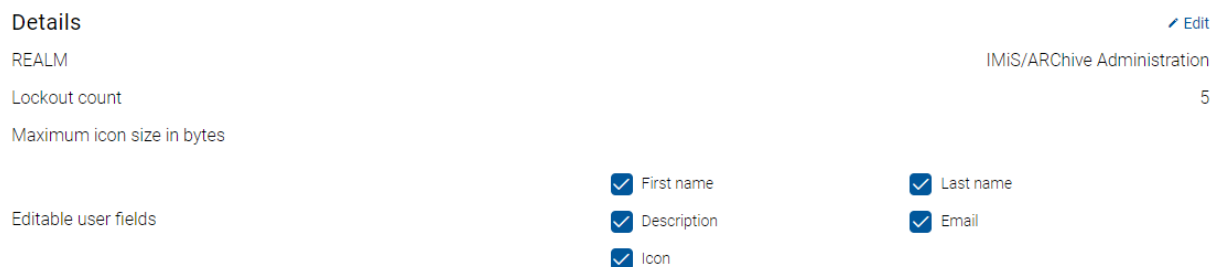
*Opomba:* Vse nastavitve parametrov v posameznem razdelku lahko naenkrat omogoči ali onemogoči z izbiro dejanja »Označi vse« (angl. *Check all*).

*Opomba:* Sprememba nastavitve revizijske sledi začne veljati po odjavi in ponovni prijavi v spletni administracijski vmesnik IMiS®/wAdmin.

### 8.5.3.4 Mapa Avtentikacija

Mapa »Avtentikacija« (angl. *Authentication*) vsebuje naslednje razdelke:

- »Osnovne nastavitve« (angl. *Details*)
- »Priključki« (angl. *Connectors*)
- »Zunanji imeniki« (angl. *External directories*).



Details [Edit](#)

REALM IMiS/ARChive Administration

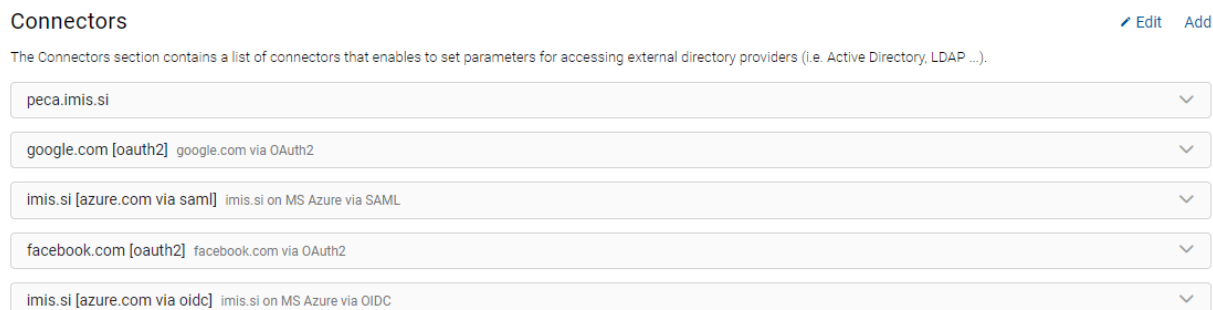
Lockout count 5

Maximum icon size in bytes

Editable user fields

- First name
- Last name
- Description
- Email
- Icon

Slika 84: Prikaz osnovnega pregleda v razdelku »Osnovne nastavitve«

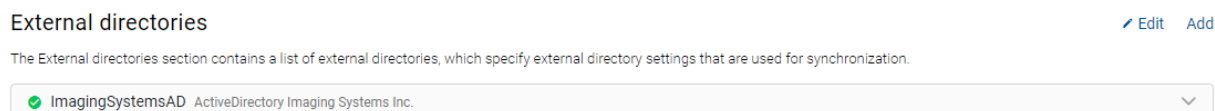


Connectors [Edit](#) [Add](#)

The Connectors section contains a list of connectors that enables to set parameters for accessing external directory providers (i.e. Active Directory, LDAP ...).

- peca.imis.si
- google.com [oauth2] google.com via OAuth2
- imis.si [azure.com via saml] imis.si on MS Azure via SAML
- facebook.com [oauth2] facebook.com via OAuth2
- imis.si [azure.com via oidc] imis.si on MS Azure via OIDC

Slika 85: Prikaz osnovnega pregleda v razdelku »Priključki«



External directories [Edit](#) [Add](#)

The External directories section contains a list of external directories, which specify external directory settings that are used for synchronization.

- ImagingSystemsAD ActiveDirectory Imaging Systems Inc.

Slika 86: Prikaz osnovnega pregleda v razdelku »Zunanji imeniki«

## Osnovne nastavitve

Razdelek »Osnovne nastavitve« (angl. Details) vsebuje nastavitve avtentikacije in avtorizacije uporabnikov. Prijavljeni uporabnik lahko ureja (angl. Edit) naslednje nastavitve:

- »Domena« (angl. Realm): Domena Kerberos storitve. Privzeta vrednost je enaka omrežni domeni z velikimi črkami.
- »Število neuspešnih prijav« (angl. Lockout count): število neuspešnih zaporednih prijav uporabnika na strežnik IMiS®/ARChive Server pred onemogočanjem dostopa. Velja za lokalne in zunanje uporabnike, če ti uporabljajo lokalno metodo prijave v strežnik IMiS®/ARChive Server. V primeru uporabe zunanjih avtentikacij (LDAP, Kerberos, ...), pa število neuspešnih zaporednih prijav pred zaklenitvijo računa določa zunanja imeniška storitev. Stanje zaklenjenosti računa določa atribut imeniške entitete »Locked«. Ta je v primeru sinhroniziranosti entitete imenika del sinhroniziranih atributov.
- »Največja velikost ikone v bajtih« (angl. Max icon size in bytes): določa največjo velikost datoteke z ikono, ki ponazarja uporabnika ali skupino uporabnikov.
- »Urejevalna polja uporabniškega profila« (angl. Editable user fields): določa polja entitet imenika (uporabnikov), ki jih je mogoče urejati:
  - »Ime« (angl. First name): ime uporabnika;
  - »Opis« (angl. Description): kratek opis uporabnika;
  - »Ikona« (angl. Icon): slika uporabnika;
  - »Priimek« (angl. Last name): priimek uporabnika;
  - »Elektronska pošta« (angl. Email): elektronska pošta uporabnika.

Details

REALM

Lockout count

Maximum icon size in bytes

Editable user fields

First name  Last name

Description  Email

Icon

Slika 87: Nastavitev parametrov v razdelku »Osnovne nastavitve«

## Priključki

Razdelek »Priključki« (angl. Connectors) vsebuje seznam priključkov, ki omogočajo prijavitelju uporabniku nastavitve parametrov za dostop do:

- ponudnikov zunanjih imenikov (npr. Active Directory, LDAP, ...);
- zunanjih ponudnikov identitet, ki omogočajo OIDC ali SAML 2.0 (Google, Microsoft, Okta ...).

Za več informacij glej poglavje [Avtentikacija z zunanjim ponudnikom identitete](#).

Z izbiro dejanja »Dodaj« (angl. Add) prijaviteljni uporabnik določi naslednje nastavitve:

- Naziv« (angl. Name): unikatni identifikator priključka.
- »Opis« (angl. Description): opis priključka.
- »Identifikator priključka« (angl. Provider identifier): unikatni identifikator priključka.
- »Gonilnik« (angl. Driver): gonilnik priključka.
- »Argumenti« (angl. Arguments): argumenti priključka, specifični za vsakokratno vrsto priključka. V parameter prijaviteljni uporabnik vnese XML niz konfiguracijskih podatkov, ki jih vtičnik uporabi pri inicializaciji priključka (naslov in poverilnice za dostop do zunanje imeniške storitve, parametri povezave, prevedbene tabele atributov, ... ipd.).

The screenshot shows the 'Connectors' configuration page. At the top, there is a title 'Connectors' and an 'Add' button. Below the title, a subtitle reads: 'The Connectors section contains a list of connectors that enables to set parameters for accessing external directory providers (i.e. Active Directory, LDAP ...)'.

The main configuration area is for a connector named 'peca.imis.si'. It includes the following fields:

- Name:** peca.imis.si
- Description:** (empty)
- Provider identifier:** ad-peca.imis.si
- Driver:** libiajaa.so.1
- Arguments:** A text area containing XML configuration code:
 

```
1 <Class>com.imis.imisarc.server.aaa.impl.ActiveDirectory</Class>
2 <LdapURL>ldap://peca.imis.si/</LdapURL>
3 <LdapUsername>iarc/</LdapUsername>
4 <LdapPassword>volvo850</LdapPassword>
5 <LdapAuthenticationType>DIGEST-MD5</LdapAuthenticationType>
6 <LdapBaseDN>DC=imis,DC=si/</LdapBaseDN>
7 <LdapUserDN>OU=IMIS,</LdapUserDN>
8 <LdapGroupDN>OU=IMIS,</LdapGroupDN>
9 <LdapUserObjectFilter>(objectClass=user)</LdapUserObjectFilter>
10 <LdapGroupObjectFilter>(objectClass=group)</LdapGroupObjectFilter>
11 <LdapAuthenticationFilter>(&(objectCategory=person)(objectClass=user))((userPrincipalName=%s)(mail=
12 <KrbServicePrincipal>IARC/iarc102.imis.si@IMIS.SI/</KrbServicePrincipal>
13 <KrbKeytabLocation>iarc/work/IARC@iarc102.imis.si.keytab/</KrbKeytabLocation>
14 <AccountAliasList>SAMAccountName,userPrincipalName,distinguishedName/</AccountAliasList>
```
- Identifier:** 04bfb5e-9167-454b-8390-e2971bc8a236

At the bottom right of the configuration area, there are 'Save' and 'Cancel' buttons. A 'Delete this connector' link is also visible below the identifier.

Slika 88: Nastavitve parametrov v razdelku »Priključek«



Po shranitvi (angl. Save) je priključek na voljo prijavljenemu uporabniku v razdelku »Priključek« (angl. Connector) v osnovnem pregledu nastavitve mape »Avtentikacija«.

## Connectors

[Edit](#) [Add](#)

The Connectors section contains a list of connectors that enables to set parameters for accessing external directory providers (i.e. Active Directory, LDAP ...).

peca.imis.si

google.com [oauth2] google.com via OAuth2

Name

Description

Provider identifier google.com\_oauth2

Driver

Arguments

```
1 <Class>com.imis.imisarc.server.aaa.impl.GenericImpersonationOIDCATValidator</Class>
2 <!-- OIDC server id which must be present in audience -->
3 <ClientId>711286933972-aeghc7pfeibsub9vc1l52vtqjifve8p.apps.googleusercontent.com</ClientId>
4 <ImpersonateClientId>711286933972-aeghc7pfeibsub9vc1l52vtqjifve8p.apps.googleusercontent.com</Impers
5 <WellKnownDocument>https://accounts.google.com/.well-known/openid-configuration</WellKnownDocument>
6 <Debug>true</Debug>
7 <Field key="sys:dir:lid:Subject" type="string">sub</Field>
8 <Field key="sys:dir:lid:Issuer" type="string">iss</Field>
```

Identifier 24fd1468-c867-4257-8ab2-6cf5cbea960a

[Delete this connector](#)

imis.si [azure.com via saml] imis.si on MS Azure via SAML

facebook.com [oauth2] facebook.com via OAuth2

imis.si [azure.com via oidc] imis.si on MS Azure via OIDC

Slika 89: Primer nastavitve priključka za dostop do zunanjega ponudnika identitete

Prijavljeni uporabnik ureja nastavitve z izbiro načina za urejanje (angl. Edit). Priključek odstrani z dejanjem »Odstrani priključek« (angl. Delete this connector).

## Zunanji imeniki

Razdelek »Zunanji imeniki« (angl. External Directories) vsebuje seznam zunanjih imenikov.

Prijavljeni uporabnik določi nastavitve zunanjih imenikov, ki se uporabljajo za sinhronizacijo s strežnikom IMiS®/ARChive Server.

Z izbiro dejanja »Dodaj« (angl. Add) prijavljeni uporabnik določi naslednje nastavitve:

- »Naziv« (angl. Name): naziv zunanjega imenika.
- »Opis« (angl. Description): opis zunanjega imenika.
- »Omogočena sinhronizacija« (angl. Enabled): označitev parametra pomeni, da je sinhronizacija omogočena. Nasprotno, z odznačitvijo prijavljeni uporabnik onemogoči sinhronizacijo zunanjega imenika z internim imenikom strežnika.
- »Priključek« (angl. Connector): unikatni naziv priključka.
- »Urnik« (angl. Schedule): urnik izvajanja sinhronizacije. Privzeta vrednost je prazen niz, kar pomeni, da se sinhronizacija zunanjega imenika z internim imenikom strežnika ne izvaja.

*Primer: Nastavitev 0 5 \* \* \* \* pomeni, da sinhronizacija izvaja vsakih 5 minut.*

Sintaksa je naslednja:

0 – sekunde (0 - 59)

5 – minute (0 - 59)

\* - ure (0 - 23)

\* - dan v mesecu (1 - 31)

\* - mesec (1 – 12)

\* - dan v tednu (0 – 6 [ponedeljek - petek], v nekaterih sistemih lahko tudi 7 [nedelja])

- »Možnosti« (angl. Options): omogoča izbiro dodatnih parametrov zunanjega imenika. Prijavljeni uporabnik lahko določi naslednja polja:
  - »Omogočena sinhronizacija« (angl. Synchronization Enabled): označen parameter pomeni, da so podatki o uporabniku sinhronizirani z zunanjim imenikom. Z odznačitvijo prijavljeni uporabnik onemogoči sinhronizacijo uporabnika z zunanjim imenikom.
  - »Sinchronizacija skupin« (angl. Synchonize groups): označitev parametra pomeni, da je sinhronizacija skupin omogočena. Nasprotno, z odznačitvijo prijavljeni uporabnik onemogoči sinhronizacijo skupin zunanjega imenika z internim imenikom strežnika.
  - »Brisanje neznanih entitet« (angl. Delete unknown entities): označitev parametra pomeni, da entitete v imeniku, ki jih med sinhronizacijo z zunanjim virom imeniške storitve ne najde, ne bodo brisane iz internega imenika strežnika. Nasprotno, z odznačitvijo prijavljeni uporabnik omogoči brisanje teh entitet med sinhronizacijo zunanjega imenika z internim imenikom strežnika.

- »Ujemanje UUID« (angl. UUID match): označitev parametra omogoči preverjanje ujemanja UUID (Unique User IDentifier) z enim od identifikatorjev Subject ali Alias. Uporabnik ustvarjen z enakim nazivom in drugačnim UUID kot že shranjeni uporabnik se ne sinhronizira, ker se UUID ne ujema. Nasprotno, z odznačitvijo parametra prijavljeni uporabnik onemogoči preverjanje ujemanja UUID. V tem primeru se bo sinhroniziral katerikoli uporabnik, ne glede na njegov UUID. Privzeto je parameter označen.
- »Sinhronizacijska polja uporabnikov« (angl. User fields): označitev posameznega parametra pomeni, da je sinhronizacija zunanega imenika z internim imenikom strežnika na nivoju določenega polja uporabnika omogočena. Nasprotno, z odznačitvijo prijavljeni uporabnik onemogoči sinhronizacijo polja uporabnika. Privzeto so vsi parametri odznačeni. Prijavljeni uporabnik lahko določi naslednja polja:
  - »Ime« (angl. First name): ime uporabnika.
  - »Priimek« (angl. Last name): priimek uporabnika.
  - »Opis« (angl. Description): opis pozicije uporabnika v podjetju.
  - »Elektronska pošta« (angl. Email): naslov elektronske pošte uporabnika.
  - »Stopnja tajnosti uporabnika« (angl. Security class level): določa do katerega nivoja tajnosti lahko uporabnik pregleduje gradivo.
  - »Ikona« (angl. Icon): slika uporabnika.
  - »Sinonim« (angl. Aliases): vsebuje alternativna uporabniška imena za uporabnika, s katerimi lahko dostopa do arhiva.
  - »Omogočeno« (angl. Enabled): omogočanje dostopa do strežnika.
  - »Pooblaščenci« (angl. Delegates): registrirani uporabniki, ki se v postopku prijave lahko predstavijo kot pooblaščene osebe za druge uporabnike in v njihovem imenu izvajajo operacije.
  - »Zaklenjeno« (angl. Locked): omogočanje dostopa uporabnikov do arhiva glede na pravice.
  - »Napredna avtentikacija« (angl. Advanced authentication): uporaba zapletenejših (HMAC) metod vzpostavitve seje s strežnikom, ki predvideva obvezne in neobvezne metapodatke o odjemalcu.
  - »Zunanja avtentikacija« (angl. External authentication): prijava zunanjih uporabnikov preko zunanjega imenika.

- »Lokalna avtentikacija« (angl. Local authentication): lokalna prijava uporabnika v strežnik z uporabo uporabniškega imena in gesla.
- »Lokalna avtentikacija preko HTTP« (angl. Local authentication over HTTP): prijava uporabnika v konfiguracijo strežnika preko HTTP protokola.
- »Avtentikacija z uporabo deljenega ključa« (angl. Pre-shared key authentication): prijava uporabnika v strežnik z deljenim ključem. Med postopkom prijave se ugotavlja identiteta uporabnika na osnovi zaupnega ključa, ki si ga delita odjemalec in strežnik.
- »Povezovanje identitet« (angl. Identity linking): omogočanje povezav z zunanjimi entitetami.
- »Sinchronizacijska polja skupin« (angl. Group fields): označitev posameznega parametra pomeni, da je sinchronizacija zunanlega imenika z internim imenikom strežnika na nivoju določenega polja skupine omogočena. Nasprotno, z odznačitvijo prijavljeni uporabnik onemogoči sinchronizacijo polja skupine.

Prijavljeni uporabnik lahko določi naslednja polja:

- »Ime« (angl. First name): prvo ime skupine.
- »Priimek« (angl. Last name): drugo ime skupine.
- »Opis« (angl. Description): opis pozicije skupine v podjetju.
- »Elektronska pošta« (angl. Email): naslov elektronske pošte skupine.
- »Stopnja tajnosti uporabnika« (angl. Security class level): določa do katerega nivoja tajnosti lahko skupina pregleduje gradivo.
- »Ikona« (angl. Icon): slika skupine uporabnikov.
- »Sinonim« (angl. Aliases): alternativna imena za skupino.
- »Omogočeno« (angl. Enabled): omogočanje dostopa skupini do strežnika.
- »Člani skupine« (angl. Members): seznam članov skupine.
- »Identifikator« (angl. Identifier): unikatni identifikator zunanlega imenika.

## External directories

[Edit](#) [Add](#)

The External directories section contains a list of external directories, which specify external directory settings that are used for synchronization.

✓ ImagingSystemsAD ActiveDirectory Imaging Systems Inc.
⌵

Name	ImagingSystemsAD	
Description	ActiveDirectory Imaging Systems Inc.	
Enabled	✓ Yes	
Connector	peca.imis.si	
Schedule	0 6 * * * *	
Options	<input type="checkbox"/> Synchronization enabled	<input type="checkbox"/> Synchronize groups
	<input type="checkbox"/> Synchronize users	<input type="checkbox"/> Delete unknown entities
	<input type="checkbox"/> UUID match	
User fields	<input checked="" type="checkbox"/> First name	<input checked="" type="checkbox"/> Last name
	<input type="checkbox"/> Description	<input checked="" type="checkbox"/> Email
	<input type="checkbox"/> Security class level	<input type="checkbox"/> Icon
	<input type="checkbox"/> Aliases	<input checked="" type="checkbox"/> Enabled
	<input type="checkbox"/> Delegates	<input checked="" type="checkbox"/> Locked
	<input type="checkbox"/> Advanced authentication	<input checked="" type="checkbox"/> External authentication
	<input type="checkbox"/> Local authentication	<input type="checkbox"/> Local authentication over HTTP
	<input type="checkbox"/> Pre-shared key authentication	<input type="checkbox"/> Identity linking
	<input checked="" type="checkbox"/> First name	<input checked="" type="checkbox"/> Last name
	<input checked="" type="checkbox"/> Description	<input checked="" type="checkbox"/> Email
Group fields	<input checked="" type="checkbox"/> Security class level	<input checked="" type="checkbox"/> Icon
	<input checked="" type="checkbox"/> Aliases	<input checked="" type="checkbox"/> Enabled
	<input type="checkbox"/> Members	
Identifier	02f045ca-5596-49c7-acd8-fda51377df40	

Slika 90: Nastavitev parametrov v razdelku »Zunanji imeniki«

Z izbiro dejanja »Dodaj« (angl. Add) v razdelku »Avtentikacija«, Prijavljeni uporabnik doda avtentikacijsko metodo. Izbira lahko med naslednjimi možnostmi:

- »Avtentikacijska metoda« (angl. Method): določa način avtentikacije (npr. LDAP, Kerberos 5 Credentials, Kerberos 5 Service Ticket).
- »Priključek« (angl. Connector): unikatni naziv priključka.

Authentication
Add

■ Remove

Method

LDAP

⌵

Connector

peca.imis.si

⌵

■ Remove

Method

Kerberos 5 Service Ticket

⌵

Connector

peca.imis.si

⌵

Save

Cancel

Slika 91: Nastavitev parametrov v razdelku »Avtentikacijska metoda«

Po shranitvi (angl. Save) je zunanji imenik prijavljenemu uporabniku na voljo v razdelku »Zunanji imeniki« (angl. External Directories) v osnovnem pregledu nastavitve mape »Avtentikacija«.

#### External directories

[Add](#)

The External directories section contains a list of external directories, which specify external directory settings that are used for synchronization.

✔ ImagingSystemsAD ActiveDirectory Imaging Systems Inc.

Slika 92: Prikaz zunanjega imenika

Prijavljeni uporabnik ureja nastavitve z izbiro načina za urejanje (angl. Edit).

Zunanji imenik odstrani z dejanjem »Odstrani zunanji imenik« (angl. Delete this external directory). Avtentikacijsko metodo odstrani z dejanjem »Odstrani« (angl. Remove).

### 8.5.3.5 Mapa Vsebine

Mapa »Vsebine« (angl. Content) vsebuje naslednje razdelke:

- »Elektronski podpisi« (angl. Digital signatures).
- »Indeksiranje celotnega besedila« (angl. Full text index).
- »Nastavitve upravljanja z vsebinami« (angl. Processing engine).
- »Pretvorniki« (angl. Converters).
- »Razčlenjevalniki« (angl. Parsers).
- »Vrste vsebin« (angl. Content types).

#### Content

##### Digital signatures

[Edit](#)

The Digital signatures section contains digital signed content settings.

Details

##### Processing engine

[Edit](#)

The Processing engine section contains the settings to manage the Full text index and Converters processing.

✔ Details

##### Full text index

[Edit](#)

The Full text index section contains the settings for indexing the full text of documents.

com.imis.imisarc.server.fti.impl.LuceneProvider

##### Converters

[Add](#)

The Converters section contains the settings of content converters. They are used to convert content from one format to another.

## Parsers

[Edit](#) [Add](#)

The Parsers section contains parser properties settings.

com.imis.imisarc.server.parser.impl.XmlSignatureParser	▼
com.imis.imisarc.server.parser.impl.OutlookMsgEmailParser	▼
com.imis.imisarc.server.parser.impl.PdfSignatureParser	▼
com.imis.imisarc.server.parser.impl.EmlSignatureParser	▼
com.imis.imisarc.server.parser.impl.RFC822Parser	▼
com.imis.imisarc.server.parser.impl.TiffSignatureParser	▼
com.imis.imisarc.server.parser.impl.ContentParser	▼

## Content types

The Content types section contains a list of supported MIME content types on the server.

1884 content types	▼
--------------------	---

Slika 93: Prikaz osnovnega pregleda v mapi »Vsebine«

### 8.5.3.5.1 Elektronski podpisi

Razdelek »Elektronski podpisi« (angl. Digital signatures) vsebuje nastavitve elektronskega podpisovanja vsebin.

#### Digital signatures

[Edit](#)

The Digital signatures section contains digital signed content settings.

Details	▼
---------	---

Slika 94: Prikaz razdelka »Elektronski podpisi« v mapi »Vsebine«

Prijavljeni uporabnik lahko ureja (angl. Edit) naslednje nastavitve:

- »Obseg preverjanja podpisov« (angl. Scope): določa način preverjanja elektronskih podpisov. Izbira lahko med naslednjimi vrednostmi:
  - »Brez podpisa« (angl. None): označuje, da se preverjanje elektronskih podpisov vsebin ne izvaja;
  - »Elektronski podpis« (angl. Signature): označuje, da se izvaja samo preverjanje elektronskih podpisov vsebin;
  - »Elektronski podpis z digitalnim potrdilom« (angl. Signature with certificate): označuje, da se izvaja preverjanje elektronskih podpisov vsebin in digitalnih potrdil;

- »Elektronski podpis z digitalnim potrdilom in preklicem« (angl. Signature with certificate and revocation): označuje, da se izvaja preverjanje elektronskih podpisov vsebin, digitalnih potrdil in preklicev digitalnih potrdil;
- »Elektronski podpis z verigo digitalnih potrdil in preklicem« (angl. Signature with certificate chain and revocation): označuje, da se izvaja preverjanje elektronskih podpisov vsebin, veriga digitalnih potrdil in preklicev digitalnih potrdil;
- »Tip filtra« (angl. Filter disposition): določa ali so vrste vsebin vključene v preverjanje elektronskih podpisov ali ne. Izbira lahko med naslednjimi vrednostmi:
  - »Vključi« (angl. Include): označuje, da so navedene vrste vsebin vključene;
  - »Izključi« (angl. Exclude): označuje, da so navedene vrste vsebin izključene (privzeta vrednost).
- »Filter vrste vsebin« (angl. Filter content types): določa nastavitve filtra za vrste vsebin, nad katerimi bo izvedeno preverjanje elektronskih podpisov.

**Digital signatures**  
The Digital signatures section contains digital signed content settings.

**Details** ^

Scope v  
Signature with certificate

Filter disposition

Filter content types v Add  
application/pdf image/tiff x

Slika 95: Nastavitve parametrov v razdelku »Elektronski podpisi«

### 8.5.3.5.2 Indeksiranje besedila vsebin

Razdelek »Indeksiranje besedila vsebin« (angl. Full text index) vsebuje nastavitve indeksiranja besedila vsebin.

#### Full text index

[Edit](#)

The Full text index section contains the settings for indexing the full text of documents.

com.imis.imisarc.server.fti.impl.LuceneProvider v

Slika 96: Prikaz razdelka »Indeksiranje besedila vsebin« v mapi »Vsebine«



Prijavljeni uporabnik lahko ureja (angl. Edit) naslednje nastavitve:

- »Identifikator ponudnika« (angl. Provider identifier): določa identifikator ponudnika, ki se uporablja za indeksiranje besedila vsebin.
- »Obseg« (angl. Scope): določa obseg izgradnje indeksa besedila vsebin.  
Prijavljeni uporabnik lahko izbira med naslednjimi vrednostmi:
  - »Brez indeksiranja« (angl. None): določa, da se indeksiranje besedila vsebine ne izvaja;
  - »Indeksiranje vsebine« (angl. Content): določa, da se indeksiranje izvaja po besedilu vsebine brez njenih metapodatkov;
  - »Indeksiranje vsebine in metapodatkov« (angl. Content with metadata): določa, da se indeksiranje izvaja po besedilu in metapodatkih vsebine (privzeta vrednost).
- »Gonilnik« (angl. Provider Driver): gonilnik za indeksiranje besedila vsebin.
- »Argumenti« (angl. Provider Arguments): določa nastavitvene parametre gonilnika za indeksiranje besedila vsebin.
- »Tip« (angl. Filter disposition): določa ali so vrste vsebin vključene v indeksiranje po besedilu ali ne. Izbira lahko med naslednjimi vrednostmi:
  - »Vključi« (angl. Include): označuje, da so vrste vsebin vključene;
  - »Izključi« (angl. Exclude): vrste vsebin so izključene (privzeta vrednost).
- »Filter vrste vsebin« (angl. Filter content types): vrste vsebin nad katerimi se izvaja indeksiranje po besedilu vsebin.

Full text index Edit

The Full text index section contains the settings for indexing the full text of documents.

com.imis.imisarc.server.fti.impl.LuceneProvider

Provider identifier: com.imis.imisarc.server.fti.impl.LuceneProvider

Scope:

Provider driver:

Provider arguments:
 

```

1 <IndexUri>https://localhost:9200/iarc103</IndexUri>
2 <!--ApiKey>LVV2ZGnu0E3kazY4LVQyVWZxd0E6CXkZDBxUTZRbHloQn3jv2xrTWvIUQ==</ApiKey-->
3 <AuthenticationUsername>iarc103</AuthenticationUsername>
4 <AuthenticationPassword>iarc103</AuthenticationPassword>
5 <Debug>false</Debug>
6 <SSLSType>JKS</SSLSType>
7 <IncludeContentDescriptionField>false</IncludeContentDescriptionField>
8 <SSLSTFile>/iarc/work/es@iarc103.imis.si.jks</SSLSTFile>
9 <SSLSPassword>imisarc</SSLSPassword>
10 <SSLProtocols>TLS</SSLProtocols>

```

Filter disposition:

Filter content types:

Slika 97: Nastavitev parametrov v razdelku »Indeksiranje celotnega besedila«

### 8.5.3.5.3 Nastavitve upravljanja z vsebinami

Razdelek »Nastavitve upravljanja z vsebinami« (angl. Processing engine) vsebuje nastavitve upravljanja z vsebinami. Vsebuje nastavitve za indeksiranje besedila vsebin in konvertiranje vsebin.

#### Processing engine

[Edit](#)

The Processing engine section contains the settings to manage the Full text index and Converters processing.

Details

Slika 98: Prikaz razdelka »Nastavitve upravljanja z vsebinami« v mapi »Vsebine«

Prijavljeni uporabnik lahko ureja (angl. Edit) naslednje nastavitve:

- »Omogočeno« (angl. Enabled): določa ali je pretvorba vsebin omogočena ali ne. Označitev parametra pomeni, da je pretvorba vsebin omogočena. Z odznačitvijo prijavljeni uporabnik onemogoči pretvorbo.
- »Število izvedb« (angl. Tasks): določa število vzporednih opravil izvajanja pretvorbe vsebin.
- »Število vsebin v vrsti« (angl. Queue length): določa največje število nalog, ki jih strežnik IMiS®/ARChive Server naenkrat dodeli enemu opravilu za pretvorbo vsebin.
- »Število ponovitev« (angl. Retry count): določa število ponovitev poizkusov pretvorbe vsebin v primeru napak pri pretvorbi.
- »Interval števila ponovitev« (angl. Retry interval): določa najmanjši čas v sekundah med poizkusi pretvorbe vsebin, ko se ta konča z napako.

#### Processing engine

The Processing engine section contains the settings to manage the Full text index and Converters processing.

Details

Enabled	<input checked="" type="checkbox"/>
Tasks	<input type="text" value="1"/>
Queue length	<input type="text" value="100"/>
Retry count	<input type="text" value="5"/>
Retry interval	<input type="text" value="3600"/>

Save Cancel

Slika 99: Nastavitve parametrov v razdelku »Nastavitve upravljanja z vsebinami«

#### 8.5.3.5.4 Pretvorniki

Razdelek »Pretvorniki« (angl. Converters) vsebuje nastavitve pretvornikov vsebin.

Namenjeni so pretvarjanju vsebin iz enega formata v drugega.

##### Converters

[Add](#)

The Converters section contains the settings of content converters. They are used to convert content from one format to another.

Slika 100: Prikaz razdelka »Pretvorniki« v mapi »Vsebine«

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi naslednje nastavitve:

- »Naziv« (angl. Name): naziv pretvornika.
- »Opis« (angl. Description): opis pretvornika.
- »Identifikator pretvornika« (angl. Provider identifier): določa unikatni naziv pretvornika.
- »Operacija na izvorni vsebini« (angl. Source operation): določa operacijo, ki se izvede na izvorni vsebini ob pretvorbi.

Prijavljeni uporabnik lahko izbira med naslednjimi možnostmi:

- »Brez izvedbe« (angl. None): ob pretvorbi se operacija na izvorni vsebini ne izvede;
- »Brisanje po pretvorbi« (angl. Delete after conversion): izvorna vsebina se po pretvorbi izbriše;
- »Nadomesti z pretvorjeno vsebino« (angl. Replace with conversion output): izvorna vsebina se izbriše in po pretvorbi nadomesti z pretvorjeno vsebino.
- »Obseg« (angl. Scope): določa nad katerim delom klasifikacijskega drevesa se izvaja pretvorba. Prijavljeni uporabnik lahko pregleduje in/ali spreminja naslednje nastavitve:
  - »Vrsta« (angl. Type): določa vrsto identifikatorja entitete (klasifikacijska oznaka, zunanji ali interni);
  - »Vrednost« (angl. Value): določa vrednost identifikatorja entitete.

Nastavljena vrednost označuje, da se pretvorba izvaja nad entitetami uvrščenimi pod izbrano in njej vsebovanimi entitetami. Če vrednost ni določena pomeni, da omejitev ni in da pretvorba zajema vse entitete na strežniku.

- »Gonilnik« (angl. Driver): gonilnik za pretvorbo vsebin.
- »Argumenti« (angl. Arguments): določa nastavitvene parametre gonilnika za pretvorbo vsebin.

- »Tip filtra« (angl. Filter disposition): določa ali so vrste vsebin vključene v pretvorbo ali ne. Izbira lahko med naslednjimi vrednostmi:
  - »Vključi« (angl. Include): označuje, da so vrste vsebin vključene;
  - »Izključi« (angl. Exclude): vrste vsebin so izključene (privzeta vrednost).
- »Vrste vsebin« (angl. Filter content types): vrsta vsebine, nad katero se izvaja pretvorba.
- »Identifikator« (angl. Identifier): unikatni identifikator pretvornika.

AbbyFRE12\_TIF\_to\_PDFA Converts TIF to PDF/A 2A with OCR

Name: AbbyFRE12\_TIF\_to\_PDFA

Description: Converts TIF to PDF/A 2A with OCR

Provider identifier: AbbyFRE12\_TIF\_to\_PDFA

Source operation: None

Scope: Classification code C=8

Driver\*: libiafreconv.so.1

Arguments:

```

1 <WorkDirectory>/iarc/work/conv</WorkDirectory>
2 <SkipTextDetection>true</SkipTextDetection>
3 <HighlightSuspiciousCharacters>true</HighlightSuspiciousCharacters>
4 <CollectStatistics>true</CollectStatistics>
5 <ProcessingReason>Pretvorba v format, primeren za dolgoročno hrambo gradiva</ProcessingReason>
6 <Language>Slovenian</Language>
7 <Language>Croatian</Language>
8 <Language>German</Language>
9 <Language>Serbian (Cyrillic)</Language>
10 <Language>English</Language>
11 <OutputSettings contentType="application/pdf">
12 <Type>PDF/A-2A</Type>
13 </OutputSettings>

```

Filter disposition: Include Exclude

Filter content types: image/tiff

Identifier: f46c9b93-eb54-42f4-9712-40e2834c4a43

Output: application/pdf

Buttons: Save Cancel

Slika 101: Nastavitev parametrov v razdelku »Pretvornik«

Z izbiro dejanja »Dodaj izhodni format« (angl. Add output) v razdelku »Izhodni format« (angl. Output), prijavljeni uporabnik določi nastavitve izhodnih formatov vsebin za pretvorbo. Izbira lahko med naslednjimi možnostmi:

- »Vrsta vsebine« (angl. Content type): določa vrsto izhodnega formata vsebine. Atribut je obvezen.

- »Opis formata« (angl. Description expression): določa način zapisa naziva pretvorjene vsebine. V primeru določitve izraza za način zapisa naziva pretvorjene vsebine se ta upošteva pri nazivu pretvorjene vsebine. V nasprotnem primeru pa naziv ostane enak nazivu izvorne vsebine.
- »Možnosti« (angl. Options): omogoča izbiro dodatnih parametrov izhodnega formata vsebine:
  - »Vrsta za FTI« (angl. Queue for FTI): določa ali je izhodna vsebina uvrščena v vrsto za izdelavo indeksa za iskanje po besedilu vsebine. Označitev parametra pomeni, da bo pretvorjena vsebina uvrščena v vrsto za izdelavo indeksa za iskanje po besedilu vsebine. Z odznačitvijo prijavljeni uporabnik določi, da pretvorjena vsebina ne bo uvrščena v vrsto za indeksiranje.
  - »Nadomesti izvor« (angl. Replace source): določa ali se izvorna vsebina zamenja s pretvorjeno vsebino. Označitev parametra pomeni, da bo pretvorjena vsebina po pretvorbi nadomestila izvorno vsebino. Z odznačitvijo prijavljeni uporabnik določi, da pretvorjena vsebina ne bo nadomestila izvorne vsebine.
  - »Samostojno« (angl. Standalone): določa ali se pretvorjena vsebina na seznamu vsebin prikaže kot samostojna vsebine (se izloči iz reprezentacij izvorne vsebine). Označitev parametra pomeni, da bo pretvorjena vsebina prikazala kot samostojna vsebina. Z odznačitvijo prijavljeni uporabnik določi, da se pretvorjena vsebina prikaže kot reprezentacija izvorne vsebine.
- »Naslednji pretvornik« (angl. Next Converter): naziv naslednjega pretvornika vsebine. V primeru izbire pretvornika v seznamu, prvi pretvorbi vsebine sledi še pretvorba v druge formate. V nasprotnem primeru se izvede samo prvotna pretvorba.

The screenshot shows a dialog box titled 'Output' with a close button 'Add output' in the top right corner. The dialog contains the following fields and options:

- Content type: application/pdf
- Description expression: %DESC\_BASE%.pdf
- Options:  Queue for FTI,  Replace source,  Standalone
- Next converter: (empty dropdown menu)
- A link 'Delete this output' is located below the 'Next converter' field.

At the bottom of the dialog are two buttons: 'Save' and 'Cancel'.

Slika 102: Nastavitev parametrov v razdelku »Izhodni format«

Po shranitvi (angl. Save) je pretvornik prijavljenemu uporabniku na voljo v razdelku »Pretvorniki« (angl. Converters) v osnovnem pregledu nastavitve mape »Vsebine«.

Converters

[Edit](#) [Add](#)

AbbyyFRE12\_TIF\_to\_PDFA Converts TIF to PDF/A 2A with OCR

Slika 103: Prikaz pretvornika

Prijavljeni uporabnik ureja nastavitve v načinu za urejanje (angl. Edit).

Pretvornik odstrani z dejanjem »Odstrani pretvornik« (angl. Delete this converter).

Izhodni format odstrani z dejanjem »Odstrani« (angl. Remove).

#### Primeri uporabe:

Zaradi lažjega razumevanja postopka pretvorbe je v nadaljevanju je navedenih nekaj primerov.

#### Primer 1:

*Za primer vzemimo pretvorbo formatov JPEG, PNG in TIFF v MS Word dokument formata DOCX in PDF/A.*

*Nastavitve na strežniku določajo, da se:*

- *Vse vsebine formatov JPEG, PNG in TIFF se ob shranitvi pretvorijo v DOCX in PDF/A.*
- *Vse izvirne vsebine se ne brišejo ali nadomestijo z pretvorjenimi vsebinami (Source operation=None).*
- *Pretvorba se izvaja samo nad vsebinami uvrščenimi pod določenim korenskim razredom (C=2).*
- *Naziv pretvorjene vsebine se ne spreminja (Description expression=%DESC\_BASE%.docx in %DESC\_BASE% [OCR].pdf).*

**JPEG, PNG, TIF -> DOCX, PDF** Converts JPEG, PNG, TIF to DOCX and PDF/A 3A with OCR

Name:

Description:

Provider identifier:

Source operation:

Scope:

Driver\*:

Arguments: 

```

1 <WorkDirectory>/iarc/work/conv</WorkDirectory>
2 <SkipTextDetection>true</SkipTextDetection>
3 <HighlightSuspiciousCharacters>true</HighlightSuspiciousCharacters>
4 <CollectStatistics>true</CollectStatistics>
5 <ProcessingReason>Pretvorba v format, primeren za dolgoročno hrambo gradiva</ProcessingReason>
6 <Language>Slovenian</Language>
7 <Language>Croatian</Language>
8 <Language>German</Language>
9 <Language>Serbian (Cyrillic)</Language>
10 <Language>English</Language>
11 <OutputSettings contentType="application/pdf">
12   <Type>PDF/A-3A</Type>
13 </OutputSettings>

```

Filter disposition:

Filter content types:

Identifier:   
[Delete this converter](#)

**Output**

**application/vnd.openxmlformats-officedocument.wordprocessingml.document**

Content type:

Description expression:

Options:  Queue for FTI  Replace source  Standalone

Next converter:

[Delete this output](#)

**application/pdf**

Content type:

Description expression:

Options:  Queue for FTI  Replace source  Standalone

Next converter:

[Delete this output](#)

Slika 104 Nastavitve osnovnih lastnosti in izhodnih parametrov

Prikaz rezultata pretvorbe v spletnem odjemalcu IMiS®/wClient je naslednji:

dev-jure1 > Finance > Accounts Payable > Credit Notes > Approvals > Approval Overdue

Title

Approval notification.jpg

Approval notification [OCR].pdf

Approval notification [OCR].docx

Slika 105: Primer pretvorbe vsebine dokumenta

### Primer 2:

Za primer vzemimo vezano pretvorbo vsebin. Vsebina se najprej pretvori iz formata BMP v JPG.

Nastavitve na strežniku določajo, da se:

- Pretvorba se izvaja samo nad vsebinami uvrščenimi pod določenim korenskim razredom (C=74).
- Izvirne vsebine se ne brišejo ali nadomestijo z pretvorjenimi vsebinami (Source operation=None).
- Naziv pretvorjene vsebine se spremeni:
  - pretvorba iz BMP v JPG: *Description expression=%DESC\_BASE%-%NOW\_YEAR%-%NOW\_MONTH%-%NOW\_DAY%.jpg*
- Upošteva se povezava na naslednji pretvornik (ImageMagic-2).

#### Content / Converter

< BACK

MORE ▾

REMOVE

Name

IMIS/ARChive Server converter

Description

ImageMagic Converter

Provider Id

ImageMagic-5

Source operation

None

Scope

Classification Code

C=101

Driver\*

libiaconvim.so.1

Arguments

FORMAT

1 <WorkDirectory>/iarc/work/conversion/<WorkDirectory>

Filter disposition

Include

Filter content types

image/bmp

Press ENTER or TAB to add item

Identifier: c6d25a2e-f1ea-40ba-9267-39e4c6b72ef1



Output

Content type  
image/jpeg

Description expression  
%DESC\_BASE%-%NOW\_YEAR%-%NOW\_MONTH%-%NOW\_DAY%.jpg

Options  
 Queue for FTI  Replace source  Standalone

Next converter  
ImageMagic-2

REMOVE

SAVE CANCEL

Slika 106: Pretvorba iz BMP v JPG: nastavitve osnovnih lastnosti in izhodnih parametrov

V primeru izbire naslednjega pretvornika (angl. Next Converter), prvi pretvorbi vsebine v JPG format sledi še pretvorba v format TIFF.

Nastavitve na strežniku določajo, da se:

- Pretvorba v TIFF format se izvaja nad vsemi vsebinami formata BMP pod določenimi korenskim razredom (vrednost atributa Value postimo prazno).
- Naziv pretvorjene vsebine se spremeni: *Description expression*=%DESC\_BASE%.pdf [OCR, %PAGE\_COUNT%pages.

## Content / Converter

< BACK MORE ▾ REMOVE

Name

Description

Provider id  
ImageMagic-2

Source operation  
None

Scope  
Classification Code C=101

Driver\*  
libiaconvim.so.1

Arguments  
FORMAT  
1 <WorkDirectory>/iarc/work/conversion<WorkDirectory>

Filter disposition  
Include

Filter content types  
Content types

Press ENTER or TAB to add item

Identifier c3287e71-068a-4ec5-9277-985303f810de

Output

Content type  
image/tiff

Description expression

Options  
 Queue for FTI  Replace source  Standalone

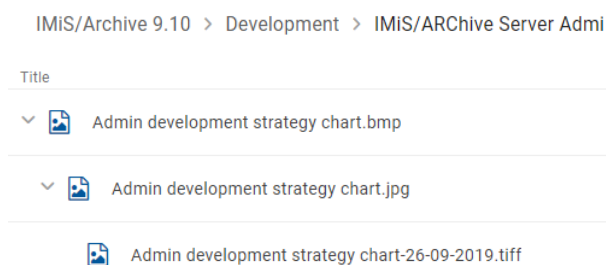
Next converter

REMOVE

SAVE CANCEL

Slika 107: Pretvorba iz JPG v TIFF: nastavitve osnovnih lastnosti in izhodnih parametrov

Prikaz rezultata vezane pretvorbe v spletnem odjemalcu IMiS®/wClient je naslednji:



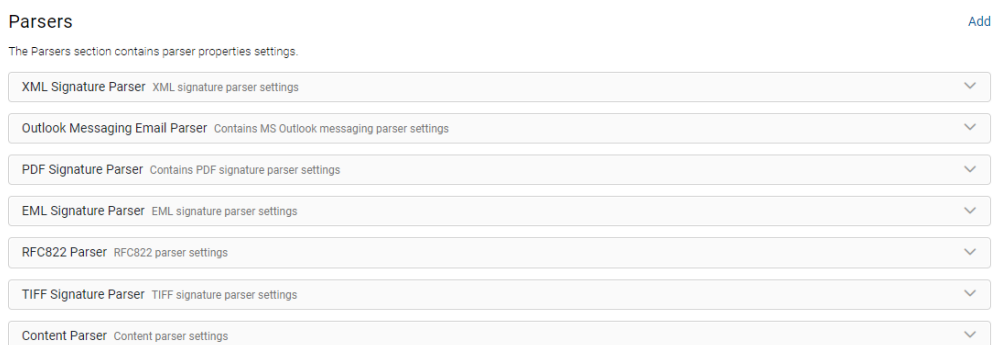
Slika 108: Primer pretvorbe iz formata BMP v JPG in JPG v TIFF

### 8.5.3.5.5 Razčlenjevalniki

Razdelek »Razčlenjevalniki« (angl. Parsers) vsebuje nastavitve lastnosti razčlenjevalnikov.

IMiS®/ARChive Server jih uporablja za:

- Izdvajanje besedila iz hranjenih vsebin različnih tipov, ki jih vrača podsistemu za indeksiranje po besedilu vsebin.
- Zajem in preverjanje veljavnosti elektronskih podpisov vsebin različnih tipov, če ti obstajajo. Elektronske podpise in pripadajoča digitalna potrdila razčlenjevalniki vračajo strežniku IMiS®/ARChive Server v hrambo, ki je ločena od vsebin in jo lahko strežnik uporablja v algoritmih strategije zagotavljanja avtentičnosti.



Slika 109: Prikaz razdelka »Razčlenjevalniki« v mapi »Vsebine«

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi naslednje nastavitve vrednosti:

- »Naziv« (angl. Name): naziv razčlenjevalnika.
- »Opis« (angl. Description): opis razčlenjevalnika.
- »Identifikator razčlenjevalnika« (angl. Provider identifier): določa unikatni naziv razčlenjevalnika.
- »Gonilnik ponudnika« (angl. Provider Driver): gonilnik za razčlenjevanje vsebin.
- »Argumenti ponudnika« (angl. Provider Arguments): določa nastavitvene parametre gonilnika za razčlenjevanje vsebin.
- »Tip filtra« (angl. Filter disposition): določa ali so vrste vsebin vključene v razčlenjevanje ali ne. Vrednost nastavljena na »Vključi« (angl. Include) označuje, da so vrste vsebin vključene. Nasprotno, s spremembo vrednosti v »Izključi« (angl. Exclude) prijavljeni uporabnik izključi vrste vsebin.
- »Vrste vsebin« (angl. Filter content types): vrsta vsebine, na kateri se izvaja razčlenjevanje.
- »Identifikator« (angl. Identifier): unikatni identifikator razčlenjevalnika.

Slika 110: Nastavitev parametrov v razdelku »Razčlenjevalniki«

Po shranitvi (angl. Save) je razčlenjevalnik prijavljenemu uporabniku na voljo v razdelku »Razčlenjevalniki« (angl. Parsers) v osnovnem pregledu nastavitve mape »Vsebine«.

Prijavljeni uporabnik spreminja nastavitve v načinu za urejanje (angl. Edit).

Razčlenjevalnik odstrani z dejanjem »Odstrani razčlenjevalnik« (angl. Delete this parser).

### 8.5.3.5.6 Vrste vsebin

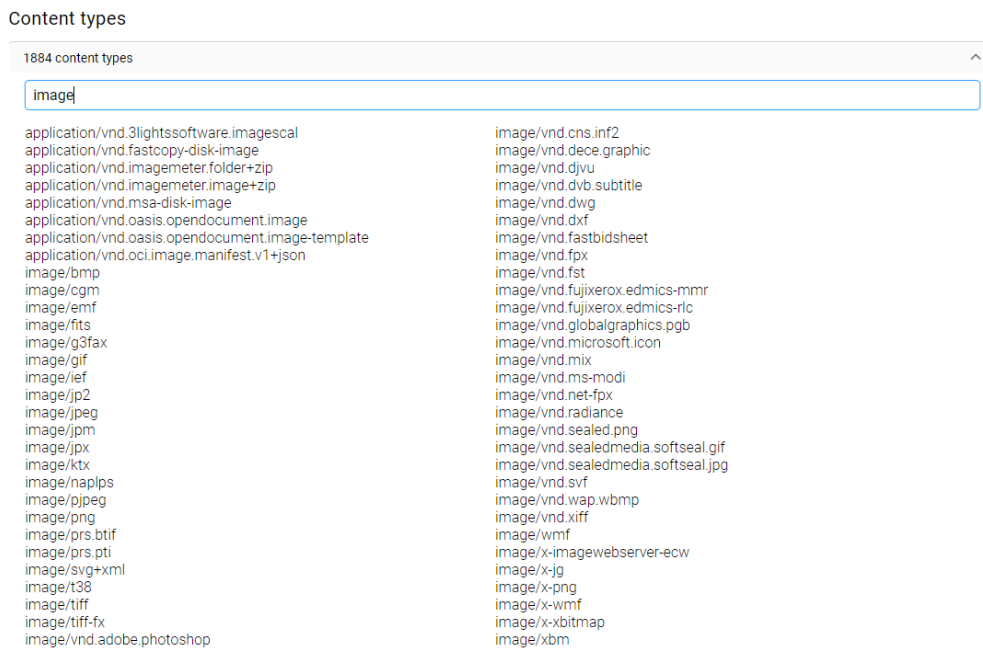
Razdelek »Vrste vsebin« (angl. Content types) vsebuje seznam podprtih MIME vrst vsebin na strežniku.

#### Content types

The Content types section contains a list of supported MIME content types on the server.

Slika 111: Prikaz razdelka »Vrste vsebin« v mapi »Vsebine«

Prijavljenemu uporabniku je omogočeno pregledovanje vrst vsebin in iskanje po seznamu.



Slika 112: Iskanje po seznamu podprtih MIME vrst vsebin

### 8.5.3.6 Mapa Imenik

Mapa »Imenik« (angl. Directory) vsebuje seznam uporabnikov strežnika.

V osnovnem pregledu se poleg iskalnika nahaja tudi seznam imeniških entitet z naslednjimi podatki:

- »Naziv uporabnika« (angl. Name): ime uporabnika ali skupine.
- »Elektronska pošta« (angl. Email): naslov elektronske pošte.
- »Imenik« (angl. Directory): naziv imenika.

Za lažje iskanje imeniških entitet v seznamu je prijavljenemu uporabniku na voljo iskalnik. Z vpisom znakov iskalnega niza, se ustrezno zoži nabor prikazanih rezultatov iskanja v seznamu.

Directory

Search

Slika 113: Iskalno polje za vpis iskalnega niza

Uporabnik ima možnost razvrščanja imeniških entitet v naslednje skupine:

- »Omogočeno« (angl. Enabled)
- »Onemogočeno« (angl. Disabled)
- »Zaklenjeno« (angl. Locked)
- »Brisano« (angl. Deleted)
- »Vsi« (angl. All).

Z izbiro pojavnega menija na označeni entiteti imenika lahko prijavljeni uporabnik izbere eno od naslednjih dejanj:

- »Onemogoči« (angl. Disable)
- »Zakleni« (angl. Lock)
- »Kopiraj«
- »Briši« (angl. Delete).

#### Directory

Search		
<span>Enabled</span> <span>Disabled</span> <span>Locked</span> <span>Deleted</span> <span>All</span> <span>Add</span>		
Name	Email	Directory
3KDCDevelopment (3KDCDevelopment)		ImagingSystemsAD
Ada Zerko (ada)	ada.zerko@imis.si	ImagingSystemsAD
Administrator (admin)	admin@acme.com	
Ales Vukman (ales)	ales.vukman@imis.si	ImagingSystemsAD
Alex Nelson (anelson)	alex.nelson@acme.com	
Anonymous (Anonymous)	anonymous@acme.com	
Benjamin Dobravec (benjamin)	benjamin.dobravec@imis.si	ImagingSystemsAD
Bine Zerko (bine)	bine.zerko@imis.si	ImagingSystemsAD

- Disable
- Lock
- Copy
- Delete

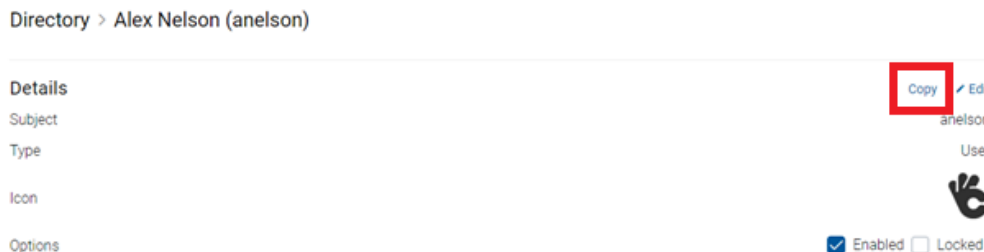
Slika 114: Prikaz osnovnega pregleda mape »Imenik«

#### 8.5.3.6.1 Entiteta imenika

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi nastavitve entitete imenika v naslednjih razdelkih:

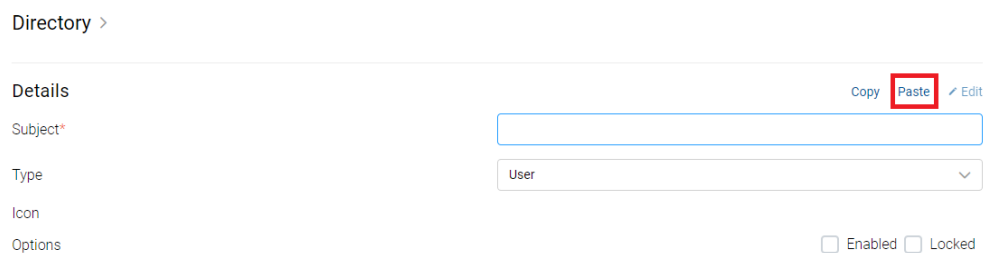
- »Osnovne nastavitve« (angl. Details)
- »Avtentikacija« (angl. Authentication)
- »Imenik« (angl. Directory).

Z izbiro entitete imenika v seznamu ima uporabnik možnost urejanja (angl. Edit) in kopiranja podatkov. Z izbiro dejanja »Kopiraj« (angl. Copy) se podatki entitete imenika prenesejo v odložišče (angl. Clipboard).



Slika 115: Kopiranje entitete imenika

Pri ustvarjanju nove entitete imenika (angl. Add) lahko prijavljeni uporabnik v načinu za urejanje podatke o predhodno shranjeni entiteti imenika »Prilepi« (angl. Paste) iz odložišča in s tem prihrani čas vnosa entitet imenika v seznam.



Slika 116: Dodajanje podatkov o entiteti imenika iz odložišča

### Osnovne nastavitve

V razdelku »Osnovne nastavitve« (angl. Details) lahko prijavljeni uporabnik določi uporabniku ali skupini naslednje parametre:

- »Oznaka uporabnika« (angl. Subject): vsebuje enolično oznako uporabnika ali skupine, oziroma njeno ime, ki je neobčutljivo na velikost znakov. S tem imenom (in izbranim geslom) uporabnik dostopa do strežnika. Vrednost polja je potrebno obvezno določiti pri novih vnosih. Na obstoječih vnosih je ni mogoče spreminjati.
- »Vrsta« (angl. Type): vsebuje vrsto uporabnika. Prijavljeni uporabnik lahko izbira med uporabnikom (angl. User) ali skupino (angl. Group). Vrednost polja je potrebno pri novih vnosih obvezno določiti. Na obstoječih vnosih je ni mogoče spreminjati.


- »Ikona« (angl. Icon): slika uporabnika ali skupine uporabnikov.  
Z izbiro dejanja »Naloži datoteko« (angl. Upload) lahko prijavljeni uporabnik doda ali spremeni ikono. Odstrani jo z dejanjem »Odstrani« (angl. Remove).
- »Možnosti« (angl. Options): omogoča izbiro dodatnih parametrov imeniške entitete:
  - »Omogočena sinhronizacija« (angl. Enabled): označen parameter pomeni, da je prijavljenemu uporabniku omogočen dostop do strežnika. Z odznačitvijo je dostop do strežnika onemogočen.
  - »Zaklenjeno« (angl. Locked): odznačen parameter pomeni, da uporabnik ni zaklenjen in lahko dostopa do arhiva glede na pravice. Nasprotno, z označitvijo nima dostopa do strežnika IMiS®/ARChive Server. Vrednost lahko prijavljeni uporabnik spreminja za lokalne uporabnike ali ne-sinhronizirane uporabnike (Synchronization enabled = False). Parameter je na voljo samo za entiteto imenika »Uporabnik« (angl. User).

*Opozorilo: Po zaklenitvi lahko prijavljeni uporabnik dostopa do entitet in izvaja akcije še do konca veljavnosti njegove seje. Ponovna prijava v strežnik in vzpostavitev seje do spremembe nastavitve ni več mogoča.*

- »Ime« (angl. First name): vsebuje ime uporabnika ali prvo ime skupine.
- »Priimek« (angl. Last name): vsebuje priimek uporabnika ali drugo ime skupine.  
Vrednost polja mora biti pri novih vnosih obvezno določena. Na obstoječih vnosih se lahko spreminja, vendar prazna vrednost ni dovoljena.
- »Opis« (angl. Description): lahko vsebuje opis pozicije uporabnika v podjetju.
- »Elektronska pošta« (angl. Email): vsebuje naslov elektronske pošte uporabnika.
- »Pregled pravic« (angl. View roles): prikaže se seznam vlog in dostopnih pravic za administracijske mape za izbranega uporabnika/skupino.  
Za več informacij glej poglavje [Pregled pravic](#).
- »Pregled efektivnih pravic« (angl. View Effective Roles): prikaže se seznam efektivnih vlog in dostopnih pravic za administracijske mape za izbranega uporabnika/skupino.  
Za več informacij glej poglavje [Pregled efektivnih pravic](#).
- »Sinonim« (angl. Aliases): vsebuje alternativna uporabniška imena za uporabnika, s katerimi lahko uporabnik dostopa do arhiva.
- »Stopnja tajnosti uporabnika« (angl. Security class level): določa do katerega nivoja tajnosti lahko uporabnik pregleduje gradivo. Pregleduje lahko samo tisto gradivo, ki ima določeno nižjo ali enako stopnjo tajnosti od njegove.



- »Pooblaščenci« (angl. Delegates): registrirani uporabniki, ki se v postopku prijave lahko predstavijo kot pooblašcene osebe za druge uporabnike in v njihovem imenu izvajajo operacije. Prijavljeni uporabnik lahko dodaja pooblašcence z vpisom oznake uporabnika (angl. Subject). Nastavitev parametra je na voljo samo za entitete imenika »Uporabnik« (angl. User).
- »Članstvo v skupinah« (angl. Member of groups): seznam skupin, v katerih je določen uporabnik član.
- »Datum spremembe« (angl. Modified): datum in čas zadnje spremembe imeniške entitete ter uporabnik, ki je spremembo izvedel.
- »Datum ustvarjanja« (angl. Created): datum in čas ustvarjanja imeniške entitete ter uporabnik, ki jo je ustvaril.

<b>Details</b>	Copy Paste Delete Edit
Subject	anelson
Type	User
Icon	 Upload Remove
Options	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Locked
First name	<input type="text" value="Alex"/>
Last name*	<input type="text" value="Nelson"/>
Description	<input type="text" value="Sales - Controlling"/>
Email	<input type="text" value="alex.nelson@acme.com"/>
<a href="#">View roles</a>	▼
Aliases	<input type="text" value="Aliases"/>
Security class level	<input type="text" value="Top Secret"/> ▼
Delegates	<input type="text" value="Keira Clay"/> -
	<input type="text" value="Marko Hren"/> -
	<input type="text" value="Benjamin Dobravec"/> +
Member of groups	<span>Everyone (sys:Everyone)</span>
Modified	5. Sep 2022, 07:23 by admin
Created	1. Jan 0001, 01:22 by sys:Administrator

Slika 117: Prikaz osnovnega pregleda v mapi »Osnovne nastavitve«

## Avtentikacija

»Avtentikacija« (angl. Authentication) omogoča preverjanja pristnosti uporabnika (angl. User) pri prijavi v strežnik. Prijavljeni uporabnik lahko izbira med naslednjimi nastavitvami:

- »Možnosti« (angl. Options): omogoča izbiro dodatnih parametrov avtentikacije:
  - »Napredna avtentikacija« (angl. Advanced): omogoča uporabo zapletenejših (HMAC) metod vzpostavitve seje s strežnikom, ki predvideva obvezne in neobvezne metapodatke o odjemalcu.
  - »Lokalna avtentikacija« (angl. Local): omogoča lokalno prijavo uporabnika v strežnik z uporabo uporabniškega imena in gesla.
  - »Avtentikacija z uporabo deljenega ključa« (angl. Pre-shared key): omogoča prijavo uporabnika v strežnik z deljenim ključem. Med postopkom prijave se ugotavlja identiteta uporabnika na osnovi zaupnega ključa, ki si ga delita odjemalec in strežnik.
  - »Zunanja avtentikacija« (angl. External): omogoča prijavo zunanjih uporabnikov preko zunanjega imenika.
  - »Lokalna avtentikacija preko HTTP« (angl. Local over HTTP): omogoča prijavo uporabnika v konfiguracijo strežnika preko HTTP protokola.
- »Spremeni geslo« (angl. Change password): prikaže se pogovorno okno za vpis novega ali spremembo obstoječega gesla. Za več informacij glej poglavje [Geslo](#).

Authentication

Options

Advanced  External

Local  Local over HTTP

Pre-shared key

Change password

Slika 118: Nastavitve parametrov v razdelku »Avtentikacija«

## Imenik

»Imenik« (angl. Directory): določa parametre za dostop entitet imenika do strežnika.

Prijavljeni uporabnik lahko določi naslednje parametre:

- »Identifikator zunanjega imenika« (angl. Identifier): identifikator (naziv) zunanjega imenika v primeru omogočene sinhronizacije.
- »Omogočena sinhronizacija« (angl. Synchronization enabled): označitev parametra pomeni, da so podatki o entiteti imenika sinhronizirani z zunanjim imenikom. Nasprotno, odznačitev onemogoči sinhronizacijo uporabnika z zunanjim imenikom.
- »Preverjanje ujemanja UUID« (angl. Ignore UUID Check): odznačen parameter pomeni, da se preverjanje UUID ne izvede. Nasprotno, z označitvijo parametra se izvede sinhronizacija posamezne entitete imenika kljub temu, da se UUID vrednosti ne ujemajo. Pri tem se prvotni UUID, ki je bil ustvarjen ob prvi sinhronizaciji z LDAP strežnikom, prepíše z novim UUID, ki je bil pridobljen skozi proces sinhronizacije. Parameter se uporablja samo pri uporabnikih ali skupinah, ki so del sinhronizacije, nastavljanje parametra na lokalnih entitetah povzroči napako.

*Opomba:* Razdelek »Imenik« (angl. Directory) se ne prikaže pri dodajanju nove entitete imenika.



Slika 119: Nastavitev parametrov v razdelku »Imenik«

Prijavljeni uporabnik shrani imeniško entiteto z dejanjem »Shrani« (angl. Save).

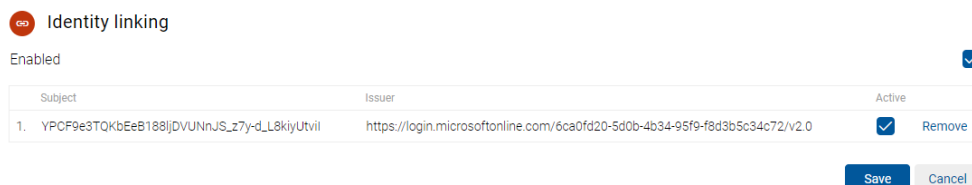
Po shranitvi lahko entiteto imenika odstrani z dejanjem »Odstrani entiteto imenika« (angl.

Delete this directory entity).

### Povezovanje identitet

V razdelku »Povezovanje identitet« (angl. Identity linking) prijavljeni uporabnik z označitvijo parametra »Omogočeno« (angl. Enabled) uporabniku omogoči vzpostavitev povezave z identiteto pri zunanjem ponudniku. Nasprotno, z odznačitvijo je ta povezava onemogočena.

V seznamu so prikazane zunanje identitete, katerim lahko prijavljeni uporabnik spremeni status (aktivna/neaktivna - angl. Active) ali pa posamezno zunanjo identiteto odstrani (angl. Remove).



Slika 120: Nastavitev parametrov v razdelku »Zunanje identitete«

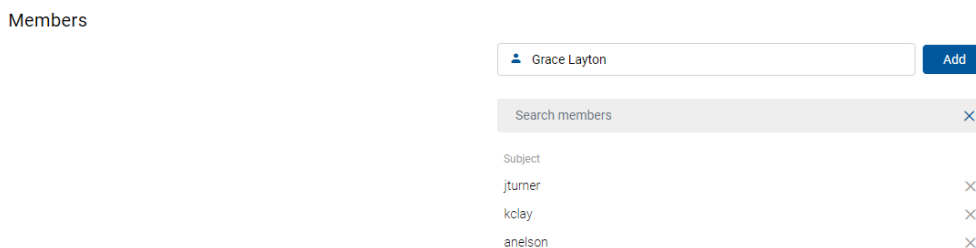
### Članstvo v skupinah

Razdelek »Članstvo« (angl. Members) se prikaže samo v primeru entitete imenika »Skupina uporabnikov« (angl. Member of groups).

V načinu za urejanje (angl. Edit) se prijavljenemu uporabniku z vpisom vsaj dveh znakov iskalnega niza v polje »Nov član« (angl. New member) prikaže nabor razpoložljivih entitet imenika.

Z izbiro in potrditvijo ustrezne z dejanjem »Dodaj« (angl. Add) se član doda v skupino.

Z vpisom vsaj enega znaka iskalnega niza v polje »Izberi člane« (angl. Search members) se prikaže nabor razpoložljivih entitet imenika.



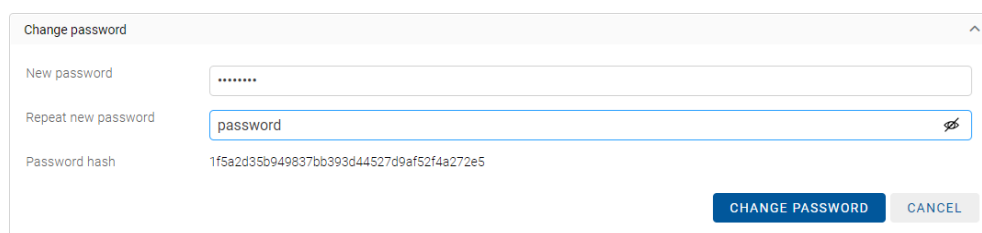
Slika 121: Dodajanje člana v skupino

Spremembe entitet imenika se upoštevajo takoj po potrditvi izbire.

### 8.5.3.6.2 Geslo

Po shranitvi novega uporabnika/skupine se prijavljenemu uporabniku odpre nov razdelek »Spremeni geslo« (angl. Change password), kjer lahko z vpisom naslednjih parametrov doda ali spremeni geslo za izbranega uporabnika:

- »Novo geslo« (angl. New password): določi novo geslo.
- »Ponovi vpis gesla« (angl. Repeat new password): ponovno vpiše zgoraj določeno geslo.
- »Prstni odtis gesla« (angl. Password hash): vsebuje 40-znakovni prstni odtis (angl. hash) gesla uporabnika, v kolikor ga je prijavljeni uporabnik že določil.



Change password

New password: .....

Repeat new password: password

Password hash: 1f5a2d35b949837bb393d44527d9af52f4a272e5

CHANGE PASSWORD CANCEL

Slika 122: Sprememba gesla

*Opomba:* S spremembo gesla in izbiro ukaza »Spremeni geslo« (angl. Change password) se polji za vpis gesla zaradi varnosti pobrišeta. Obenem se spremeni tudi prstni odtis gesla.

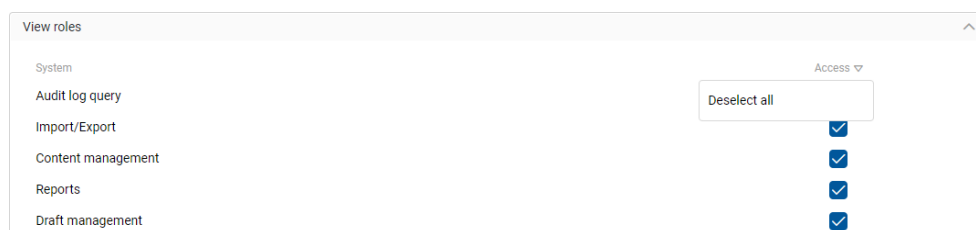
### 8.5.3.6.3 Pregled pravic

V sklopu »Pregled pravic« (angl. View roles) prijavljeni uporabnik za izbranega uporabnika določi:

- »Sistemske vloge«, ki uporabniku omogočajo izvajanje določenih operacij na strežniku.
- »Konfiguracijske vloge«, ki uporabniku omogočajo pravice branja in spreminjanja vrednosti v konfiguracijskih mapah.

V razdelku »Sistemske vloge« (angl. System) z označitvijo parametra uporabnikom ali skupinam omogoči naslednje sistemske vloge:

- »Revizijska sled« (angl. Audit log query): pridobivanje revizijske sledi.
- »Uvoz / Izvoz« (angl. Import / Export): uvoz in izvoz gradiva.
- »Upravljanje z vsebinami« (angl. Content management): izvajanje zahtev za indeksiranje in samodejno pretvorbo vsebine.
- »Poročila« (angl. Reports): prikaz in tiskanje sistemskih poročil o zadevah, dokumentih, vsebini dokumentov, hrambi, pregledih, dostopih, entitetah, razredih (in zadevah) načrta razvrščanja gradiva, brisanih entitetah in entitetah za izbris.
- »Upravljanje z različicami dokumenta« (angl. Draft management):
  - zavrženje osnutka dokumenta (angl. Discard), v kolikor ima uporabnik pravico brisanja (angl. Delete) ali vlogo »Upravljanje z različicami dokumenta«;
  - objavo osnutka dokumenta (angl. Check in), v kolikor ima uporabnik pravico urejanja (angl. Edit) in vlogo »Upravljanje z različicami dokumenta«, ali pa je naveden kot lastnik osnutka dokumenta;
  - vsa ostala dejanja v smislu vidljivostjo osnutka dokumenta.



Slika 123: Nastavitev parametrov v razdelku »Sistemske vloge«

Z izbiro puščice ob nazivu stolpca za nastavitev sistemskih vlog (angl. Access) se uporabniku prikaže dejanje »Izberi vse« (angl. Select all), oziroma »Počisti izbiro« (angl. Deselect all).

S tem je prijavljenemu uporabniku omogočena izbira vseh parametrov naenkrat.

***Opomba:** Prikaz različice dokumenta, ki jo je ustvaril drug uporabnik je odvisen od dostopnih pravic uporabnika do dokumenta.*

***Opozorilo:** Po spremembi vloge uporabnika veljajo trenutne vloge še do konca veljavnosti njegove seje ali ponovne prijave v arhiv.*

V razdelku »Konfiguracija« (angl. Configuration) prijavljeni uporabnik nastavi eksplicitne pravice za branje (angl. Read) in urejanje (angl. Edit) naslednjih parametrov:

- »Avtentikacija« (angl. AAA settings; AAA= Authentication, Authorization, Accounting)
- »Nadzor dostopov« (angl. Access control)
- »Nastavitve arhiva« (angl. Archive settings)
- »Atributi« (angl. Attributes)
- »Nastavitve revizijske sledi« (angl. Audit log settings)
- »Šifranti« (angl. Codelists)
- »Nastavitve vsebine« (angl. Content settings)
- »Številčenje« (angl. Counters)
- Entiteta imenika [uporabnik]« (angl. Directory entry)
- »Entiteta imenika [skupina]« (angl. Directory group)
- »Nestrukturirana hramba« (angl. Object staging)
- »Nastavitve LTANS« (angl. LTANS)
- »Profili« (angl. Profiles)
- »Hramba« (angl. Retention)
- »Varnostne nastavitve« (angl. Security settings)
- »Predloge« (angl. Templates)
- »Volumni« (angl. Volumes).

Configuration	Read ▾	Update ▾
AAA settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Access control	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Archive settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Attributes	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Audit log settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Codelists	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Content settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Counters	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Directory entity	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Directory group	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Object staging	<input checked="" type="checkbox"/>	<input type="checkbox"/>
LTANS settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Profiles	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Retention	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Security settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Templates	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Volumes	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Slika 124: Nastavitve parametrov v razdelku »Konfiguracijske vloge«

Z izbiro puščice ob nazivu stolpca za nastavitve eksplicitnih pravic za branje (angl. Read) in urejanje (angl. Edit) se prijavljenemu uporabniku prikaže dejanje »Izberi vse« (angl. Select all), oziroma »Počisti izbiro« (angl. Deselect all). S tem je omogočena izbira vseh parametrov naenkrat.

#### 8.5.3.6.4 Pregled efektivnih pravic

V sklopu »Pregled efektivnih vlog« (angl. View effective roles) se prijavljenemu uporabniku prikažejo efektivne vloge in pravice za konfiguriranje strežnika za uporabnika ali skupino. Prikaz je informativne narave, zato vlog in pravic v tem razdelku ni mogoče spreminjati.

View effective roles		Access
System		
Audit log query		☑
Import/Export		☑
Content management		☑
Reports		☑
Draft management		☑
Configuration	Read	Update
AAA settings	☑	
Access control	☑	
Archive settings	☑	
Attributes	☑	
Audit log settings	☑	
Codelists	☑	
Content settings	☑	
Counters	☑	
Directory entity	☑	
Directory group	☑	
Legacy archival	☑	
LTANS settings	☑	
Profiles	☑	
Retention	☑	
Security settings	☑	
Templates	☑	
Volumes	☑	

Slika 125: Pregled efektivnih pravic za izbranega uporabnika



### 8.5.3.7 Mapa Nestrukturirana hramba

Mapa »Nestrukturirana hramba« (angl. Object staging) vsebuje naslednje razdelke:

- »Shranjevalni profili« (angl. Storage profiles).
- »Vsebniki objektov« (angl. Object containers).
- »Sinonimi vrst vsebin« (angl. Content type aliases).

#### Object staging

The screenshot displays the 'Object staging' interface with three main sections, each with an 'Edit' and 'Add' link:

- Storage profiles**: Contains two entries: 'Dokumenti' and 'NLBLG', both with a green checkmark and a dropdown arrow.
- Object containers**: Contains two entries: 'Custom Document' and 'sys:LegacyObject', both with a green checkmark and a dropdown arrow.
- Content type aliases**: Contains seven entries, each with a dropdown arrow:
  - application/vnd.openxmlformats-officedocument.presentationml.presentation
  - application/vnd.openxmlformats-officedocument.presentationml.slideshow
  - application/vnd.openxmlformats-officedocument.presentationml.template
  - application/vnd.openxmlformats-officedocument.spreadsheetml.sheet
  - application/vnd.openxmlformats-officedocument.spreadsheetml.template
  - application/vnd.openxmlformats-officedocument.wordprocessingml.document
  - application/vnd.openxmlformats-officedocument.wordprocessingml.template

Slika 126: Prikaz osnovnega pregleda v mapi »Nestrukturirana hramba«

#### Shranjevalni profili

Razdelek »Shranjevalni profili« (angl. Storage profiles) vsebuje nastavitve profilov za shranjevanje vsebin preko odjemalcev za nestrukturirano arhiviranje na strežnik IMiS®/ARChive Server.

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi naslednje nastavitve:

- »Profil« (angl. Profile): določa profil za shranjevanje vsebin preko odjemalcev za nestrukturirano arhiviranje.
- »Vsebnik« (angl. Container): določa entiteto (razred, zadeva) pod katero se shranjujejo vsebine preko protokola nestrukturiranega arhiviranja. Prijavljeni uporabnik lahko pregleduje in/ali spreminja naslednje nastavitve:
  - »Vrsta« (angl. Type): določa vrsto identifikatorja entitete (interni, zunanji ali klasifikacijska oznaka);
  - »Vrednost« (angl. Value): določa vrednost identifikatorja entitete.  
Nastavljena vrednost označuje, da se bo vsebina odjemalcev za nestrukturirano arhiviranje shranjevala pod to entiteto.
- »Predloga« (angl. Template): določa vrsto predloge entitet, ki se uporabijo pri shranjevanju vsebin odjemalcev za nestrukturirano arhiviranje.
- »Status« (angl. Status): določa privzet status entitete po shranjevanju vsebin odjemalcev za nestrukturirano arhiviranje. Status »Odprto« (angl. Opened) pomeni, da po shranjevanju ostane entiteta odprta, pri »Zaprto« (angl. Closed) pa se entiteta po shranjevanju zapre.
- »Naziv« (angl. Title): določa privzet naziv entitete pri shranjevanju posamezne vsebine odjemalcev za nestrukturirano arhiviranje.
- »Opis« (angl. Description): določa privzet opis entitete pri shranjevanju posamezne vsebine odjemalcev za nestrukturirano arhiviranje.
- »Opis vsebine« (angl. Object description): določa privzet opis vsebine pri shranjevanju posamezne vsebine (datoteka) odjemalcev za nestrukturirano arhiviranje.
- »Onemogočen« (angl. Disabled): označen parametra določa, da je dostop do shranjevalnega profila onemogočen.
- »Vrni identifikator vsebine« (angl. Return content identifier): označen parametra določa, da se bo v aplikacijo, ki dostopa do podatkov in vsebin shranjenih na strežniku IMiS®/ARChive Server vračal identifikator vsebine. Nasprotno, z odznačitvijo prijavljeni uporabnik določi, da se bo v aplikacijo vračal identifikator entitete.
- »Uporabniki« (angl. Browsers): imeniške entitete, ki lahko dostopajo do shranjevalnih profilov. Z izbiro ikone » + «, prijavljeni uporabnik doda imeniško entiteto tipa uporabnik/skupina, z » - «, pa jo odstrani. Za več informacij o imeniških entitetah glej poglavje [Mapa Imenik](#).

Storage profiles Add

● Dokumenti

Profile: Dokumenti

Container: Classification code

Template:

Status:

Title:

Description:

Object description:

Disabled:  No

Return content identifier:

Browsers:  +

[Delete this storage profile](#)

Slika 127: Nastavitev parametrov v razdelku »Shranjevalni profili«

Po shranitvi (angl. Save) je shranjevalni profil prijavljenemu uporabniku na voljo v razdelku »Shranjevalni profili« (angl. Storage profiles) v osnovnem pregledu nastavitve mape »Nestrukturirano arhiviranje«.

Storage profiles Edit Add

● DZ-AV

● DZ-JAVNO

Slika 128: Prikaz shranjevalnega profila

Prijavljeni uporabnik ureja nastavitve z izbiro načina za urejanje (angl. Edit).

Shranjevalni profil odstrani z dejanjem »Odstrani shranjevalni profil« (angl. Delete this storage profile).

## Vsebniki objektov

Razdelek »Vsebniki objektov« (angl. Object containers) vsebuje nastavitve za shranjevanje datotek iz odjemalcev za nestrukturirano arhiviranje na strežnik IMiS®/ARChive Server.

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi naslednje nastavitve:

- »Predloga« (angl. Template): določa predlogo za ustvarjanje entitete (dokumenta), ki vsebuje attribute vrste »File«.
- »Atribut« (angl. Attribute): določa atribut vrste »File«, kamor se shranjuje datoteka preko odjemalca za nestrukturirano arhiviranje.
- »Onemogočen« (angl. Disabled): označen parameter določa, ali je vsebnik objektov onemogočen.

The screenshot shows a configuration window titled 'Object containers' with an 'Add' button in the top right. The window contains a list of containers, with 'Custom Document' selected. Below the list, there are three configuration fields: 'Template' set to 'Custom document (Custom Document)', 'Attribute' set to 'Custom Content (CustomContent)', and 'Disabled' set to 'No' with a green checkmark. A 'Delete this object container' link is visible below the 'Disabled' field. At the bottom right, there are 'SAVE' and 'CANCEL' buttons.

Slika 129: Nastavitev parametrov v razdelku »Vsebniki objektov«

Vsebnik objektov odstrani z dejanjem »Odstrani vsebnik objektov« (angl. Delete this object container).

Po shranitvi (angl. Save) je vsebnik objektov prijavljenemu uporabniku na voljo v razdelku »Vsebniki objektov« (angl. Object containers) v osnovnem pregledu nastavitve mape »Nestrukturirano arhiviranje«.

The screenshot shows a list titled 'Object containers' with 'Edit' and 'Add' buttons in the top right. The list contains one entry: 'Custom Document' with a green checkmark icon and a dropdown arrow on the right.

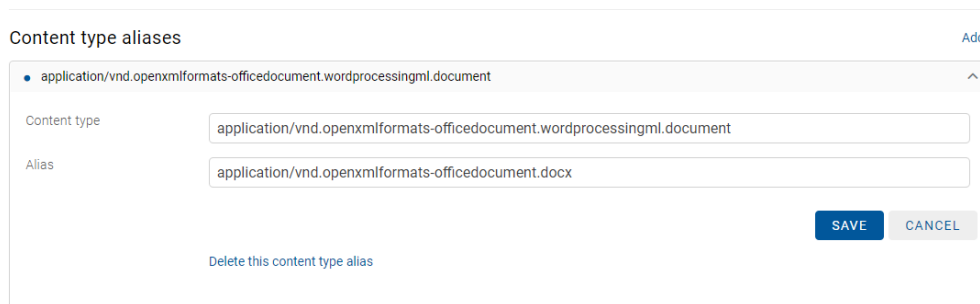
Slika 130: Prikaz vsebnika objektov

## Sinonimi vrst vsebin

Razdelek »Sinonimi vrst vsebin« (angl. Content type aliases) vsebuje nastavitve sinonimov standardnih vrst vsebin, ki se uporabljajo pri dostopu do enakih vsebin preko vmesnika za nestrukturirano arhiviranje na strežnikih IMiS®/ARChive Server. Protokol nestrukturirane hrambe (Legacy API) ima omejeno velikost naziva vrste vsebin (63 znakov), preko katerega ni možno izmenjevati vsebin, katerih vrste presegajo dolžino 63 znakov (npr. MS Office Open formati). Za več informacij glej poglavje [Mapa Vrste vsebin](#).

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljenemu uporabniku določi naslednje nastavitve:

- »Vrsta vsebine« (angl. Content type): določa standardno vrsto vsebine predpisano s strani združenja IANA.
- »Sinonim« (angl. Alias): določa sinonim za standardno vrsto vsebine pri dostopu do enakih vsebin preko protokola za nestrukturirano arhiviranje.



Content type aliases Add

- application/vnd.openxmlformats-officedocument.wordprocessingml.document

Content type:

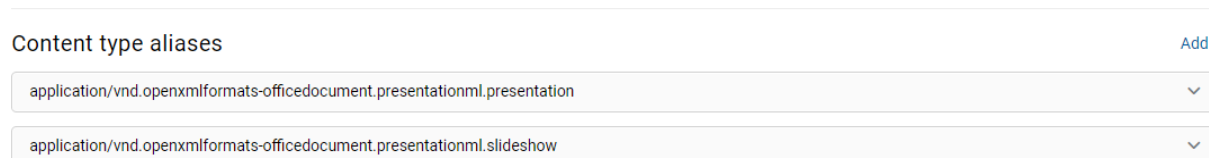
Alias:

[Delete this content type alias](#)

Slika 131: Nastavitev parametrov v razdelku »Sinonimi vrst vsebin«

Vsebnik objektov odstrani z dejanjem »Odstrani sinonim vrste vsebine « (angl. Delete this content type alias).

Po shranitvi (angl. Save) je sinonim vrste vsebin prijavljenemu uporabniku na voljo v razdelku »Sinonimi vrst vsebin« (angl. Content type aliases) v osnovnem pregledu nastavitve mape »Nestrukturirano arhiviranje«.



Content type aliases Add

- application/vnd.openxmlformats-officedocument.presentationml.presentation
- application/vnd.openxmlformats-officedocument.presentationml.slideshow

Slika 132: Prikaz sinonima vrste vsebine

### 8.5.3.8 Mapa LTANS

LTANS se uporablja za zagotavljanje avtentičnosti hranjenega gradiva preko ustvarjanja in dolgoročnega vzdrževanja dokaznih elementov o nespremenljivosti hranjenega gradiva.

Mapa »LTANS« (angl. Long Term Archive and Notary Services - LTANS) vsebuje nastavitve razvrščene v naslednje razdelke:

- »Osnovne nastavitve« (angl. Details)
- »Ponudniki časovnega žigosanja« (angl. Timestamp providers)
- »Pravila časovnega žigosanja« (angl. Timestamping rules)
- »Pravila veriženja časovnih žigov« (angl. Timestamp chaining rules).

LTANS

---

**Details** [Edit](#)

Enabled ✔ Yes

Minimum batch size 1

Maximum batch size 256

Timestamping schedule 0\*/10\*\*\*\*

Timestamp chaining schedule 003\*\*\*

---

**Timestamp providers** [Edit](#) [Add](#)

The Timestamp providers section contains the settings for timestamp providers.

SI-TSA\_SHA256\_RFC3161 ▼

SYMANTEC SHA-256 RFC3161 ▼

---

**Timestamping rules** [Edit](#) [Add](#)

The Timestamping rules section contains the settings for the timestamping rules.

✔ SI-TSA\_SHA256\_RFC3161 ▼

✔ SYMANTEC RFC3161 ▼

---

**Timestamp chaining rules** [Edit](#) [Add](#)

The timestamp chaining rules section contains the settings for the timestamp chaining rule. It specifies the schedule for the execution of timestamping of the digital certificate chains.

✔ SYMANTEC RFC3161 ▼

Slika 133: Prikaz osnovnega pregleda v mapi »LTANS«

## Osnovne nastavitve

V razdelku »Osnovne nastavitve« (angl. Details) prijavljeni uporabnik ureja (angl. Edit) naslednje LTANS nastavitve:

- »Omogočeno« (angl. Enabled): označitev parametra pomeni, da je omogočeno zagotavljanje avtentičnosti hranjenega gradiva. Z odznačitvijo prijavljeni uporabnik onemogoči zagotavljanje avtentičnosti hranjenega gradiva.
- »Najmanjša velikost paketa« (angl. Minimum batch size): določa najmanjšo število arhivskih informacijskih paketov (AIP), ki se časovno žigosajo z enim časovnim žigom. Vrednost ne sme biti manjša od 1 ali večja od največje velikosti paketa.
- »Največja velikost paketa« (angl. Maximum batch size): določa največje število arhivskih informacijskih paketov (AIP), ki se časovno žigosajo z enim časovnim žigom. Vrednost ne sme biti večja od 1.000.000 ali manjša od najmanjše velikosti paketa.
- »Urn timer časovnega žigosanja« (angl. Timestamping schedule): določa urnik izvajanja časovnega žigosanja. Privzeta vrednost je 0 0 \* \* \* \* \*.
- »Urn timer veriženja časovnih žigov« (angl. Timestamping chaining schedule): določa urnik izvajanja časovnega žigosanja digitalnih potrdil v verigi. Nastavljena vrednost na strežniku je 0 0 5 \* \* \* \* \*.

Details	
Enabled	<input checked="" type="checkbox"/>
Minimum batch size	<input type="text" value="1"/>
Maximum batch size	<input type="text" value="256"/>
Timestamping schedule	<input type="text" value="0*/10****"/>
Timestamp chaining schedule	<input type="text" value="0 0 5****"/>

Slika 134: Nastavitev parametrov v razdelku »Nastavitve«

## Ponudniki časovnega žigosanja

Razdelek »Ponudniki časovnega žigosanja« (angl. Timestamp providers) določa podatke o nazivu in vrsti ponudnika časovnega žigosanja.

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi naslednje nastavitve:

- »Naziv« (angl. Name): naziv ponudnika časovnega žigosanja.
- »Opis« (angl. Description): kratek opis ponudnika časovnega žigosanja.

- »Identifikator ponudnika« (angl. Provider identifier): identifikator ponudnika časovnega žigosanja. Podatek je obvezen.
- »Privzeto« (angl. Default): označitev parametra pomeni, da je ponudnik časovnega žigosanja privzet. Nasprotno, z odznačitvijo prijavljeni uporabnik označi, da ponudnik ni privzet.
- »Zgoščevalni algoritem« (angl. Digest): vrednost določa zgoščevalni algoritem. Prijavljeni uporabnik lahko izbira med naslednjimi vrednostmi: MD5, SHA1, SHA224, SHA256, SHA384 in SHA512.
- »Gonilnik« (angl. Driver): gonilnik ponudnika časovnega žigosanja. Podatek je obvezen.
- »Argumenti« (angl. Arguments): določa nastavitvene parametre gonilnika ponudnika časovnega žigosanja.
- »Identifikator« (angl. Identifier): določa enolični identifikator ponudnika časovnega žigosanja. Ustvari se po shranitvi ponudnika.

Timestamp providers Add

The Timestamp providers section contains the settings for timestamp providers.

SI-TSA\_SHA256\_RFC3161

SYMANTEC SHA-256 RFC3161

Name: SYMANTEC SHA-256

Description: RFC3161

Provider identifier: SYMANTEC RFC3161

Default:

Digest: SHA-256

Driver\*: libiajtsp.so.2

Arguments

```
1 <Class>com.imis.imisarc.server.tsp.impl.RFC3161Provider</Class>
2 <WorkingDirectory>/iarc/work/tsp/</WorkingDirectory>
3 <Service>
4 <Protocol>HTTP</Protocol>
5 <Address>http://sha256timestamp.ws.symantec.com/sha256/timestamp</Address>
6 <Interface>RFC3161</Interface>
7 <AuthType>NONE</AuthType>
8 </Service>
9 <RepeatOnFailure>3</RepeatOnFailure>
```

Identifier: ef15efc2-f6a6-47a7-88ad-c0b116c93c40  
[Delete this timestamp provider](#)

Save Cancel

Slika 135: Nastavitev parametrov v razdelku »Ponudnik časovnega žigosanja«

Ponudnika odstrani z dejanjem »Odstrani ponudnika časovnega žigosanja« (angl. Delete this timestamp provider).



Po shranitvi (angl. Save) je ponudnik časovnega žigovanja prijavljenemu uporabniku na voljo v razdelku »Ponudniki časovnega žigovanja« (angl. Timestamp providers) v osnovnem pregledu nastavitve mape »LTANS«.

### Timestamp providers

[Add](#)

The Timestamp providers section contains the settings for timestamp providers.

SI-TSA\_SHA256\_RFC3161

SYMANTEC SHA-256 RFC3161

Slika 136: Prikaz ponudnika časovnega žigovanja

### Pravila časovnega žigovanja

Razdelek »Pravila časovnega žigovanja« (angl. Timestamping rules) določa nastavitve pravil časovnega žigovanja.

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi naslednje nastavitve:

- »Ponudnik« (angl. Provider): določa podatke o ponudniku časovnega žigovanja.
- »Omogočeno« (angl. Enabled): določa ali je časovno žigovanje omogočeno ali ne. Označitev parametra pomeni, da je časovno žigovanje omogočeno. Z odznačitvijo prijavljeni uporabnik onemogoči časovno žigovanje.
- »Vrsta pravila« (angl. Type): določa vrsto pravila časovnega žigovanja. Eksplicitna pravila se upoštevajo pri odločanju ali se bo na entiteti izvedlo časovno žigovanje. V samem postopku časovnega žigovanja pa se v razširjanju nabora podrejenih entitet dodatno upoštevajo implicitna in eksplicitna pravila.
- »Obseg« (angl. Scope): določa nad katerim delom klasifikacijskega drevesa se upošteva pravilo časovnega žigovanja. Prijavljeni uporabnik lahko določi ali pregleduje naslednje nastavitve:
  - »Vrsta identifikatorja« (angl. Type): določa vrsto identifikatorja entitete (interni, zunanji ali klasifikacijska oznaka);
  - »Vrednost« (angl. Value): določa vrednost identifikatorja entitete. Nastavljena vrednost označuje, da bo pravilo časovnega žigovanja veljalo na entitetah uvrščenih pod izbrano in njej vsebovanimi entitetami. Če vrednost ni določena pomeni, da omejitev ni in da pravilo velja za celoten strežnik.

- »Vključi vsebovane entitete« (angl. Include children): vrednost določa ali pravilo časovnega žigosanja velja tudi na vsebovanih entitetah. Označitev parametra pomeni, da pravilo velja. Z odznačitvijo prijavljeni uporabnik določi, da pravilo časovnega žigosanja ne velja za vsebovane entitete.
- »Filter predloge« (angl. Template filter): omogoča omejevanje nabora entitet po predlogi za katere velja pravilo časovnega žigosanja.
- »Iskalni niz« (angl. Search expression): omogoča omejevanje nabora entitet po iskalnem nizu za katere velja pravilo časovnega žigosanja.
- »Identifikator« (angl. Identifier): določa unikatni identifikator pravila časovnega žigosanja. Ustvari se po shranitvi pravila.

**Timestamping rules** Add

The Timestamping rules section contains the settings for the timestamping rules.

SI-TSA\_SHA256\_RFC3161

Provider\* SI-TSA\_SHA256\_RFC3161

Enabled

Type Explicit

Scope Classification code C-3

Include children

Template filter

Search expression

Identifier 21a2b776-a5bd-4113-a42f-19d00770b829  
[Delete this timestamping rule](#)

Slika 137: Nastavitev parametrov v razdelku »Pravila časovnega žigosanja«

Pravilo odstrani z dejanjem »Odstrani pravilo časovnega žigosanja« (angl. Delete this timestamping rule).

Po shranitvi (angl. Save) je pravilo časovnega žigosanja prijavljenemu uporabniku na voljo v razdelku »Pravila časovnega žigosanja« (angl. Timestamping rules) v osnovnem pregledu nastavitve mape »LTANS«.

#### Timestamp providers

[Add](#)

The Timestamp providers section contains the settings for timestamp providers.

SI-TSA\_SHA256\_RFC3161

SYMANTEC SHA-256 RFC3161

Slika 138: Prikaz pravila časovnega žigosanja

#### Pravila veriženja časovnih žigov

Razdelek »Pravila veriženja časovnih žigov« (angl. Timestamp chaining rules) vsebuje nastavitve pravil veriženja časovnega žigosanja. Določa urnik izvajanja časovnega žigosanja digitalnih potrdil v verigi.

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi naslednje nastavitve:

- »Ponudnik« (angl. Provider): določa podatke o ponudniku časovnega žigosanja.
- »Omogočeno« (angl. Enabled): določa ali je veriženje časovnih žigov omogočeno ali ne. Označitev parametra pomeni, da je veriženje omogočeno. Z odznačitvijo prijavljeni uporabnik onemogoči veriženje časovnih žigov.
- »Zgoščevalni algoritem« (angl. Digest): vrednost določa zgoščevalni algoritem, uporabljen v verigi. Prijavljeni uporabnik lahko izbira med naslednjimi vrednostmi: MD5, SHA1, SHA224, SHA256, SHA384 in SHA512.
- »Pretek časovnega žigosanja« (angl. Expiration): določa časovni okvir v katerem mora biti digitalno potrdilo, ki je izvedlo časovno žigosanje še veljavno, da se časovno žigosanje podaljša.
- »Identifikator« (angl. Identifier): določa unikatni identifikator pravila veriženja časovnih žigov. Ustvari se po shranitvi pravila.

### Timestamp chaining rules

[Edit](#) [Add](#)

The timestamp chaining rules section contains the settings for the timestamp chaining rule. It specifies the schedule for the execution of timestamping of the digital certificate chains.

SYMANTEC RFC3161	
Provider	SYMANTEC SHA-256
Enabled	<input checked="" type="checkbox"/> Yes
Digest	SHA-256
Expiration	30d
Identifier	5f97df7d-48ca-4c6d-85fe-18e6a17413a8

Slika 139: Nastavitev parametrov v razdelku »Pravila veriženja časovnih žigov«

Pravilo odstrani z dejanjem »Odstrani pravila veriženja časovnih žigov« (angl. Delete this timestamp chaining rule).

Po shranitvi (angl. Save) je pravilo veriženja časovnih žigov prijavljenemu uporabniku s pravico na voljo v razdelku »Pravila veriženja časovnih žigov« (angl. Timestamp chaining rules) v osnovnem pregledu nastavitve mape »LTANS«.

### Timestamp chaining rules

[Edit](#) [Add](#)

The timestamp chaining rules section contains the settings for the timestamp chaining rule. It specifies the schedule for the execution of timestamping of the digital certificate chains.

SYMANTEC RFC3161	
------------------	--

Slika 140: Prikaz pravila veriženja časovnih žigov

### 8.5.3.9 Mapa Varnost

Mapa »Varnost« (angl. Security) vsebuje naslednje razdelke:

- »Javni atributi z neomejenim dostopom« (angl. Unrestricted public attributes).
- »Hramba digitalnih potrdil« (angl. Certificate Store).
- »Digitalna potrdila« (angl. Certificates).

## Security

### Unrestricted public attributes [Edit](#)

The Unrestricted public attributes section influences the display of entities in the material classification plan. If the list is empty, meaning it does not contain attributes, the user does not see the entities if he does not have the right to read entities. On the contrary, if the list contains at least one attribute, the user, regardless if he has the right to read entities, sees the entity (without its name and its key properties), access rights, retention periods and its system properties.

### Session [Edit](#)

Security context refresh interval

0 s

### Certificate store [Edit](#)

The Certificate Store section contains the settings related to digital certificates and to the functionalities of obtaining revocation data.

Types

OCSP [CRL](#)

Retrieval client implementation

com.imis.imisarc.server.security.cert.RevocationClientImpl

Proxy host

Proxy port

Proxy username

Proxy password

Validities

### Certificates [Add](#)

The Certificates section contains a list of trusted issuers of digital certificates.

✓ CN=Halcom Root CA,O=Halcom,C=SI

✓ CN=Halcom Secure Server CA 1,O=Halcom,C=SI

✓ CN=ImagingSystemsCA,DC=imis,DC=si

✓ CN=SI-TRUST Root,2.5.4.97=#130E56415453492D3137363539393537,O=Republika Slovenija,C=SI

✓ CN=SIGEN-CA G2,2.5.4.97=#130E56415453492D3137363539393537,O=Republika Slovenija,C=SI

Slika 141: Prikaz osnovnega pregleda v mapi »Varnost«

### Javni atributi z neomejenim dostopom

Z dodajanjem atributov v seznam v zavihku »Javni atributi z neomejenim dostopom« prijavljeni uporabnik vpliva na prikaz entitet v načrtu razvrščanja gradiva.

Če je seznam prazen, torej ne vsebuje atributov, uporabnik v primeru, da nima pravice branja entitete, ne vidi obstoja entitete. Nasprotno pa, če se v seznamu nahaja vsaj en atribut, uporabnik kljub temu, da nima pravice branja entitete, vidi obstoj entitete (brez naziva entitete in ključnih vrednosti atributov), pravice dostopa in sistemske lastnosti entitete.

V načinu za urejanje (angl. Edit) prijavljeni uporabnik v spustnem meniju iskalnega polja »Izberi atribut« (angl. Select attribute) izbere ustrezen atribut.

Atribut je javno dostopen za vse uporabnike ne glede na pravice. Na seznam jih dodaja z ukazom **Dodaj** (angl. Add).

#### Unrestricted public attributes

The Unrestricted public attributes section influences the display of entities in the material classification plan. If the list is empty, meaning it does not contain attributes, the user does not see the entities if he does not have the right to read entities. On the contrary, if the list contains at least one attribute, the user, regardless if he has the right to read entities, sees the entity (without its name and its key properties), access rights, retention periods and its system properties.

Attribute

Slika 142: Nastavitev parametrov v razdelku »Javni atributi z neomejenim dostopom«

## Seja

Razdelek »Seja« (angl. Session) vsebuje nastavitev »Intervala osveževanja seje« (angl. Session security context refresh interval). Prijavljeni uporabnik določi na koliko sekund se bo seja osveževala.

## Hramba digitalnih potrdil

Razdelek »Hramba digitalnih potrdil« (angl. Certificate Store) vsebuje nastavitve povezane z digitalnimi potrdili in funkcionalnostmi pridobivanja podatkov o preklicih digitalnih potrdil.

Prijavljeni uporabnik lahko ureja (angl. Edit) naslednje nastavitve:

- »Vrste« (angl. Types): določa vrste informacij o preklicih digitalnih potrdil.
  - »Seznam preklicanih digitalnih potrdil« (angl. CRL): označen parameter pomeni, da je seznam preklicanih digitalnih potrdil omogočen. Z odznačitvijo postane dostop do seznama onemogočen.
  - »Protokol za preverjanje statusa digitalnih potrdil« (angl. OCSP): označen parameter pomeni, da je spletni protokol za preverjanje statusa digitalnih potrdil omogočen. Z odznačitvijo postane spletni protokol onemogočen.
- »Implementacija odjemalca za preklice digitalnih potrdil« (angl. Retrieval client implementation): določa implementacijo odjemalca za informacije o preklicih digitalnih potrdil.
- »Naslov posredniškega strežnika« (angl. Proxy host): določa IP naslov posredniškega strežnika z informacijami o preklicih digitalnih potrdil.
- »Številka vrata posredniškega strežnika« (angl. Proxy port): določa številko vrat za dostop do posredniškega strežnika z informacijami o preklicih digitalnih potrdil.

- »Uporabniško ime posredniškega strežnika« (angl. Proxy username): določa uporabniško ime za dostop do posredniškega strežnika z informacijami o preklicih digitalnih potrdil.
- »Geslo posredniškega strežnika« (angl. Proxy password): določa geslo za dostop do posredniškega strežnika z informacijami o preklicih digitalnih potrdil.
- »Veljavnost« (angl. Validities): seznam veljavnosti informacij o preklicih digitalnih potrdil.

**Certificate store**  
The Certificate Store section contains the settings related to digital certificates and to the functionalities of obtaining revocation data.

Types  CRL  OCSP

Retrieval client implementation

Proxy host

Proxy port

Proxy username

Proxy password

Validities Add

Slika 143: Nastavitev parametrov v razdelku »Shramba digitalnih potrdil«

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi naslednje nastavitve:

- Pot do strežnika« (angl. URL): določa URL naslov poti do strežnika.
- »Časovno obdobje« (angl. Period): določa čas veljavnosti informacije o preklicih digitalnih potrdil.

**Certificate store validity** ×

URL

Period

Add another

Slika 144: Nastavitev parametra »Veljavnost hrambe digitalnih potrdil«

## Digitalna potrdila

Razdelek »Digitalna potrdila« (angl. Certificates) vsebuje seznam zaupanja vrednih izdajateljev digitalnih potrdil.

Z izbiro dejanja »Dodaj« (angl. Add) prijavljeni uporabnik dodaja digitalna potrdila.

Z izbiro digitalnega potrdila v seznamu se prikažejo naslednje nastavitve:

- »Identifikator« (angl. Identifier): enoličen identifikator digitalnega potrdila.
- »Naziv« (angl. Subject): polno (razločevalno) ime digitalnega potrdila.
- »Omogočen« (angl. Enabled): določa ali je digitalno potrdilo je zaupanja vrednega izdajatelja omogočeno.
- »Vrsta« (angl. Type): vrsta digitalnega potrdila.
- »Izdajatelj« (angl. Issuer): polno (razločevalno) ime izdajatelja digitalnega potrdila po standardu X.509.
- »Veljavno od« (angl. Valid From): datum in čas začetka veljavnosti digitalnega potrdila.
- »Veljavno do« (angl. Valid To): datum in čas zaključka veljavnosti digitalnega potrdila.

The screenshot shows the 'Certificates' section in a web interface. At the top, there is a title 'Certificates' and an 'Add' button. Below the title, a message states: 'The Certificates section contains a list of trusted issuers of digital certificates.' There are three entries in the list, each with a green checkmark and a dropdown arrow. The selected entry is expanded to show a detailed view of a certificate. At the top of this view, there are two buttons: 'Disable this certificate' and 'Download'. Below these buttons is a table with the following data:

Identifier	1000003
Subject	/C=SI/O=POSTA/OU=POSTArCA
Enabled	<input checked="" type="checkbox"/> Yes
Type	CA
Issuer	/C=SI/O=POSTA/OU=POSTArCA
Valid from	7. Feb 2003 11:36
Valid to	7. Feb 2023 12:06

Slika 145: Prikaz lastnosti digitalnega potrdila

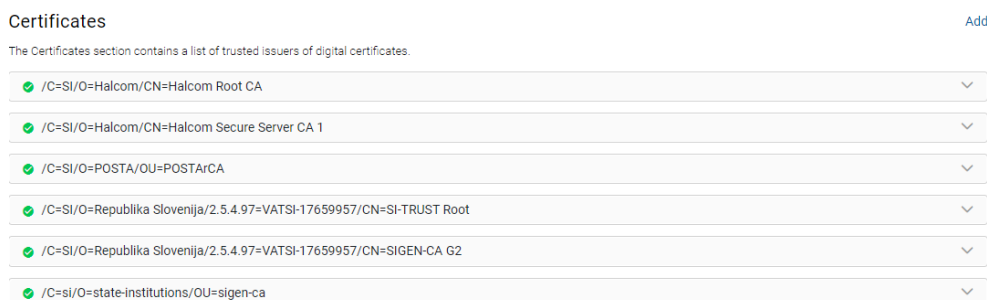
Prijavljeni uporabnik onemogoči izbrano digitalno potrdilo zaupanja vrednega izdajatelja digitalnih potrdil z dejanjem »Onemogoči digitalno potrdilo« (angl. Disable this certificate).

Ponovno ga omogoči z izbiro ukaza »Omogoči digitalno potrdilo« (angl. Enable this certificate).



Digitalno potrdilo lahko prenese na računalnik ali napravo z izbiro dejanja »Prenos« (angl. Download).

Digitalno potrdilo je prijavljenemu uporabniku na voljo v razdelku »Digitalna potrdila« (angl. Certificates) v osnovnem pregledu nastavitve mape »Varnost«.



Slika 146: Prikaz seznama digitalnih potrdil

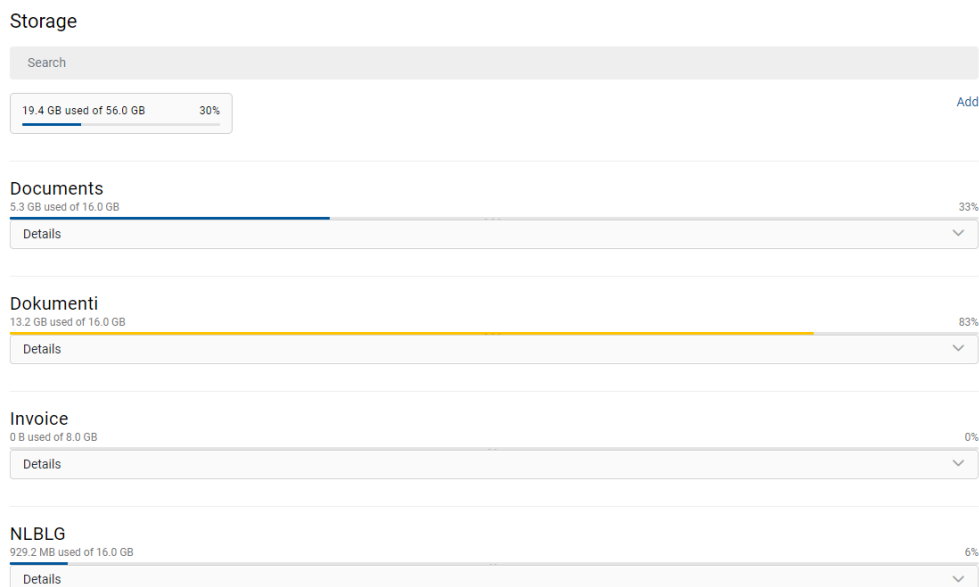
### 8.5.3.10 Mapa Strežnik

Mapa »Strežnik« (angl. Storage) vsebuje seznam shranjevalnih profilov (angl. Storage profiles) in volumnov (angl. Storage volumnes).

Za lažje iskanje je prijavljenemu uporabniku omogočeno iskanje po vnesenih znakih v iskalno polje (angl. Search) in izbira shranjevalnega profila v seznamu.

V osnovnem pregledu se poleg iskalnika profilov in volumnov ter prikaza podatkov o celotnem razpoložljivem prostoru, nahaja tudi seznam profilov.

- »Naziv profila« (angl. Name): naziv profila. Podatek je obvezen.
- »Uporabljeno« (angl. Usage): prikazuje velikost zasedenega prostora in odstotek zasedenosti prostora za posamezen profil v giga-bajtih (GB).



Slika 147: Prikaz osnovnega pregleda v mapi »Strežnik«

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi naslednje nastavitve:

- »Naziv profila« (angl. Name): vsebuje enolično ime profila. Podatek je obvezen.
- »Opis« (angl. Description): vsebuje kratek opis profila.
- »Razpoložljiv prostor« (angl. Size): velikost razpoložljivega prostora za profil v (giga)bajtih.
- »Uporabljeno« (angl. Usage): velikost zasedenega prostora za profil v giga-bajtih (GB).
- »Število objektov« (angl. Objects): število hranjenih objektov v profilu.
- »Možnosti« (angl. Options): omogoča izbiro lastnosti profila:
  - »Samo za branje« (angl. Read only): označen parameter pomeni, da v profilu ni mogoče ustvarjati novih objektov, obstoječi pa so samo za branje. Prijavljeni uporabnik označi parameter, če ne želi spreminjanja vsebine profila.
  - »Zapiši enkrat, beri večkrat« (angl. Write once, read many): odznačen parameter pomeni, da je vsebino mogoče zapisati in brati večkrat. Nasprotno, z označitvijo parametra je vsebino mogoče zapisati samo enkrat, medtem ko je za branje na voljo večkrat.
  - »Prepoved dodajanja vsebin« (angl. Stop adding objects): označen parameter pomeni, da vsebin ni mogoče dodajati na profil. Nasprotno, z odznačitvijo parametra jo je mogoče dodajati.

- »Uporabljeno v« (angl. Used by): določa pod katerim razredom se bo izbrani profil uporabljal. V kolikor vrednost identifikatorja ne določi, se profil uporablja na nivoju arhiva, sicer pa samo pod določenim razredom.

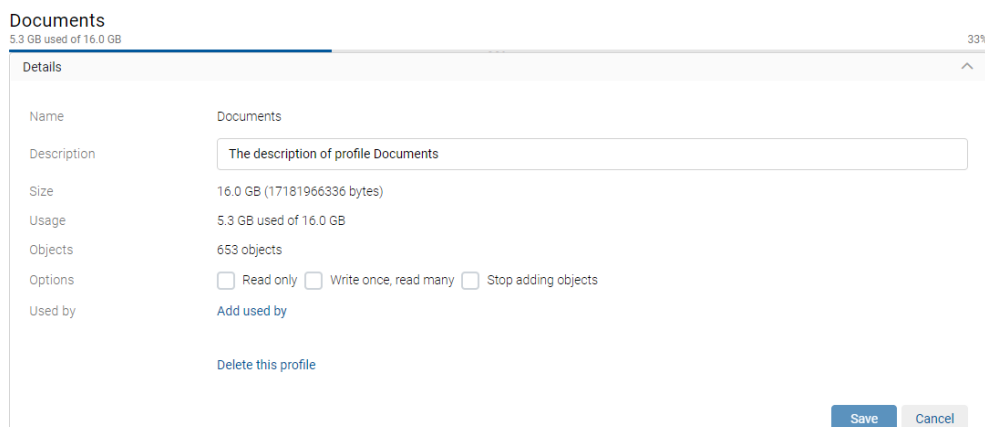
Z izbiro ukaza »Dodaj uporabljeno v« (angl. Add used by) prijavljeni uporabnik izbere eno od naslednjih možnosti ...

- »Klasifikacijska oznaka« (angl. Classification code)
- »Zunanji identifikator razreda« (angl. External)
- »Interni identifikator razreda« (angl. Internal).

... in določi vrednost.



Slika 148: Izbira dejanja »Dodaj uporabljeno v«



Slika 149: Nastavitev parametrov shranjevalnega profila

Po shranitvi profila (angl. Save) lahko prijavljeni uporabnik v načinu za urejanje (angl. Edit) ureja nastavitve profila in dodaja volumne.

Shranjevalni profil odstrani z dejanjem »Odstrani shranjevalni profil« (angl. Delete this storage profile).

Z izbiro dejanja »Dodaj volumen« (angl. Add volume) določi naslednje nastavitve:

- »Ime« (angl. Name): enolično ime volumna.
- »Opis« (angl. Description): vsebuje kratek opis volumna.
- »Lokacija« (angl. Location): logična pot do volumna na datotečnem sistemu. Podatek je obvezen.
- »Razpoložljiv prostor« (angl. Size): velikost razpoložljivega prostora na volumnu v bajtih. Volumnu lahko prijavljeni uporabnik dodeli več prostora tako, da vpiše novo vrednost ali s povečanjem po 1024 bajtov ustrezno poveča vrednost. V primeru, da želi preprečiti nadaljnje shranjevanje objektov v volumen, izenači velikost razpoložljivega prostora z vrednostjo atributa »Uporabljeno« (angl. Used).
- »Uporabljeno« (angl. Usage): prikazuje velikost zasedenega prostora za posamezen volumen v giga-bajtih (GB).
- »Zaporedje profila« (angl. Profile sequence): določi položaj v vrsti volumnov profila. Z izbiro vrednosti »Prvi« (angl. First) ga lahko postavi na začetek vrste ali pa izbere obstoječe ime volumna za katerim želi, da se volumen umesti.

*Opomba:*

*V primeru, da na volumnu še ni objektov, je možno ime profila in položaj spreminjati, sicer pa sta vrednosti po prvem shranjevanju nespremenljivi.*

- »Število objektov« (angl. Objects): število hranjenih objektov v posameznem volumnu.
- »Priklopljen« (angl. Mounted): odznačitev parametra pomeni, da volumen ni dosegljiv za uporabo.
- »Možnosti« (angl. Options): omogoča izbiro lastnosti volumna:
  - »Samo za branje« (angl. Read only): označen parameter pomeni, da v volumnu ni mogoče ustvarjati novih objektov, obstoječi pa so samo za branje. Prijavljeni uporabnik označi parameter, če ne želi spreminjanja vsebine volumna.
  - »Zapiši enkrat, beri večkrat« (angl. Write once, read many): odznačen parameter pomeni, da je vsebino mogoče zapisati in brati večkrat. Nasprotno, z označitvijo parametra je vsebino mogoče zapisati samo enkrat, medtem ko je za branje na voljo večkrat.
  - »Prepoved dodajanja vsebin« (angl. Stop adding objects): označen parameter pomeni, da vsebin ni mogoče dodajati v volumen. Nasprotno, z odznačitvijo parametra jo je mogoče dodajati.

Volumes Add volume

**vol04**  
432.0 kB used of 2.0 MB 6 objects on /iarc/vol/vol04  
21%

Name: vol04

Description:

Location: /iarc/vol/vol04

Size: 2097152

Usage: 432.0 kB used of 2.0 MB

Profile sequence: 0

Objects: 6

Mounted: Yes

Options:  Read only  Write once, read many  Stop adding objects

[Delete this volume](#)

Slika 150: Prikaz nastavitve volumna

**Opozorilo:** Prijavljeni uporabnik lahko povečuje ali zmanjšuje razpoložljiv prostor volumna v bajtih. V primeru, da vrednost atributa »Velikost« (angl. Size) izenači ali zmanjša pod vrednost atributa »Uporabljeno« (angl. Used), onemogoči dostop do volumna.

Po shranitvi (angl. Save) je volumen prijavljenemu uporabniku na voljo v pregledu izbranega profila.

Documents 33%

5.3 GB used of 16.0 GB

Details

Name: Documents

Description:

Size: 16.0 GB (17181966336 bytes)

Usage: 5.3 GB used of 16.0 GB

Objects: 653 objects

Options:  Read only  Write once, read many  Stop adding objects

Used by: [Add used by](#)

[Delete this profile](#)

Volumes Add volume

**vol04**  
432.0 kB used of 2.0 MB 6 objects on /iarc/vol/vol04  
21%

**vol00**  
5.3 GB used of 8.0 GB 647 objects on /iarc/vol/vol00  
67%

**vol01**  
0 B used of 8.0 GB 0 objects on /iarc/vol/vol01  
0%

Slika 151: Prikaz volumna v pregledu izbranega profila

***Opozorilo:** Za uveljavitev sprememb nastavitve vrednosti v mapi »Volumni« (angl. Volumes) je potrebno ponovno zagnati strežnik IMiS®/ARChive Server.*

Prijavljeni uporabnik odstrani volumen tako, da v načinu za urejanje v seznamu volumnov izbere dejanje »Odstrani volumen« (angl. Delete this volume).

***Opozorilo:** Za uveljavitev sprememb nastavitve vrednosti v mapi »Profili« (angl. Profiles) je potrebno ponovno zagnati strežnik IMiS®/ARChive Server.*

### 8.5.3.11 Mapa Tipi

V mapi »Tipi« (angl. Types) so prijavljenemu uporabniku na voljo naslednje vsebovane mape:

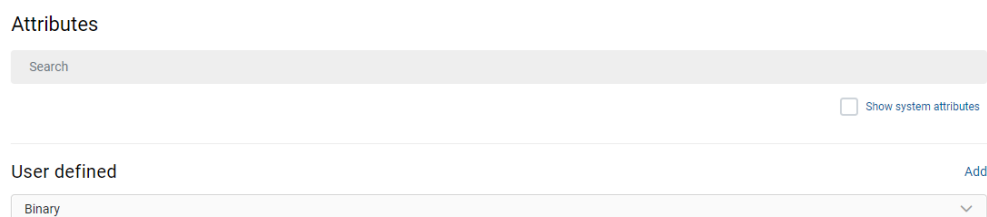
- »Atributi« (angl. Attributes)
- »Šifranti« (angl. Codelists)
- »Številčenje« (angl. Counters)
- »Hramba« (angl. Retention)
- »Predloge« (angl. Templates).

### 8.5.3.12 Mapa Atributi

Mapa »Atributi« (angl. Attributes) vsebuje seznam atributov, ki so opisani z njihovimi vrednostmi. Mapa vsebuje naslednje razdelke:

- »Uporabniško določeni« (angl. User defined).
- »Sistemski« (angl. System), v kolikor prijavljeni uporabnik označi parameter »Prikaži sistemske attribute« (angl. Show system attributes).

V osnovnem pregledu je naveden naziv atributa (angl. Name).



Attributes

Search

Show system attributes

User defined Add

Binary

Slika 152: Prikaz osnovnega pregleda v mapi »Atributi«

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi naslednje nastavitve:

- »Ime« (angl. Name): vsebuje naziv atributa. Če gre za sistemski atribut, je na začetku navedena vrsta atributa (sys:, eml:, prm:, trf:), kateri sledi kratek opis. Vrednost za naziv atributa je potrebno pri novih vnosih obvezno določiti pred shranjevanjem. Po shranjevanju je ni mogoče več spreminjati. Podatek je obvezen.
- »Labela« (angl. Label): vsebuje uporabniku prijazno oznako atributa.
- »Vrsta« (angl. Type): določa vrsto atributa (DirectoryEntity, Binary, Boolean, Int XXX, Double, Date, DateTime, Decimal, File, String, Time, UInt XXX). Vrednost za vrsto atributa je potrebno pri novih vnosih izbrati pred shranjevanjem, saj jo po shranjevanju ni mogoče spreminjati. Podatek je obvezen.
- »Opis« (angl. Description): vsebuje kratek opis atributa.
- »Validacijska formula« (angl. ValidationExpression): določa vrednost, ki predstavlja regularni izraz (angl. Regular expression), s katerim se nove ali spremenjene vrednosti atributa preverjajo.

Več o sintaksi in pravilih: [http://en.wikipedia.org/wiki/Regular\\_expression](http://en.wikipedia.org/wiki/Regular_expression).

*Primeri validacijske formule:*

*Na strežniku IMiS®/ARChive Server je izvedena Perl sintaksa regularnih izrazov.*

*Celotna vrednost atributa se mora ujemati z sintakso validacijske formule. Na spletnemu naslovu <http://www.perfect.com/articles/regextutor.shtml> lahko uporabnik preveri ustreznost sintakse. V nadaljevanju navajamo nekaj primerov. Vrednosti so pisane v enojnih narekovajih in niso del vrednosti.*

*Regularni izraz: 'A-Za-z'*

*Sprejeta vrednost: vrednost 'A-Za-z'*

*Vrednost atributa mora biti enaka vrednosti regularnega izraza.*

*Regularni izraz: '[A-Za-z]'*

*Sprejete vrednosti: ena črka, ki ima vrednosti med 'A' in 'Z' ali 'a' in 'z'*

*Vse ostale kombinacije (npr: 'ab', 'Ab', 'aB', '123a' ipd.) so neveljavne.*

*Regularni izraz: 'a\*b'*

*Sprejete vrednosti: kombinacije vrednosti 'ab', 'aaaaab', 'aaaaaaaaaab', lahko tudi samo 'b'.*

*Zvezdica pomeni, da predhodni znak 'a' ni prisoten ali pa se lahko večkrat ponovi. Vse ostale kombinacije, ki delno ustrezajo (npr: '123aaaab', 'aaab123') ali ne ustrezajo (npr: 'gbrtz', '12345') so neveljavne.*

*Regularni izraz: 'a+b'*

*Sprejete vrednosti: kombinacije vrednosti 'ab', 'aaaaab' ipd. Znak '+' zahteva prisotnost predhodnega znaka 'a', ki se lahko tudi ponavlja. Vrednost 'b' v tem primeru ni veljavna. Za vse ostale kombinacije velja enako kot v prejšnjem primeru.*

*Regularni izraz: '.at'*

*Sprejete vrednosti: vse 3 črkovne vrednosti, ki se končajo na 'at' (npr. 'cat', 'tat', 'pat', '5at', ipd). Vse ostale vrednosti so neveljavne.*

- »Možnosti« (angl. Options): omogoča izbiro dodatnih parametrov atributa:
  - »Iskalen« (angl. Searchable): določa, ali je možno iskati po njeni vrednosti. Označitev parametra pomeni, da je iskanje po vrednosti atributa možno s funkcijami iskanja.
  - »Unikaten« (angl. Unique): Označitev parametra pomeni, da gre za unikatno vrednost atributa na nivoju strežnika. Prijavljeni uporabnik nastavi parameter, če ne želi da pride do vnosa vrednosti atributa, ki jo že določa druga entiteta.
  - »Izbornik« (angl. PickList): Označitev parametra pomeni, da so vrednosti vnaprej določene in zato ročni vnos izven seznama dovoljenih vrednosti ni možen.

## Attributes

Show system attributes

---

### User defined

[Edit](#) [Add](#)

Binary
^

Name	Binary
Label	<input type="text" value="Binary"/>
Type	Binary
Description	<input type="text"/>
Validation expression	<input type="text"/>
Options	<input type="checkbox"/> Searchable <input type="checkbox"/> Unique <input type="checkbox"/> Pick list
Used by	<input type="button" value="D01"/> <input type="button" value="Custom Document"/> <input type="button" value="FiledDocumentTest1"/> <input type="button" value="FiledDocumentTest2"/>

[Copy](#)
[Paste](#)
[Delete this attribute](#)

Slika 153: Dodajanje novega atributa



Z izbiro dejanja »Kopiraj« (angl. Copy) se podatki entitete imenika prenesejo v odložišče (angl. Clipboard).

Prijavljeni uporabnik lahko v načinu za urejanje podatke o predhodno shranjenem atributu »Prilepi« (angl. Paste) iz odložišča in s tem prihrani čas vnosa atributov v seznam.

Atribut odstrani tako, da ga v načinu za urejanje (angl. Edit) izbere v seznamu in odstrani z ukazom »Odstrani atribut« (angl. Delete this attribute) v ukazni vrstici. Odstrani ga lahko samo v primeru, če atribut še ni povezan na predlogo, na kateri so že ustvarjene entitete.

Po shranitvi (angl. Save) je atribut prijavljenemu uporabniku na voljo v osnovnem pregledu nastavitev mape »Atributi«.

S povezavo atributa na izbrano predlogo (poglavje [Mapa Predloge](#)) lahko prijavljeni uporabnik poleg zgoraj navedenih nastavitev pregleduje tudi parameter:

- »Uporabljen v« (angl. Used by): vsebuje nazive predlog, v katerih je atribut uporabljen.

Za lažje iskanje atributov v seznamu je prijavljenemu uporabniku na voljo iskalnik. Z vpisom vsaj enega znaka v iskalno polje, se ustrezno zoži nabor prikazanih rezultatov iskanja v seznamu.

Attributes

actj x

Show system attributes

User defined Add

User defined attributes are empty

System

sys.ret.pol:Action v

sys.ret.rev:Action v

sys.trf.MoveAgent v

Slika 154: Vpis iskalnega niza v iskalno polje

Prijavljeni uporabnik odstrani atribut tako, da v načinu za urejanje (angl. Edit) izbere atribut v seznamu in ga odstrani z ukazom »Odstrani atribut« (angl. Delete this attribute) v ukazni vrstici. Odstrani ga lahko samo v primeru, če atribut še ni povezan na predlogo, na kateri so že ustvarjene entitete.

### 8.5.3.13 Mapa Šifranti

Mapa »Šifranti« (angl. Codelists) vsebuje seznam šifrantov, katerim lahko prijavljeni uporabnik določi nabor vrednosti. Mapa vsebuje naslednje razdelke:

- »Uporabniško določeni« (angl. User defined).
- »Sistemski« (angl. System), v kolikor prijavljeni uporabnik označi parameter »Prikaži sistemske šifrante« (angl. Show system codelists).

V osnovnem pregledu so navedeni naslednji podatki o šifrantih:

- »Predloga« (angl. Template): predloga, na katero je vezan šifrant.
- »Atribut« (angl. Attribute): atribut, na katerega je vezan šifrant.

#### Codelists

Show system codelists

#### User defined

[Edit](#) [Add](#)

Any template / evaluation	
Attribute	evaluation
Template	Any template
Keywords	1:{alias=1 star}
	2:{alias=2 star}
	3:{alias=3 star}
	4:{alias=4 star}
	<a href="#">Copy</a>

Document 02 / LP

#### System

Any template / sys.eml:Priority

Any template / sys.prm:Status

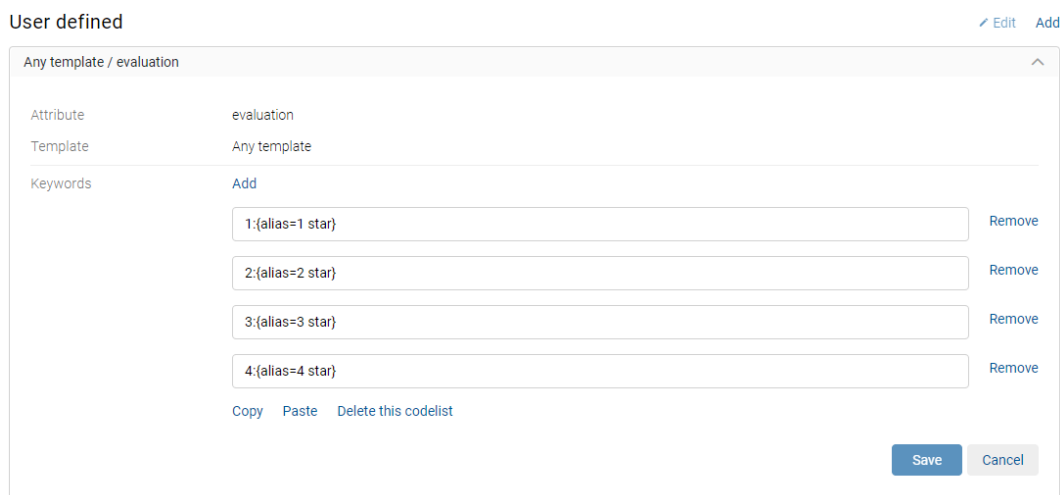
Any template / sys.ret.pol>Action

Slika 155: Prikaz osnovnega pregleda v mapi »Šifranti«

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi naslednje nastavitve:

- »Atribut« (angl. Attribute): iz seznama razpoložljivih atributov prijavljeni uporabnik izbere ustrezen atribut. Po shranjevanju nastavitve ni mogoče spreminjati. Podatek je obvezen.
- »Predloga« (angl. Template): iz seznama razpoložljivih predlog prijavljeni uporabnik izbere posamezno predlogo ali vse predloge (angl. All templates).

- »Ključne besede« (angl. Keywords): vsebuje nabor razpoložljivih vrednosti atributa. Prijavljeni uporabnik lahko doda ključno besedo z ukazom »Dodaj« (angl. Add), odstrani pa jo z izbiro »Odstrani« (angl. Remove).



User defined / Edit Add

Any template / evaluation ^

Attribute	evaluation
Template	Any template
Keywords	Add

Remove

Remove

Remove

Remove

[Copy](#) [Paste](#) [Delete this codelist](#)

Save Cancel

Slika 156: Dodajanje novega šifranta

Z izbiro dejanja »Kopiraj« (angl. Copy) se podatki šifranta prenesejo v odložišče (angl. Clipboard).

Prijavljeni uporabnik lahko v načinu za urejanje podatke o predhodno shranjenem šifrantu »Prilepi« (angl. Paste) iz odložišča in s tem prihrani čas vnosa šifrantov v seznam.

Šifrant odstrani tako, da ga v načinu za urejanje (angl. Edit) izbere in odstrani z ukazom »Odstrani šifrant« (angl. Delete this codelists).

Po shranitvi (angl. Save) je šifrant na voljo prijavljenemu uporabniku v osnovnem pregledu nastavitev mape »Šifranti«.

***Opozorilo:** Pri dodajanju vrednosti je potrebno paziti na pravilno sintakso zapisa (npr. 1:{alias="value"}). Razpoložljiva vrednost atributa je lahko zapisana v narekovajih.*

### 8.5.3.14 Mapa Številčenje

V mapi »Številčenje« (angl. Counters) prijavljeni uporabnik določa števec, ki se uporabljajo za ustvarjanje vrednosti izbranih atributov.

Za razred (angl. Class), zadevo (angl. Case) in dokument (angl. Document) določi do katerega nivoja v načrtu razvrščanja gradiva lahko ustvarja vsebovane entitete.

V osnovnem pregledu so navedeni naslednji podatki o števcih:

- »Vrsta« (angl. Scope)
- »Nivo« (angl. Level)
- »Osnova nivoja« (angl. Level aspect)



Slika 157: Prikaz osnovnega pregleda mape »Številčenje«

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi naslednje nastavitve:

- »Vrsta« (angl. Scope): določa vrsto entitete (razred, zadeva ali dokument). Na obstoječih vnosih je ni mogoče spreminjati. Podatek je obvezen.
- »Osnova nivoja« (angl. Level aspect): označuje položaj entitete v načrtu razvrščanja gradiva glede na nadrejeno entiteto. Prijavljeni uporabnik lahko izbira med vrednostmi »Relativna« (angl. Relative) in »Absolutna« (angl. Absolute). V primeru izbire vrednosti »Relativna«, se določa enoličnost številčenja s poljem »Enoličnost« (angl. Unique within). V primeru izbire vrednosti »Absolutna« pa bo številčenje enolično na nivoju celotnega arhiva. Podatek je obvezen.

- »Nivo« (angl. Level): označuje nivo entitete v načrtu razvrščanja gradiva. Z določitvijo novega nivoja razreda, zadeve ali dokumenta, lahko prijavljeni uporabnik s pravico »Ustvarjanje entitet« (angl. Create entities) ustvari novo vsebovano entiteto te vrste. Na obstoječih vnosih je ni mogoče spreminjati. Podatek je obvezen.
- »Atribut« (angl. Storage): predstavlja atribut, za katerega se vrednost ustvari s števcem. Prijavljeni uporabnik lahko izbira med »Klasifikacijsko oznako« (angl. Classification code) in uporabniško določenimi atributi. Na obstoječih vnosih jo ni mogoče spreminjati. Podatek je obvezen.
- »Enoličnost« (angl. Unique within): določa enoličnost števca znotraj izbranega konteksta. Podatek je obvezen. Prijavljeni uporabnik lahko izbira med naslednjimi konteksti:
  - »Arhiv« (angl. Archive): enoličnost velja za celotni arhiv;
  - »Zadnji razred« (angl. Leaf class): enoličnost velja za zadnji razred v verigi nadrejenih razredov;
  - »Nadrejen razred« (angl. Parent): enoličnost velja za nadrejeni razred;
  - »Prvi razred« (angl. Root class): enoličnost velja za prvi razred v verigi nadrejenih razredov.
- »Začetna vrednost« (angl. Initial value): začetna vrednost števca vrednosti atributa, ki je izbran v polju »Atribut« (angl. Storage).
- »Interval povečanja« (angl. Increment): določa v kakšnih korakih se bo povečeval števec pri vrednosti atributa, ki je izbran v polju »Atribut« (angl. Storage).
- »Format zapisa« (angl. Format): zapis vrednosti atributa, ki je izbran v polju »Atribut« (angl. Storage).

Folder / Level 4 / Relative

Scope	Folder
Level aspect	Relative
Level	4
Storage	sys.ClassificationCode
Unique within*	Parent
Initial value	1
Increment	1
Format	%05@count@
Validation expression	

Copy Paste Delete this counter

Save Cancel

Slika 158: Dodajanje novega števca

Z izbiro dejanja »Kopiraj« (angl. Copy) se podatki števca prenesejo v odložišče (angl. Clipboard).

Prijavljeni uporabnik lahko v načinu za urejanje podatke o predhodno shranjenem števcu »Prilepi« (angl. Paste) iz odložišča in s tem prihrani čas vnosa števcov v seznam.

Števec odstrani tako, da ga v načinu za urejanje (angl. Edit) odstrani z ukazom »Odstrani števec« (angl. Delete this counter).

Po shranitvi (angl. Save) je števec na voljo prijavljenemu uporabniku v osnovnem pregledu nastavitev mape »Številčenje«.

*Opozorilo: Administrator strežnika mora skrbno načrtovati strukturo drevesa entitet. Zaradi pravilnega razvrščanja entitet v načrtu razvrščanja gradiv je priporočljivo, da vnaprej predvidi število korenskih razredov. Glede na število korenskih razredov ustrezno določi format (angl. Format).*

*Primer: Vrednost »%02@count@« atributa Format na zgornji sliki določa, da se klasifikacijske oznake razredov zapisujejo v vrstnem redu od 1 – 99. Razredi s klasifikacijsko oznako med 100 in 199, bi se ob tej nastavitvi razvrščali med 10 in 20, kar vodi v nepreglednost načrta razvrščanja gradiva. V kolikor je vnaprej predvideno število razredov okoli 100, je potrebno vrednost atributa Format nastaviti na »%03@count@«.*

### 8.5.3.15 Mapa Hramba

Mapa »Hramba« (angl. Retention) vsebuje naslednja razdelka:

- »Politike hrambe« (angl. Retention policies)
- »Zadržanje uničenja« (angl. Disposition holds).

The screenshot shows a web interface for the 'Retention' map. It is divided into two main sections:

- Disposition holds:** This section has a title 'Disposition holds' and a subtitle 'The Disposition hold section contains the disposition hold settings.' To the right of the title are links for 'Edit' and 'Add'. Below the subtitle is a dropdown menu currently set to 'Legacy procedure'.
- Retention policies:** This section has a title 'Retention policies' and a subtitle 'The Retention policies section contains a list of retention policies.' To the right of the title are links for 'Edit' and 'Add'. Below the subtitle is a list of five dropdown menus, each representing a retention policy: 'Permanent', '1-year', '2-years', '5-years', and '10-years'.

Slika 159: Prikaz osnovnega pregleda v mapi »Hramba«

#### Zadržanje uničenja

Razdelek »Zadržanje uničenja« (angl. Disposition hold) vsebuje nastavitve.

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi naslednje nastavitve:

- »Naziv« (angl. Name): enoličen naziv zadržanja uničenja. Vrednost se po shranjevanju lahko spremeni, ne sme pa biti prazna. Podatek je obvezen.
- »Razlog« (angl. Reason): privzeti razlog za zadržanje uničenja v postopku izvajanja odbiranja in izločanja. Podatek je obvezen.
- »Opis« (angl. Description): kratek opis zadržanja uničenja.

Po shranitvi (angl. Save) se zapisu zadržanja uničenja dodajo še naslednji podatki:

- Ustvarjeno« (angl. Created): datum, čas in uporabnik (avtor) ustvarjenega zadržanja uničenja.
- »Identifikator« (angl. Identifier): enoličen identifikator zadržanja uničenja.

Disposition holds [Edit](#) [Add](#)

The Disposition hold section contains the disposition hold settings.

Legacy procedure ^

Name\*

Reason\*

Description

Created 3. Jun 2020, 15:50 by admin

Identifier 364c6d9f1acd8d791c1bc9c9c502bae4568564fe9da701092360759482b062f7

[Copy](#) [Paste](#) [Delete this disposition hold](#)

Slika 160: Dodajanje zadržanja uničenja

Z izbiro dejanja »Kopiraj« (angl. Copy) se podatki o zadržanju uničenja prenesejo v odložišče (angl. Clipboard).

Prijavljeni uporabnik lahko v načinu za urejanje podatke o predhodno shranjenem zadržanju uničenja »Prilepi« (angl. Paste) iz odložišča in s tem prihrani čas vnosa zadržanj uničenja v seznam.

Zadržanje uničenja odstrani tako, da ga v načinu za urejanje (angl. Edit) odstrani z ukazom »Odstrani zadržanje uničenja« (angl. Delete this disposition hold).

### Politike hrambe

Razdelek »Politike hrambe« (angl. Retention policies) vsebuje seznam politik hrambe.

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi naslednje nastavitve:

- »Naziv« (angl. Name): enoličen naziv politike hrambe. Vrednost se po shranjevanju lahko spremeni, ne sme pa biti prazna. Podatek je obvezen.
- »Dejanje« (angl. Action): privzeto dejanje iz seznama dejanj za entitete, ki so na voljo v izvedbi postopka odbiranja in izločanja. Podatek je obvezen.
- »Razlog« (angl. Reason): privzeti razlog za dejanja, ki se bodo izvedla v postopku izvajanja odbiranja in izločanja. Podatek je obvezen.



- »Sprožilec« (angl. Trigger): iskalni niz, s katerim se izvede iskanje entitet v postopku izvajanja odbiranja in izločanja.
- »Opis« (angl. Description): kratek opis politike hrambe.
- »Podroben opis« (angl. Detailed description): podroben opis politike hrambe.

Po shranitvi (angl. Save) se zapisu politike hrambe dodajo še naslednji podatki:

- »Ustvarjeno« (angl. Created): datum, čas in uporabnik (avtor) ustvarjene politike hrambe.
- »Identifikator« (angl. Identifier): enoličen identifikator politike hrambe.

Retention policies [Edit](#) [Add](#)

The Retention policies section contains a list of retention policies.

Permanent

1-year

2-years

5-years

Name*	5-years
Action*	Dispose <input type="button" value="v"/>
Reason*	Dispose after 5 years retention
Trigger	[Review Trigger] + 5Y < @NOW@
Description	Dispose after 5 years retention
Detailed description	Records must be kept 5 years from the end of the year when they were closed
Created	18. Feb 2020, 20:12 by admin
Identifier	0a9cbc12b0cd5aba609042fd353031b7e1941b0f1fd59be0ad6c00e1190e9058 <a href="#">Copy</a> <a href="#">Paste</a> <a href="#">Delete this retention policy</a>
Mandates	No retention policy mandates. <span style="float: right;"><a href="#">Add</a></span>

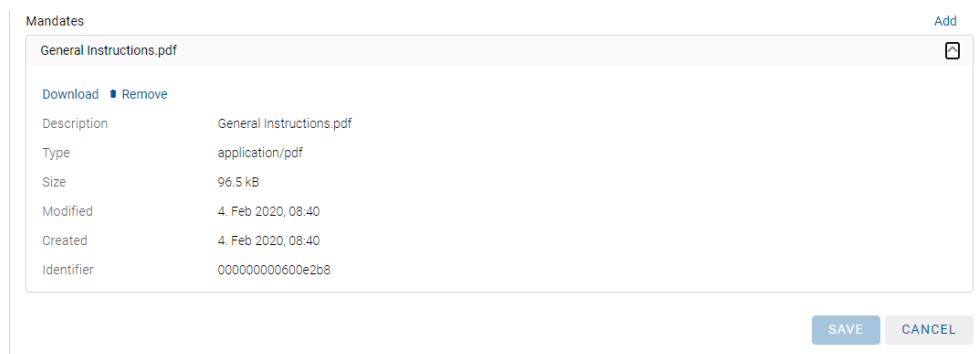
Slika 161: Dodajanje podatkov o politiki hrambe

Z izbiro dejanja »Kopiraj« (angl. Copy) se podatki o politiki hrambe prenesejo v odložišče (angl. Clipboard).

Prijavljeni uporabnik lahko v načinu za urejanje podatke o predhodno shranjeni politiki hrambe »Prilepi« (angl. Paste) iz odložišča in s tem prihrani čas vnosa politik hrambe v seznam.

Politiko hrambe odstrani tako, da jo v načinu za urejanje (angl. Edit) odstrani z ukazom »Odstrani politiko hrambe« (angl. Delete this retention policy).

Pooblastila za posamezno politiko hrambe lahko prijavljeni uporabnik doda z izbiro ukaza »Dodaj« (angl. Add) in izbiro obstoječe datoteke s pooblastilom na datotečnem sistemu.



Slika 162: Prikaz pooblastila za politiko hrambe

Z ukazom »Naloži« (angl. Download) odpre izbrano datoteko v oknu brskalnika.

Izbrano pooblastilo lahko odstrani z ukazom »Odstrani« (angl. Remove).

### 8.5.3.16 Mapa Predloge

Mapa »Predloge« (angl. Templates) vsebuje seznam predlog. V seznamu so navedeni naslednjimi podatki o predlogah:

- »Naziv« (angl. Name): naziv predloge.
- »Opis« (angl. Description): kratek opis predloge.
- »Število entitet« (angl. Entity count«): število entitet v katerih je uporabljena predloga.

Templates

Search

Show system templates

User defined Add

Title	Description	Entity count
Case	Folder/Case entity	20
Class	Class entity	234
Class01	Test	4
Custom Document	Custom document include custom content attribute	26
Custom Email Filled	Filed Custom Email	1
Custom Email Standalone	Autonomous Custom Email	1
D01	Document 01	644
Document	Standalone document entity	527

Slika 163: Prikaz osnovnega pregleda v mapi »Predloge«

Predloge so razvrščene v naslednje razdelke:

- »Uporabniško določene« (angl. User defined).
- »Sistemske« (angl. System), v kolikor prijavljeni uporabnik označi parameter »Prikaži sistemske predloge« (angl. Show system templates). Sistemskih predlog ni mogoče spreminjati.

### Osnovne nastavitve

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik določi naslednje nastavitve:

- »Ime« (angl. Name): enoličen naziv predloge. Po prvem shranjevanju postane vrednost nespremenljiva. Podatek je obvezen.
- »Podedovano od« (angl. Inherited from): določi iz katere predloge se predloga katero ustvarja, deduje. Ta prevzame vse attribute od podedovane predloge. Po prvem shranjevanju postane vrednost nespremenljiva.
- »Vrsta predloge« (angl. Type): glede na izbrano vrednost atributa »Podedovano od« se samodejno določi vrsta predloge: »Dokument« (angl. Document), »Zadeva« (angl. Folder) ali »Razred« (angl. Class). Po prvem shranjevanju postane vrednost nespremenljiva.
- »Labela« (angl. Label): vrednost atributa predstavlja oznako predloge.
- »Opis« (angl. Description): kratek opis predloge.
- »Uporabi na predlogi« (angl. Use under template): z izbiro dejanja »Dodaj« (angl. Add) je prijavljenemu uporabniku omogočeno dodajanje predloge v kateri je določena predloga uporabljena.
- »Uporabi na entiteti« (angl. Use under entity): z izbiro dejanja »Dodaj« (angl. Add) je prijavljenemu uporabniku omogočeno dodajanje entitete v kateri je določena predloga uporabljena.

New template

Details Copy Paste Edit

Name\*

Type Folder

Inherited from\*

Label

Description

Use under template Add

Use under entity Add

Create Cancel

Slika 164: Dodajanje nove predloge

Po shranitvi (angl. Save) je prijavljenemu uporabniku dodatno na voljo naslednji podatek:

- »Število entitet« (angl. Entity count): število entitet v katerih je uporabljena predloga.

Templates > CustomFolder

Details		Copy	Edit
Name	CustomFolder		
Type	Folder		
Inherited from	Case		
Label	CustomFolder		
Description	Custom folder include custom content		
Entity count	0		
Use under template			
Use under entity			

Attributes

Inherited attributes from Case

External Identifier (sys:ExternalIds)	▼
Title (sys:Title)	▼
Description (sys:Description)	▼
Keywords (sys:Keywords)	▼

Slika 165: Pregled podatkov o predlogi

Z izbiro dejanja »Dodaj« (angl. Add) lahko prijavljeni uporabnik na predlogo doda atribut in določi naslednje nastavitve:

- »Naziv« (angl. Attribute): naziv atributa. Prijavljeni uporabnik ga izbere iz nabora atributov, ki so na voljo.
- »Vrsta« (angl. Type): vrsta atributa.
- »Opis« (angl. Description): kratek opis atributa.
- »Možnosti« (angl. Options): omogoča izbiro lastnosti atributa:
  - »Samo za dodajanje« (angl. AppendOnly): označitev parametra pomeni, da je vrednost atributa možno k obstoječim vrednostim le dodajati;
  - »Vključen v AIP« (angl. Include in AIP): označitev parametra pomeni, da so vrednosti atributa del arhivskega informacijskega paketa;
  - »Podedovan« (angl. Inherited): označitev parametra pomeni, da se vrednosti atributa dedujejo iz nadrejene hierarhije;

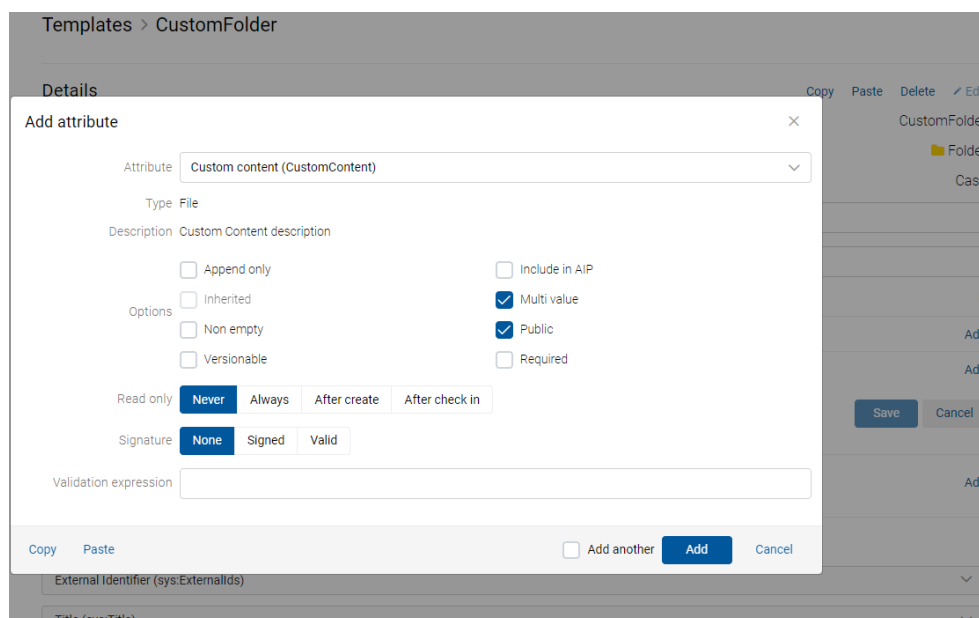
*Opomba:* Lastnost je onemogočena za attribute Binary, File, StringMax v pogovornem oknu za dodajanje atributa na predlogo in pri urejanju.

- »Več vrednosti« (angl. MultiValue): označitev parametra pomeni, da ima atribut lahko več vrednosti;
- »Vrednost ni prazna« (angl. Non Empty): označitev parametra pomeni, da vrednost atributa ne sme biti prazna;
- »Javen« (angl. Public): označitev parametra pomeni, da je atribut javno dostopen za vse uporabnike ne glede na pravice;
- »Verzionabilen« (angl. Versionable): označitev parametra pomeni, da je omogočeno verzioniranje atributa;
- »Obvezen« (angl. Required): označitev parametra pomeni, da je vrednost atributa obvezna.
- »Atribut samo za branje« (angl. Read only): označuje, ali se vrednost atributa lahko spreminja ali ne. Veljavne vrednosti parametra so naslednje:
  - »Nikoli« (angl. Never): vrednost atributa se lahko spreminja kadarkoli;
  - »Vedno« (angl. Always): vrednosti atributa se ne sme spreminjati.
  - »Po shranitvi« (After Create): vrednost atributa se po prvi shranitvi dokumenta ne sme več spreminjati;
  - »Po vložitvi osnutka« (After Check In): vrednost atributa se po vložitvi osnutka dokumenta ne sme več spreminjati.
- »Vrsta validacije podpisa« (angl. Signature): vrednost nastavljena na:
  - »Brez« (angl. None) označuje, da se na vsebini ne preverja prisotnost elektronskega podpisa;
  - »Podpisano« (angl. Signed) označuje, da se na vsebini preverja prisotnost elektronskega podpisa;
  - »Veljaven« (angl. Valid) označuje, da se na vsebini preverja prisotnost in veljavnost elektronskega podpisa.

*Opomba:* Veljavnost elektronskega podpisa se preverja glede na »Obseg preverjanja podpisov« (angl. Verification scope). Za več informacij glej poglavje [Elektronski podpisi](#).

- »Validacijska formula« (angl. Validation expression): določa vrednost, ki predstavlja regularni izraz (angl. Regular expression), s katerim se nove ali spremenjene vrednosti atributa preverjajo.

Več o sintaksi in pravilih: [http://en.wikipedia.org/wiki/Regular\\_expression](http://en.wikipedia.org/wiki/Regular_expression).



Slika 166: Dodajanje ali spreminjanje podatkov in lastnosti atributa

Z izbiro dejanja »Kopiraj« (angl. Copy) se podatki o atributu ali predlogi prenesejo v odložišče (angl. Clipboard).

Prijavljeni uporabnik lahko v načinu za urejanje podatke o predhodno shranjenem atributu ali predlogi »Prilepi« (angl. Paste) iz odložišča in s tem prihrani čas vnosa atributov ali predlog v seznam.

Predlogo odstrani tako, da jo v načinu za urejanje (angl. Edit) odstrani z ukazom »Odstrani zadržanje uničenja« (angl. Delete this disposition hold).

Prijavljeni uporabnik lahko odstrani predlogo tako, da jo v načinu za urejanje (angl. Edit) izbere v osnovnem pregledu in izbere ukaz »Odstrani predlogo« (angl. Delete this template). To izvede samo v primeru, če je število entitet v katerih je uporabljena predloga enako 0.

### Atributi povezani na predlogo


Z izbiro dejanja »Dodaj« (angl. Add) se atribut doda v seznam atributov povezanih na predlogo (angl. Attributes).

Templates > Custom Document

---

**Details**

Name Custom Document

Type  Document

Inherited from Document

Label

Description

Entity count 3




Use under template Class x Add

Use under entity Add


SAVE CANCEL

---

**Attributes**  Show inherited attributes Add




-  Content (sys:Content) ▼
-  Custom Content (CustomContent) ▼
-  String 200 (String200) ▼

Slika 167: Prikaz atributov povezanih na predlogo

Uporabnik lahko spreminja vrstni red atributov na predlogi z izbiro ikone  pred atributom in premikom na ustrezno mesto na način »Povleci in spusti« (angl. Drag and Drop).

S spremembo vrstnega reda atributov na predlogi se spremeni tudi vrstni red prikazanih atributov na entiteti osnovani na tej predlogi. Za več informacij glej poglavje [Vnos metapodatkov entitete v IMiS®/wClient Priročniku](#).

**Attributes**  Show inherited attributes Add

-  Content (sys:Content) ▼
-  Custom Content (CustomContent) ▼
-  String 200 (String200) ▼

Slika 168: Sprememba vrstnega reda atributov na predlogi

Z izbiro »Prikaži podedovane attribute« (angl. Show inherited attributes) se prikaže seznam podedovanih atributov vezanih na izbrano predlogo.

Slika 169: Prikaz podedovanih atributov povezanih na predlogo

**Opozorilo:** Prijavljeni uporabnik lahko dodaja samo uporabniško določene attribute. Sistemski atributi so podedovani iz predloge.

**Opozorilo:** Omejitve za lastnosti atributov na predlogah, na osnovi katerih so že izdelane entitete so naslednje:

- Dovoljena je sprememba lastnosti »Multivalue« iz »False« v »True«, ne pa tudi obratno.
- Dovoljena je sprememba lastnosti »Required« iz »False« v »True«, ne pa tudi obratno.
- Dovoljena je sprememba lastnosti »Inherited« iz »False« v »True«, ne pa tudi obratno.
- Brisanje atributa iz predloge, na osnovi katerih so že izdelane entitete ni mogoče.

**Opozorilo:** Nastavitev se upošteva samo na atributih tipa »Datoteka« (angl. File).

Za lažje iskanje atributov v seznamu je prijavljenemu uporabniku na voljo iskalnik. Z vpisom vsaj enega znaka v iskalno polje, se ustrezno zoži nabor prikazanih rezultatov iskanja v seznamu.

Title	Description	Entity count
Email	Standalone e-mail entity	4
FiledEmail	E-mail filed into a folder/case entity	0

Slika 170: Vpis iskalnega niza v iskalno polje



## 9 ODPRAVLJANJE TEŽAV

V primeru težav in napak je pomembno, da administratorji in uporabniki postopajo pravilno.

Z morebitnim nestrokovnim posegom lahko pride do dodatnega poslabšanja stanja strežnika IMiS®/ARChive Server, s tem pa tudi do težje odprave napake.

Uporabniki/Administratorji morajo biti seznanjeni s pravilnim načinom uporabe strežnika in postopati v skladu z uporabniško dokumentacijo.

Priporočljivo je, da se ob morebitnih težavah obrnejo na ustrezno strokovno osebo v organizaciji (sistemske administratorje).

Sistemskim administratorjem svetujemo, da tudi s pomočjo dokumentacije ugotovijo mesto napake in se po potrebi o nadaljnjih korakih posvetujejo z našimi strokovnjaki.

### 9.1 Kako se težavam izognemo?

Redni periodični pregledi delovanja strežnika IMiS®/ARChive Server so bistvenega pomena pri pravočasnem odkrivanju morebitnih težav in napak v delovanju.

Mednje sodijo tudi pregledi usklajenosti diskovnega sistema (samostojni disk ali diskovno polje) in datotečnega sistema. Težavam z diskovnim sistemom se izognemo tudi tako, da izberemo zanesljivo strojno opremo in poskrbimo, da so uporabljene diskovne kapacitete priklopljene na strežnik lokalno s primerno redundanco.

Izogibamo se diskovnim sistemom NAS ali souporabi diskov na drugih strežnikih oziroma diskovnih kapacitetah, ki so dosegljive preko lokalne mreže.

Periodično preverjamo tudi konsistentnost interne baze strežnika. Več informacij o pogostih vzrokih je na voljo v poglavju [Konfiguriranje](#).

Bistvenega pomena je tudi opsijska veljavna vzdrževalna pogodba, ki zagotavlja minimalne odzivne čase v primeru težjih napak ali izpada sistema.

## 9.2 Pogoste težave

### Opis pogoste težave 1

Na odjemalcih IMiS®/Scan ali IMiS®/View se ob poizkusu pregledovanja objekta shranjenega na strežniku IMiS®/ARChive Server pojavi »Napaka 61523«.

Drugi odjemalci (npr. IMiS®/Storage Connector) javljajo napako:

```
IMiS/ARC Client <IASession.Open> Failed to establish connection to the cluster node <10.1.1.10, 16807> (Reason: Error <TimedOut> occurred while opening network connection.).
```

Strežnik je sicer omrežno dostopen, servis na vratih, kjer posluša, pa ni dostopen (preverjanje s telnet programom)

```
[user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=4 ttl=64 time=0.183 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=5 ttl=64 time=0.164 ms

--- iarc.acme.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.164/0.450/1.530/0.540 ms
```

```
[user1@test ~]# telnet iarc.acme.com 16807
Trying 10.0.0.10...
.. (daljši premor) ...
telnet: connect to address 10.1.1.10: Connection timed out
[user1@test ~]#
```

Strežnik sicer deluje, kar preverimo s konzolnim ukazom na strežniku, kjer je nameščen:

```
[user1@iarc ~]# sudo service iarc status
Status of IMiS/ARChive HSM Storage Server: iarc (pid 23209) is running...
[user1@iarc ~]#
```

### Vzrok težave 1

Požarni zid na strežniku ali omrežju med odjemalcem in strežnikom preprečuje komuniciranje odjemalcev IMiS® s strežnikom IMiS®/ARChive Server preko TCP vrat 16807 ali drugih, v primeru drugačne nastavitve TCP vrat v `/etc/iarc.conf` datoteki.

## Rešitev težave 1

Požarni zid je potrebno ponovno nastaviti tako, da bo dovoljeval komunikacijo odjemalcev IMiS® s strežnikom.

## Opis pogoste težave 2

Ob poizkusu shranjevanja novega objekta, strežnik vrne odgovor:

```
You cannot create an entity with template »%TEMPLATE_NAME%« under specified parent since it's not included in the list of allowed templates.
```

Strežnik je sicer omrežno dostopen, servis na vratih, kjer posluša, se odziva (preverjanje s telnet programom)

```
[user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=4 ttl=64 time=0.183 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=5 ttl=64 time=0.164 ms
```

```
--- iarc.acme.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.164/0.450/1.530/0.540 ms
```

```
[user1@test ~]# telnet iarc.acme.com 16807
Trying 10.1.1.10...
Connected to iarc.acme.com.
Escape character is '^]'.
Connection closed by foreign host.
[user1@test ~]#
```

Strežnik deluje, kar dodatno preverimo s konzolnim ukazom na strežniku, kjer je nameščen:

```
[user1@iarc ~]# sudo service iarc status
Status of IMiS/ARChive HSM Storage Server: iarc (pid 23209) is running...
[user1@iarc ~]#
```

### Vzrok težave 2

Odjemalec skuša shraniti objekt z obstoječo predlogo, ki ni uvrščena v seznam dovoljenih predlog na nadrejeni entiteti.

### Rešitev težave 2

Preveriti je potrebno seznam dovoljenih predlog na nadrejeni entiteti, klasifikacijsko oznako nadrejene entitete ter samo predlogo. V primeru, da je uporabljena napačna predloga ali pa je odjemalec poskušal uvrstiti entiteto na napačno mesto v načrtu razvrščanja gradiva, je potrebno popraviti napako na odjemalcu in znova shraniti objekt. Drugače je potrebno dodati predlogo v seznam dovoljenih predlog.

### Opis pogoste težave 3

Ob poizkusu shranjevanja novega objekta na strežnik IMiS®/ARChive Server z odjemalcem IMiS®/Scan se pojavi »Napaka #14«. Drugi odjemalci (npr. IMiS®/Storage Connector) pri poizkusu shranitve objekta s strežnika dobijo naslednji odgovor:

```
Not enough space on storage profile »%PROFILE_NAME%«. Required %FILE_SIZE% bytes..
```

Strežnik je sicer omrežno dostopen, servis na vratih, kjer posluša, se odziva (preverjanje s telnet programom):

```
[user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data:
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=4 ttl=64 time=0.183 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=5 ttl=64 time=0.164 ms
```

```
--- iarc.acme.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.164/0.450/1.530/0.540 ms
```

```
[user1@test ~]# telnet iarc.acme.com 16807
Trying 10.1.1.10...
Connected to iarc.acme.com.
Escape character is '^]'.
Connection closed by foreign host.
[user1@test ~]#
```

Strežnik deluje, kar dodatno preverimo s konzolnim ukazom na strežniku, kjer je nameščen:

```
[user1@iarc ~]# sudo service iarc status
Status of IMiS/ARChive HSM Storage Server: iarc (pid 23209) is running...
[user1@iarc ~]#
```

### Vzrok težave 3

Prišlo je do zapolnitve vseh volumnov znotraj profila za shranjevanje, ki je bil uporabljen ob shranjevanju novega objekta.

### Rešitev težave 3

Profilu strežnika, ki mi je zmanjkalo prostora dodamo ustrezno število novih volumnov.

### Opis pogoste težave 4

Ob zagonu strežnika IMiS®/ARChive Server se na konzoli pojavi izpis:

```
[user1@iarc ~]# sudo service iarc start

WARNING: Network subsystem not running or (RT)NETLINK interface not configured in this kernel. If you're sure
that your network is UP you can ignore this message. Continue loading IMiS/ARChive HSM Storage Server...

Starting IMiS/ARChive HSM Storage Server:          [ OK ]
[user1@iarc ~]#
```

Strežnik ni omrežno dostopen:

```
[user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
... (premor) ...
From 192.168.92.32 icmp_seq=2 Destination Host Unreachable
From 192.168.92.32 icmp_seq=3 Destination Host Unreachable
From 192.168.92.32 icmp_seq=4 Destination Host Unreachable
... (prekinemo test s CTRL-C) ...
^C
--- iarc.acme.com ping statistics ---
7 packets transmitted, 0 received, +3 errors, 100% packet loss, time 6937ms
[user1@test ~]#
```

#### Vzrok težave 4

Ob zagonu strežnika omrežni podsistem operacijskega sistema ni deloval.

#### Rešitev težave 4

Potrebno je vzpostaviti delovanje omrežnega podsistema in nato ponovno zagnati strežnik.

Če se sporočilo pojavi ponovno, gre verjetno za nezdržljivost strežnika z operacijskim sistemom.

#### Opis pogoste težave 5

Ob zagonu strežnika IMiS®/ARChive Server se na konzoli pojavi izpis:

```
[user1@iarc ~]# sudo service iarc start
```

```
WARNING: Network subsystem not running or (RT)NETLINK interface not configured in this kernel. If you're sure that your network is UP you can ignore this message. Continue loading IMiS/ARChive HSM Storage Server...
```

```
Starting IMiS/ARChive HSM Storage Server:          [ OK ]
```

```
[user1@iarc ~]#
```

Strežnik ni omrežno dostopen:

```
[user1@test ~]# ping iarc.acme.com
```

```
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
```

```
... (premor) ...
```

```
From 192.168.92.32 icmp_seq=2 Destination Host Unreachable
```

```
From 192.168.92.32 icmp_seq=3 Destination Host Unreachable
```

```
From 192.168.92.32 icmp_seq=4 Destination Host Unreachable
```

```
... (prekinemo test s CTRL-C) ...
```

```
^C
```

```
--- iarc.acme.com ping statistics ---
```

```
7 packets transmitted, 0 received, +3 errors, 100% packet loss, time 6937ms
```

```
[user1@test ~]#
```

V dnevniku se v nasledju pojavijo zapisi:

```
<datum in ura zapisa> [iarcd:<decimalna vrednost>:<decimalna vrednost>] INFO[6] Preforking 1 connection
handling childs.
<datum in ura zapisa> [iarcd:<decimalna vrednost>:<decimalna vrednost>] WARN[4] Cannot bind socket 0 to
address [10.1.1.10] on port [16807], error 99: Cannot assign requested address. Socket will be closed.
<datum in ura zapisa> [iarcd:<decimalna vrednost>:<decimalna vrednost>] ERRI[3] Server was unable to open
any configured listening socket.
<datum in ura zapisa> [iarcd:<decimalna vrednost>:<decimalna vrednost>] INFO[6] Child 2922 exited with exit
code 0.
<datum in ura zapisa> [iarcd:<decimalna vrednost>:<decimalna vrednost>] INFO[6] Fatal error occured. Server
is shutting down.
```

### Vzrok težave 5

Ob zagonu strežnika omrežni podsistem operacijskega sistema ne deluje ali pa so v nastavitveni datoteki napačne mrežne nastavitve.

### Rešitev težave 5

Potrebno je preveriti delovanje omrežnega podsistema in ustrezno urediti omrežne nastavitve v nastavitveni datoteki `/etc/iarc.conf`.

### Opis pogoste težave 6

Ob zagonu strežnika IMiS®/ARChive Server se na konzoli pojavi sporočilo:

```
[user1@iarc ~]# sudo service iarc start
Error accessing IMiS/ARChive Database directory (<pot-do-baze>). Check user iarc access to this directory
(must be rwx)
[user1@iarc ~]#
```

Strežnik je sicer omrežno dostopen:

```
[user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=4 ttl=64 time=0.183 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=5 ttl=64 time=0.164 ms

--- iarc.acme.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.164/0.450/1.530/0.540 ms
[user1@test ~]#
```

### Vzrok težave 6

Izvajalni program strežnika ne more dostopati do svoje interne baze podatkov zaradi:

- napačne nastavitve v nastavitveni datoteki `/etc/iadbprovider.xml`, sekcija `/IMiSARChive/Configuration/Database/DriverArguments/DatabaseLocation` in/ali napačno nastavljenih dostopnih pravic in/ali lastništva nad nastavljenim imenikom;
- interna baza ni dosegljiva, ker disk, na katerem se interna baza strežnika nahaja, ni povezan na pravi imenik.

### Rešitev težave 6

Preveriti je potrebno pravilnost nastavitve lokacije interne baze podatkov strežnika, določene v `/etc/iadbprovider.xml`,

Sekcija `/IMiSARChive/Configuration/Database/DriverArguments/DatabaseLocation`, če ta obstaja.

Privzeta vrednost v primeru, da te nastavitve ni v nastavitveni datoteki,

je `/iarc/db`. Preveriti je potrebno pravice in lastništva imenika in datotek znotraj imenika,

ki je naveden kot imenik, ki vsebuje datoteke interne baze podatkov. Uporabnik, ki izvaja procese strežnika (privzeto `iarc`), mora imeti pravice branja, pisanja in ustvarjanja novih datotek v tem imeniku. Skupini, kateri pripada uporabnik, ki izvaja procese strežnika (privzeto `iarc`) zadošča pravica branja.

V kolikor je imenik `/iarc` prazen, je najverjetnejši vzrok nedosegljivost diska, na katerem se po privzetih nastavitvah v imeniku `/iarc/db` sicer nahaja interna baza strežnika in je potrebno najprej zagotoviti dosegljivost tega diska.

### Opis pogoste težave 7

Po ponovnem zagonu (angl. Restart) celotnega strežnika IMiS®/ARChive Server se na odjemalcih IMiS®/Scan in IMiS®/View ob poizkusu pregledovanja objektov shranjenih na strežniku pojavi »Napaka 61523«. Drugi odjemalci (npr. IMiS®/Storage Connector) javljajo napako:

```
IMiS/ARC Client <IASession.Open> Failed to establish connection to the cluster node <10.1.1.10, 16807> (Reason: Error <TimedOut> occurred while opening network connection.).
```



Strežnik je sicer omrežno dostopen.

```
[user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=4 ttl=64 time=0.183 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=5 ttl=64 time=0.164 ms

--- iarc.acme.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.164/0.450/1.530/0.540 ms

[user1@test ~]#
```

Strežnik sicer deluje, status strežnika kot storitve pa javlja naslednje:

```
[user1@iarc ~]# sudo service iarc status
Status of IMiS/ARChive HSM Storage Server: iarc is stopped
[user1@iarc ~]#
```

### Vzrok težave 7

Zagonska skripta strežnika ni aktivirana v sekvenci za zagon strežniških servisov.

### Rešitev težave 7

Urediti je potrebno samodejni zagon strežnika kot storitve ob zagonu operacijskega sistema:

```
[user1@iarc ~]# sudo chkconfig iarc on
[user1@iarc ~]#
```

Preverimo uspešnost izvedbe ukaza:

```
[user1@iarc ~]# sudo chkconfig iarc --list
iarc      0:off 1:off 2:on 3:on 4:on 5:on 6:off [user1@iarc ~]#
```

Nato strežnik zaženemo z ukazom:

```
[user1@iarc ~]# sudo service iarc start
Starting IMiS/ARChive HSM Storage Server:      [ OK ]
[user1@iarc ~]#
```

## Opis pogoste težave 8

Ob zagonu strežnika IMiS®/ARChive Server se na konzoli pojavi izpis:

```
[user1@iarc ~]# sudo service iarc start
Starting IMiS/ARChive HSM Storage Server:
WARNING: Maximum number of file handles (ulimit -n) allowed for
user iarc or group iarc is 1024. Set allowable maximum to
at least 4096 by adding following two lines to /etc/security/limits.conf:
iarc      hard      nofile    4096
iarc      soft      nofile    4096
or
@iarc     hard      nofile    4096
@iarc     soft      nofile    4096
If you still receive this message after modifying /etc/security/limits.conf
check if Pluggable Authentication Modules (PAM) include module
pam_limits.so in session service for user iarc and/or group iarc
(see Linux-PAM system administrators guide on how to manage modules)
IMiS/ARChive will continue to run normally with current setting..
      [ OK ]
[user1@iarc ~]#
```

Storitev po zagonu sicer normalno deluje. Čez čas postane strežnik nedosegljiv za seje novih odjemalcev. V dnevniku se pojavijo zapisi:

```
<datum in ura zapisa> [iarcd:<decimalna vrednost>:<decimalna vrednost>] CRIT[2] No child process can accept
new connection.
```

## Vzrok težave 8

Strežnik je dosegel največje možno število odprtih datotek in zato ne more več sprejemati novih povezav. Vsako povezavo namreč operacijski sistem zazna kot »odprto datoteko«.

## Rešitev težave 8

Potrebno je preveriti sistemsko nastavitve največjega možnega števila odprtih datotek za uporabnika `iarc`, pod katerim strežnik teče.

V nadaljevanju so opisane težave, ki jih uporabniki in administratorji pogosto srečujejo pri delu s spletnim administracijskim vmesnikom IMiS®/wAdmin.

### **Napaka pri dostopu do arhiva - »Connection refused«**

Vzrok težave: Napaka pri odpiranju povezave do strežnika IMiS®/ARChive Server, ki je lahko posledica:

- Napačnega URL naslova.
- Nedelujočega strežnika. Strežnik IMiS®/ARChive Server ni zagnan ali pa je zaradi napake ugasnjen.
- Požarnega zidu (angl. Firewall) na spletnem administracijskem vmesniku (IMiS®/wAdmin) ali omrežju med odjemalcem in strežnikom, ki preprečuje komunikacijo odjemalcev s strežnikom.

Rešitev težave: Preveriti je potrebno veljavnost URL naslova.

V kolikor težava ni odpravljena, je potrebno preveriti ali je strežnik IMiS®/ARChive Server zagnan. Če strežnik deluje, je potrebno preveriti komunikacijo med spletnim administracijskim vmesnikom in strežnikom ter po potrebi ponovno konfigurirati požarni zid tako, da bo dovoljeval komunikacijo administracijskega vmesnika s strežnikom.

### **Napaka pri prijavi uporabnika - »Unauthorized (401)«**

Vzrok težave: Neregistrirano ali neveljavno uporabniško ime ali napačno geslo.

Rešitev težave: Preveriti je potrebno ali sta uporabniško ime in geslo pravilno podana (npr. uporaba velikih/malih črk, brez začetnih ali končnih presledkov, ... ipd.).

V kolikor to ne reši težave, je potrebno obvestiti pooblaščenega uporabnika, da preveri ali je uporabnik s tem imenom dejansko registriran na strežniku IMiS®/ARChive Server.

## **9.3 Redkejšje težave**

### Opis redke težave 1

Ob poizkusu pregledovanja objekta shranjenega na strežniku IMiS®/ARChive Server se na odjemalcu IMiS®/View ali IMiS®/Scan pojavi »Napaka 11«.

Drugi odjemalci (npr. IMiS®/Storage Connector) pri poizkusu pridobivanja objekta s strežnika dobijo naslednji odgovor:

```
OpenObject failed on object with id <id objekta>' (error: 0x564e4f56)
```

Strežnik je sicer omrežno dostopen, servis na vratih, kjer posluša, se odziva (preverjanje s telnet programom)

```
[user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data:
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=4 ttl=64 time=0.183 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=5 ttl=64 time=0.164 ms

--- iarc.acme.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.164/0.450/1.530/0.540 ms
```

```
[user1@test ~]# telnet iarc.acme.com 16807
Trying 10.1.1.10...
Connected to iarc.acme.com.
Escape character is '^]'.
Connection closed by foreign host.
[user1@test ~]#
```

Strežnik deluje, kar dodatno preverimo s konzolnim ukazom na strežniku, kjer je nameščen:

```
[user1@iarc ~]# sudo service iarc status
Status of IMiS/ARChive HSM Storage Server: iarc (pid 23209) is running...
[user1@iarc ~]#
```

### Vzrok težave 1

Odjemalec skuša odpreti objekt, ki je pravilno vpisan v interni bazi strežnika, vendar vsebina objekta ni na svojem mestu ali manjka.

### Rešitev težave 1

Potrebno je pridobiti:

- podatke o identifikatorju objekta iz aplikacije, ki arhivski sistem uporablja (npr.: 4c9f36d38b4d6985b1ec11a5a14a7e9db89edd0cb36923010b6624c667ef142);
- vsebino parametra IdentPassword iz nastavitvene datoteke strežnika /etc/iarc.conf;
- podatke o kupcu.

Vse skupaj je potrebno poslati po e-pošti na naslov: [podpora@imis.si](mailto:podpora@imis.si).

Naše tehnično osebje nato dešifrira identifikator objekta, ki je osnova za informacijo in nadaljnje postopke restavracije iz varnostnih kopij ali iskanje po datotečnem sistemu, v kolikor se ne nahaja na izvornem mestu. To je možno samo v primeru, ko ga je nekdo s pravicami upravljalca strežnika premaknil ali izbrisal iz izvornega mesta.

### Opis redke težave 2

Ob poizkusu pregledovanja objekta shranjenega na strežniku IMiS®/ARChive Server se na odjemalcih IMiS®/Scan ali IMiS®/View pojavi »Napaka pri branju IMiS objekta«. Drugi odjemalci (npr. IMiS®/Storage Connector) pri poizkusu pridobivanja objekta s strežnika dobijo naslednji odgovor:

```
Unable to locate database record for entity <decimalna vrednost>
```

Strežnik je sicer omrežno dostopen, servis na vratih, kjer posluša, se odziva (preverjanje s telnet programom)

```
[user1@test ~]# ping iarc.acme.com
PING iarc.acme.com (10.1.1.10) 56(84) bytes of data.
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=1 ttl=64 time=0.653 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=2 ttl=64 time=0.190 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=3 ttl=64 time=0.186 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=4 ttl=64 time=0.183 ms
64 bytes from iarc.acme.com (10.1.1.10): icmp_seq=5 ttl=64 time=0.164 ms

--- iarc.acme.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.164/0.450/1.530/0.540 ms
```

```
[user1@test ~]# telnet iarc.acme.com 16807
Trying 10.1.1.10...
Connected to iarc.acme.com.
Escape character is '^]'.
Connection closed by foreign host.
[user1@test ~]#
```

Strežnik deluje, kar dodatno preverimo s konzolnim ukazom na strežniku, kjer je nameščen:

```
[user1@iarc ~]# sudo service iarc status
Status of IMiS/ARChive HSM Storage Server: iarc (pid 23209) is running...
[user1@iarc ~]#
```

### Vzrok težave 2

Odjemalec skuša odpreti objekt, ki ni vpisan v interni bazi strežnika.

### Rešitev težave 2

Potrebno je pridobiti:

- podatke o identifikatorju objekta iz aplikacije, ki arhivski sistem uporablja (npr.: 4c9f36d38b4d6985b1ec111a5a14a7e9db89edd0cb36923010b6624c667ef142);
- vsebino parametra IdentPassword iz nastavitvene datoteke strežnika  
/etc/iarc.conf;
- interno podatkovno bazo (vsebino imenika /iarc/db ) v stisnjeni obliki ali njeno tekstualno obliko;
- podatke o kupcu.

Vse skupaj je potrebno poslati po e-pošti na naslov: [podpora@imis.si](mailto:podpora@imis.si).

Naše tehnično osebje nato dešifrira identifikator objekta, ki je osnova za informacijo in nadaljnje postopke ugotavljanja stanja interne podatkovne baze in vzroka za izpad zapisa, ki je osnova za pravilne operacije z objektom v inventarju strežnika.

## 9.4 Seznam napak storitve, ki se beležijo v dnevnik delovanja

### 9.4.1 Nivo 0 – Emergency

EMERG: »Unknown exception caught.«

EMERG: Exception caught <opis>

Napaka se zgodi v primeru, ko pride do težke napake pri delovanju strežnika IMiS®/ARChive Server, ki pa ni evidentirana oziroma predvidena kot možna napaka.

Razlogi so različni: od stanja okolja do morebitnih napak v aplikacijski kodi storitve.

### 9.4.2 Nivo 1 – Alert

ALERT: »Unhandled error will cause current thread to exit. Details: <opis napake>«

ALERT: »Unknown unhandled error will cause current thread to exit«

Napaka pomeni, da je na strežniku IMiS®/ARChive Server prišlo do napake, ki se ni pravilno obdelala. Nit, v kateri je prišlo do neobdelane napake se bo končala. Če se napaka ponovi v drugih nitih lahko privede do ohromitve storitve (angl. Denial of service).

ALERT: »Error opening configuration file«

Do napake lahko pride ob zagonu strežnika IMiS®/ARChive Server v primeru, ko konfiguracijska datoteka `iarc.conf` ni dostopna, posledično zagon strežnika ni mogoč.

### 9.4.3 Nivo 2 – Critical

CRIT: »Server is unable to log audit logging configuration changes. Reason: '<opis napake>'. Terminating process.«

Napaka pomeni, da strežnik IMiS®/ARChive Server ne more zapisati sprememb konfiguracije profilov revizijske sledi v revizijsko sled.

CRIT: »Locale parameter '<vrednost>' for LC\_ALL is not formatted according to POSIX standard and cannot be used. Use format II CCI.CHARSET[@variant]]«.

CRIT: Cannot set environment variable "LC\_ALL" value to "<vrednost>" which is required.

CRIT: Cannot initialize LC\_ALL locale setting to "<vrednost>".

CRIT: Cannot initialize LC\_ALL locale setting in std and boost namespace to "<vrednost>".

Strežnik IMiS®/ARChive Server ne more nastaviti zelenih regionalnih nastavitev za razvrščanje in prevajanje znakov, ki presegajo obseg ACSII kodne tabele. V kolikor je nastavev ena izmed ponujenih, ko izvedemo ukaz `locale -a`, je napaka zgolj teoretična.

CRIT: »Failed to daemonize process (error '<številka napake>')«

Napaka pomeni, da se strežnik IMiS®/ARChive Server ni uspel pognati kot zaledni proces, posledično delovanje strežnika ni mogoče.

CRIT: »Signal SIGSEGV/SIGABRT occurred. Process will shut down...«

Pri delu z delovnim spominom strežnika IMiS®/ARChive Server je prišlo napake. Strežnik takoj prekine z delom. Potreben je poseg administratorja strežnika, navadno ponoven zagon storitve.

#### **9.4.4 Nivo 3 – Error**

Zaradi velikega števila napak, ki se lahko pojavijo na strežniku, so v nadaljevanju opisana le nekatera najpogostejša opozorila, ki se zapišejo v strežniški dnevnik med delovanjem IMiS®/ARChive Server.

ERR: »Unknown ObjectID version information.«

ERR: »Error '<številka napake>' while cyphering internal block«

ERR: »Error '<številka napake>' while deciphering external block«

ERR: »Entity id consistency check failed (1st server id '<id strežnika>' is invalid)«

ERR: »Entity id consistency check failed (2nd server id '<id strežnika>' is invalid)«

Odjemalec je zahteval objekt, katerega struktura identifikatorja strežniku IMiS®/ARChive Server ni znana, ga ne more dešifrirati ali ga nima evidentiranega v svoji interni bazi. Zahtevo odjemalca strežnik zavrže.

ERR: »RemoveObject failed on object with id '<id objekta>' (error: <koda napake>).«

Strežnik IMiS®/ARChive Server je prejel regularno zahtevo za brisanje objekta, vendar brisanje ni izvedljivo. Potreben je poseg strokovnjaka izdelovalca programske opreme za razrešitev vprašanja, zakaj postopek izbrisa ni možen (navadno vzrok zaradi pravic nad datotečnim sistemom in datotekami HSM inventarja).

ERR: »OpenObject failed on object with id '<id objekta>' (error: <koda napake>).«

Pri poizkusu branja objekta je prišlo do napake. IMiS®/ARChive Server objekta ne more odpreti. Potreben je poseg strokovnjaka izdelovalca programske opreme, saj gre za objekt, ki je sicer vpisan v inventar objektov vendar ostaja vprašanje, zakaj postopek ni možen (navadno vzrok zaradi pravic nad datotečnim sistemom in datotekami HSM inventarja)



ERR: »Not enough space on storage profile '<ime profile>'. Required '<velikost>' bytes.

Na volumnih, ki pripadajo profilu <id profila> je zmanjkalo prostora.

ERR: »Storage profile with id '<id profila>' does not exist.«

V zahtevi odjemalca je bila uporabljena napačna ali neobstoječa številka profila.

ERR: »Unexpected FIN (status '<status seje>')«

Odjemalec IMiS® je nepričakovano zaključil sejo ali pa je poslal signal za zaključek seje po tem, ko je zaradi neaktivnosti sejo zaključil že strežnik IMiS®/ARChive Server sam.

ERR: »Error in ConnInfoGetLib request (req->seq). Processing skipped.«

ERR: »Error in ConnInfoGetLib request, IACxLibsBroker not initialized or invalid value for 'req->seq'. Processing skipped.«

Odjemalec IMiS® je strežniku IMiS®/ARChive Server poslal nepravilno zahtevo za komunikacijsko knjižnico.

ERR: »Cannot open file <ime knjižnice>.«

Odjemalec IMiS® je strežniku IMiS®/ARChive Server poslal pravilno zahtevo za komunikacijsko knjižnico, vendar te ni na svojem mestu. Napaka navadno pomeni nepopolno namestitvev, napačno nastavitvev v nastavitveni datoteki /etc/iarc.conf ali problem pravic za uporabnika iarc.

ERR: »Unknown transmission handle.«

ERR: »Unknown transmission handle <ročica>«

Operacijski sistem je strežniku IMiS®/ARChive Server posredoval neregularno ročico vozla (i-node) povezave. Napaka je najverjetneje posledica napačnega delovanja operacijskega sistema.

ERR: »Unknown ConnInfo request: <koda> - ignoring!«

Strežnik IMiS®/ARChive Server je prejel neregularno zahtevo za podatke o povezavi z odjemalcem. Zahtevo strežnik zavrže.

ERR: »Invalid request size: <velikost zahtevka>.«

Strežnik IMiS®/ARChive Server je prejel zahtevek, katerega velikost ni regularna.

Zahtevo strežnik zavrže kot neveljaven.

ERR: »Unknown request <koda zahtevka> received. Closing connection.«

Strežnik IMiS®/ARChive Server je prejel neregularen zahtevek in zaprl odprto povezavo.

Največkrat je to posledica poizkusa vzpostavitve povezave preko TCP vrat strežnika s strežniku nepoznanim protokolom.

ERR: »Invalid audit query size <decimalna vrednost>«

ERR: »Invalid sess cond.type (<decimalna vrednost>)«

ERR: »Invalid sess cond.offset (<decimalna vrednost>)«

ERR: »Invalid ts cond.offset (<decimalna vrednost>)«

ERR: »Invalid objid cond.offset (<decimalna vrednost>)«

ERR: »AuditQuery::GetNextAddress(), line <decimalna vrednost>, error <decimalna vrednost>«

Strežnik je prejel zahtevek za iskanje po revizijski sledi, ki ima neveljavno strukturo. Vzrok za napako je nepravilno delovanje odjemalca, napaka je sicer zgolj teoretična.

ERR: »Error closing file descriptor.«

Prišlo je do systemske napake pri zapiranju datoteke. Napaka je navadno posledica napake programerja, vzrok zanjo pa je lahko tudi nepravilno delovanje operacijskega sistema.

ERR: »mkstemp("<ime datoteke>") error <koda napake>.«

ERR: »Error generating temporary file from template '<ime datoteke>' (error <koda napake>)«

Prišlo je do napake pri ustvarjanju začasne datoteke z imenom <ime datoteke>. Napaka je navadno posledica pomanjkanja prostora na disku, pravic uporabnika iarc, lahko pa je tudi posledica nepravilnega delovanja operacijskega sistema.

ERR: »unlink("<ime datoteke>") error <koda napake>.«

ERR: »Error <koda napake> while deleting cache file '<ime datoteke>'«

ERR: »File '<ime datoteke>' failed to remove (error '<koda napake>')«

ERR: »Error removing temporary file '<ime datoteke>' (error <koda napake>)«

Prišlo je do napake pri brisanju datoteke z imenom <ime datoteke>.

Napaka je lahko posledica napake v programu, verjetneje pa gre za napako pravic dostopa za uporabnika iarc ali nepravilno delovanje operacijskega sistema.

ERR: »User '<uporabnik>' at connection <število> denied due to authentication failure - Authentication request sequence mismatch (request subid:proto:stage = COPN CLIAUTH:SRP6A:<število>, valid COPN CLIAUTH:SRP6A:<število>, session stage = <število>);«

ERR: »Error creating server SRPC-6a evidence for user '<uporabnik>'. Connection <število> denied (reason: <razlog>).«

ERR: »Connection <število> denied due to authentication failure - Authentication request sequence mismatch (request subid:proto:stage = COPN CLIAUTH:SRP6A:<število>, valid COPN CLIAUTH:SRP6A:[<število>/<število>], session stage = <število>);«

ERR: »Connection <število> denied (reason: Unknown Authentication mode requested (id = <število>))«

Napaka pri avtentikaciji uporabnika. Razlogi so različni, od posredovanja napačnih poverilnic do (redko) napačne uporabe avtentikacijskega protokola. Dostop takšnim sejam je zavrnjen.

ERR: »Error opening archive.«

ERR: »Error opening archive. Reason: '<opis napake>'«

Napaka pri odpiranju arhiva. Najverjetnejši razlog je napaka v podatkih ali nekonsistenca nastavitvev arhiva. V primeru napake je potreben pregled strokovnjaka proizvajalca.

ERR: »Access mode '<način dostopa>' is unsupported.«

ERR: »Unsupported access mode '<način dostopa>'«

V zahtevi je določen neveljaven način dostopa. Dovoljeni vrednosti sta: »RO« in »RW«.

Napaka na odjemalcu IMiS®/wClient.

ERR: »ACL entry for '<entiteta imenika>' is internal and cannot be updated.«

Prepovedano spreminjanje liste dostopnih pravic na sistemskih entitetah imenika.

ERR: »Address '< omrežni naslov>' structure is not supported.«

Napačen format omrežnega naslova. Vpisati je potrebno ali veljavno ime gostitelja, veljaven IPv4 naslov ali veljaven IPv6 naslov z opsijskim dodatkom omrežnih vrat. Ločilo med omrežnim naslovom in omrežnimi vrati je znak »:«.

Napaka pri nastavitvi produkta.

ERR: »Attribute 'destination' contains the value '%s' which resolves to an unknown attribute«

ERR: »Attribute 'destination' identifies the attribute '%s' which type '%u' is not supported for entity identification storage«

Napaka pri nastavitvi števecv za samodejno številčenje entitet.

ERR: »Binary, File and StringMax are unsortable.«

Razvrščanje atributov tipa »Binary«, »File« in »StringMax« ni mogoče.

Napačna uporaba funkcionalnosti sortiranja na odjemalcu IMiS®/wClient.

ERR: »Both IP addresses need to be of the same length and same protocol.«

Napaka pri določanju razpona IP naslovov iz zahteve za vpogled v revizijsko sled.

Obe strani razpona morata biti iste družine. Napačno posredovana vrednost razpona iz odjemalca IMiS®/wClient.

ERR: »Can't move an entity into its own subtree.«

Premik entitete v lastno vsebovano entiteto ni mogoč.

ERR: »Collection handle '<šestnajstiška vrednost>' is invalid.«

Referenca (handle) na zbirko je neveljavna. Napaka na odjemalcu IMiS®/wClient.

Možni razlogi za napako so:

- Zbirka je bila predhodno zaprta.
- Seja iz katere izvira referenca je bila zaprta in ponovno odprta nova seja.
- Referenca ni nikoli obstajala.

ERR: »Username for session required but not provided.«

ERR: »Computer name for session required but not provided.«

ERR: »Private Address for session required but not provided.«

ERR: »Audit log message is required but missing or empty.«

Strežnik IMiS®/ARChive Server je nastavljen tako, da pri zapisu revizijske sledi zahteva obvezne podatke, kot so uporabniško ime, ime računalnika, interni IP naslov ali razlog za izvedbo dane operacije. Če kateri izmed obveznih podatkov ni prisoten, se izvedba operacije zavrne.

Napaka je bodisi v nastavitvah strežnika ali pa na strani odjemalca IMiS®/wClient, ki ne pošilja zahtevanih podatkov.

ERR: »Decrypted Authentication payload starting sequence is invalid.«

Napaka pri avtentikaciji. Napaka na odjemalcu IMiS®/wClient.

ERR: »Destination is already a parent of the specified entity. Move is not possible.«

Premik ne spremeni umestitve entitete v načrtu razvrščanja gradiva in posledično ni smiseln.

Premik se ne izvede. Napaka na odjemalcu IMiS®/wClient.

ERR: »Element count must be greater than 0.«

Število elementov na strani zbirke entitet mora biti pozitivno število. Napaka na odjemalcu IMiS®/wClient.

ERR: »Encoding (<število>) not recognized.«

Zahtevano šifriranje (encoding) za enolične oznake entitet v rezultatu poizvedbe revizijske sledi ni bilo prepoznano. Dovoljene vrednosti so 1 (BASE 16), 2 (BASE 64) in 3 (BASE 85).

ERR: »Entity handle '<šestnajstiško število>' is invalid.«

ERR: »Entity handle is invalid.«

Referenca (handle) na entiteto je neveljavna. Napaka na odjemalcu IMiS®/wClient.

Možni razlogi za napako so:

- Entiteta je bila predhodno zaprta.
- Seja iz katere izvira referenca je bila zaprta in ponovno odprta nova seja.
- Referenca ni nikoli obstajala.

ERR: »Entity handle is invalid or you're trying to open a binary object in read-write mode while the parent entity is opened in read-only mode.«

Referenca ni veljavna (za zgornji opis napake (glej [Entity handle is invalid.](#)) ali poizkus odprtja binarnega objekta v načinu za pisanje, čeprav je nadrejena entiteta odprta v načinu za branje.

ERR: »Entity handle must be provided.«

Zahteva brez reference na entiteto ni veljavna. Napaka na odjemalcu IMiS®/wClient.

ERR: »Entity id type cannot be NONE.«

Tip enoličnega identifikatorja entitete v zahtevku ne sme biti N (NONE).

Dovoljene vrednosti so I (šifriran interni), E (eksterni) ali C (klasifikacijska oznaka).

Napaka na odjemalcu IMiS®/wClient.

ERR: »Entity identifier not specified.«

ERR: »Entity unique identifier (id or handle) must be provided.«

Zahteva ne vsebuje veljavnega enoličnega identifikatorja entitete.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Entity type '<tip>' is unknown.«

Zahteva ne vsebuje veljavnega tipa entitete. Dovoljene vrednosti so C (razred), F (zadeva) in D (dokument). Napaka na odjemalcu IMiS®/wClient.

ERR: »Entity type '<število>' is not a valid template entity type.«

ERR: »Template enumeration type '<število>' is not a valid entity type.«

Predloga vsebuje neveljavno vrednost tipa entitete, ki jo opisuje. Dovoljene vrednosti so v razponu od 1 do 5. Napaka na odjemalcu IMiS®/wClient.

ERR: »Error converting IP address«

Napaka pri pretvorbi znakovnega niza v veljaven IP naslov. Napaka na odjemalcu IMiS®/wClient.

ERR: »Exactly 2 id tags are required in mv request.«

Zahteva za premik mora vsebovati natančno dve enolični oznaki entitete.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Insufficient rights to create file property in the specified entity.«

ERR: »Insufficient rights to create subentities in the destination entity.«

ERR: »Insufficient rights to create subentities under the specified parent.«

Uporabnik nima pravice izvesti zahtevane operacije. Če bi uporabnik moral imeti pravico izvajanja operacije je potrebno preveriti listo dostopnih pravic in jo po potrebi spremeniti.

ERR: »Invalid date part (<manjkajoči parameter>).«

ERR: »Invalid date part.«

ERR: »Invalid time part <manjkajoči parameter>).«

ERR: »Invalid time part.«

ERR: »Invalid times-tamp.«

ERR: »Date value '<datum>' cannot be converted to timestamp parts. Reason: '<opis napake>'«

ERR: »Time value '<čas>' cannot be converted to timestamp parts. Reason: '<opis napake>'«

Napaka pri pretvorbi znakovnega niza v datum/čas.

ERR: »Invalid old password.«

ERR: »New password is required but missing or empty.«

ERR: »Old password is required but missing or empty.«

Napaka pri spremembi gesla. Možnih je več vzrokov:

- Staro geslo ni pravilno.
- Staro geslo ali novo geslo nista podani.

Napaka je na odjemalcu IMiS®/wClient.

ERR: »Invalid property scope '<znak>' requested.«

Neveljavna vrednost za obseg vrnjenih atributov v »rd« zahtevi. Veljavne vrednosti so:

N (ne vračaj), S (naštete), A (vse) in P (javne). Napaka na odjemalcu IMiS®/wClient.

ERR: »Invalid tag %u.«

ERR: »Invalid tag name %u.«

Napaka pri izvajanju zahteve. Neveljavna XML etiketa.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Invalid value id '<število>' cannot be opened.«

Neveljaven identifikator vrednosti binarne vsebine.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Invalid XML request: Unknown root tag '<ime>' found.«

Neznana korenska etiketa (root tag) v zahtevi.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Invalid/Unsupported key type '<identifikator>'.«

Nepodprt tip avtentikacijskega ključa.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Malformed classification code '<koda>' (<napaka>).«

Nepravilno oblikovana klasifikacijska oznaka.

ERR: »Malformed counter definition '%s'.«

Nepravilna konfiguracija števca ustvarjanja klasifikacijske oznake.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Malformed expression '%s'.«

Nepravilen izraz v tabeli šifrantov. Napaka v konfiguraciji.

ERR: »Newly created Binary object identified by '%llu' was not created from this session and cannot be assigned to the property '%s'.«

ERR: »Newly created Binary object identified by '%llu' was not created from this session.«

V zahtevi je posredovan neveljaven identifikator binarnega objekta.

Napaka na odjemalcu IMiS®/wClient.

ERR: »No legacy archival configuration for profile '%s'«

Arhivski profil ni vključen v konfiguracijo za arhiviranje.



ERR: »Page element count '<število elementov>' exceeds maximum allowed size of '< število elementov >' elements.«

Število elementov na strani zbirke entitet mora biti manjše od najvišjega dovoljenega števila elementov (10000). Napaka na odjemalcu IMiS®/wClient.

ERR: »Parent required but not specified.«

Zahteva mora vsebovati enolično identifikacijsko številko nadrejene entitete, pod katero se ustvari nova entiteta. Napaka na odjemalcu IMiS®/wClient.

ERR: »Property '<ime atributa>' is not a streamable property.«

Napačen tip atributa. Podatkovni tok je mogoč samo na atributih tipa »Binary«, »File« in »StringMax«. Napaka na odjemalcu IMiS®/wClient.

ERR: »Malformed boolean value '<vrednost>'.«

Nepravilna vrednost binarnega atributa na zahtevi. Dovoljene vrednosti so 0, 1, true ali false. Napaka na odjemalcu IMiS®/wClient.

ERR: »Property name must be provided.«

Zahteva mora vsebovati ime atributa. Napaka na odjemalcu IMiS®/wClient.

ERR: »Provided client application name contains invalid UTF-16 characters.«

Ime odjemalca v zahtevi vsebuje nedovoljen UTF-16 znak. Napaka na odjemalcu IMiS®/wClient.

ERR: »Provided client local address '<IP naslov>' cannot be converted into its binary form (Detail: <opis napake>)«

Napaka pri pretvorbi internega IP naslova. Navadno označuje napačno obliko posredovanega naslova. Napaka na odjemalcu IMiS®/wClient.

ERR: »Provided client local address contains invalid UTF-8 characters.«

Odjemalčev lokalni IP naslov v zahtevi vsebuje nedovoljen UTF-8 znak.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Provided computer name contains invalid UTF-16 characters.«

Ime uporabnikovega računalnika v zahtevku vsebuje nedovoljen UTF-16 znak.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Provided username contains invalid UTF-16 characters.«

Uporabniško ime v zahtevi vsebuje nedovoljen UTF-16 znak.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Reason for deletion required but missing or empty.«

Uporabnik mora obvezno podati razlog za brisanje. Napaka na odjemalcu IMiS®/wClient.

ERR: »Server was unable to decrypt authentication payload using any configured crypto contexts.«

Težava pri avtentikaciji na starem vmesniku, saj ni bilo mogoče dešifrirati avtentikacijskega paketa. Napaka na odjemalcu IMiS®/wClient.

ERR: »Start index '<začetni indeks>' exceeds collection element count '<število elementov>'.«

Neveljaven začetni indeks na zbirki. Začetni indeks ne sme biti višji od števila elementov v zbirki.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Template '<ime>' is internal and cannot be used.«

Uporaba internih predlog ni dovoljena. Napaka na odjemalcu IMiS®/wClient.

ERR: »The password is not encoded in correct UTF-8 sequence.«

Geslo ni veljaven UTF-8 znakovni niz. Napaka na odjemalcu IMiS®/wClient.

ERR: »The SRP6A group you provided is not supported (id=<število>).«

SRP6A skupina ni podprta.

ERR: »Timestamp must be a range.«

Zahteva za poizvedbo po revizijski sledi mora obvezno vsebovati časovni razpon iskanih zahtevkov. Napaka na odjemalcu IMiS®/wClient.

ERR: »Unable to make query without any parameters.«

Zahtevek za poizvedbo po revizijski sledi mora obvezno vsebovati vsaj en parameter.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Unable to search objects by object id range.«

ERR: »We cannot have ranges of objects«

Zahteva za poizvedbo po revizijski sledi ne sme vsebovati razpona po enoličnih oznakah objekta.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Unknown collection management operation '<znak>'«

Zahteva vsebuje nedovoljeno vrednost za upravljanje z zbirko. Dovoljeni vrednosti sta C (briši zbirko) in I. Napaka na odjemalcu IMiS®/wClient.

ERR: »Unknown property '<ime atributa>'«

ERR: »Unknown property code '<ime atributa>'«

Atribut ne obstaja. Napaka na odjemalcu IMiS®/wClient.

ERR: »Unknown stream handle (<šestnajstiško število>). Ignoring request.«

Nepravilna referenca na podatkovni niz. Napaka na odjemalcu IMiS®/wClient.

ERR: »Unknown value id '<število>' requested or error opening a stream.«

Neveljaven identifikator vrednosti binarne vsebine. Napaka na odjemalcu IMiS®/wClient.

ERR: »Unknown XML Parser error.«

Neznana napaka pri procesiranju XML zahteve. Napaka na odjemalcu IMiS®/wClient.

ERR: »Unknown xml tag encountered: '<število>'«

ERR: »Unknown xml tag encountered: '<string>'«

Pri procesiranju XML zahteve se je pojavila nepoznana XML etiketa.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Unsupported object id size.«

Za šifrirane enolične oznake entitete sta dovoljeni samo dve dolžini: 24 in 32 znakov.

Napaka na odjemalcu IMiS®/wClient.

ERR: »XML Parser error: domain=%d, code=%d, msg='%s', level='%s', line=%d«

Težava pri procesiranju XML zahteve. Napaka na odjemalcu IMiS®/wClient.

ERR: »You cannot create a <tip entitete> from template '<ime predloge>' (Reason: Template is not of type <tip entitete>).«

Predloge ni mogoče uporabiti na danem tipu entitete.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Unable to open the listening port on address '['<naslov>]:<port>' (Reason: '<razlog>').«

ERR: »Unable to bind the listening socket to address '['%s]:%u' (Reason: '%s').«

Napaka pri odpiranju omrežnega naslova za serviranje zahtevkov. Razlog je naveden v sporočilu »Reason«.

ERR: »Access denied. System entities can not be opened.«

Operacija »odpri« na sistemski entiteti ni dovoljeno.

ERR: »Classification code cannot be set for existing entities.«

Spreminjanje klasifikacijske oznake na obstoječi entiteti ni dovoljeno.

ERR: »Classification code is set to be generated automatically.«

Klasifikacijska oznaka se ustvari samodejno. Ročno nastavljanje ni dovoljeno.

ERR: »Invalid stream object for CS OBJ UPDATE request.«

Neveljavna zahteva za odpiranje podatkovnega toka (angl. Stream) na starem vmesniku.

ERR: »Invalid CS OBJ CREATE request packet size: <dolžina>.«

ERR: »Invalid CS OBJ OPEN request packet size: '<dolžina>'.«

ERR: »Invalid CS OBJ UPDATE request packet size: '<dolžina>'.«

ERR: »Invalid CS OBJ REMOVE request packet size: '<dolžina>'.«

Neveljavna dolžina zahtevka na starem vmesniku.

ERR: »<ime atributa>' property not found.«

Atribut ne obstaja.

ERR: »Default storage profile is not set.«

Napaka v nastavitvi. Potrebno je določiti privzeti arhivski profil.

ERR: »Storage profile '<oznaka>' doesn't exist.«

Napaka v nastavitvi. Arhivski profil z dano oznako ne obstaja.

ERR: »Error acquiring an instance of Full Text Index Service provider.«

Napaka v nastavitvah servisa za iskanje po celotnem besedilu.

ERR: »Classification code is set to be generated automatically but generator is not configured for the entity's hierarchy level.«

Napaka v nastavitvi. Samodejno ustvarjanje klasifikacijskih oznak ni nastavljeno za vse nivoje v načrtu razvrščanja gradiva.

ERR: »Classification code must be set to be generated automatically for the destination entity's subentities.«

ERR: »Classification code must be set to be generated automatically for the whole moving entity's hierarchy.«

ERR: »Missing classification code generator. Entity type: '<tip entitete>', Absolute level: <nivo>, Relative level: <nivo>.2

Napaka v nastavitvah. Operacija premik obvezno potrebuje nastavljeno samodejno ustvarjanje klasifikacijskih oznak na ciljnem drevesu.

ERR: »Non-empty entities cannot be deleted.«

Brisana entiteta ne sme vsebovati vsebovanih entitet. Najprej je potrebno izbrisati vsebovane entitete.

ERR: »Entity '<id>' cannot be opened in exclusive mode.«

Entiteta je že odprta v načinu za pisanje v neki drugi seji.

ERR: »Value '<id>' is currently being edited. Close all editable streams before opening a new one.«

ERR: »Value '<id>' is currently being edited through stream '<referenca streama>'. Close it before opening a new one.«

Atribut tipa podatkovni tok je že odprt za pisanje.

ERR: »Closed entities cannot be edited.«

Status dotične entitete (ali nadrejene) je »Closed«. Kakršno koli spreminjanje zaprte entitete ni dovoljeno.

ERR: »Access denied. Request requires user-credentials authenticated session or higher.«

Za izvajanje želene operacije je potrebno vzpostaviti sejo z avtentikacijo.

ERR: »Adding new entities under closed entities is not allowed.«

Status dotične entitete (ali nadrejene) je »Closed«. Dodajanje novih vsebovanih entitet pod zaprto entiteto ni dovoljeno.

ERR: »Destination status is 'Closed'. Adding new entities under it is not allowed.«

Kakršnokoli spreminjanje entitete s statusom »Closed« je prepovedano. To vključuje tudi dodajanje novih vsebovanih entitet.

ERR: »Access denied. (You do not have the right to delete the property '<ime>')«

Uporabnik nima pravice brisanja atributov na entiteti.

ERR: »Access denied. (You do not have the right to create the property '<ime>')«

Uporabnik nima pravice dodajanja atributov na entiteti.

ERR: »Access denied. (You do not have the right to edit the property '<ime>')«

Uporabnik nima pravice spreminjanja vrednosti atributov na entiteti.

ERR: »Query result set is to large. Try to decrease datetime range.«

Rezultat poizvedbe revizijske sledi zajame več rezultatov kot jih je sistem zmožen obdelati. Spremeniti je potrebno parametre iskanja, da bo vrnjenih manj rezultatov. Najlažje se to stori z zmanjšanjem časovnega razpona iskanih dogodkov.

ERR: »Binary transfer operations on draft are not allowed.«

Premik vsebine iz osnutka ali v osnutek entitete ni dovoljen.

ERR: »Operation is not allowed because entity '<identifikator>' is used in another binary transfer/manage operation.«

Večkratne operacije na vsebini entitete niso dovoljene. Pred začetkom izvajanja druge operacije je potrebno najprej končati tekočo operacijo,.

ERR: »Operation is not allowed because action value bits and action value are missing.«

ERR: »Operation is not allowed because action value bits and action value are present (only one value is allowed).«

Izvedba operacije nad vsebino entitete ni mogoča, saj manjkajo informacije o operaciji, ali pa je informacija o operaciji poslana po starem in novem formatu, kar pa ni dovoljeno.

Napaka na odjemalcu IMiS®/wClient.

ERR: »Reason for classification code change is required but is missing or empty.«

Razlog je obvezen parameter pri Izvedbi operacije zamenjave klasifikacijske oznak.

ERR: »Changing classification code is not possible because parent classification code configuration does not allow it.«

Zamenjava klasifikacijske oznake ni mogoča, saj konfiguracija nadrejene entitete preprečuje, da bi se klasifikacijska oznaka zamenjala.

#### **9.4.5 Nivo 4 – Warning**

Zaradi velikega števila opozoril, ki se lahko pojavijo na strežniku, so v nadaljevanju opisana le nekatera najpogostejša opozorila, ki se zapišejo v strežniški dnevnik med delovanjem strežnika IMiS®/ARChive Server.

WARN: »Error authenticating request from [<ip naslov>] using Basic HTTP authentication.

Reason: <opis napake>«

WARN: »Error authenticating request from [<ip naslov>] using Basic HTTP authentication.

Reason: <opis napake>«

WARN: »Internal error authenticating request from [<ip naslov>] using Basic HTTP authentication.«

WARN: »Error authenticating request from [<ip naslov>] using Digest HTTP authentication.

Reason: <opis napake>«

WARN: »Error authenticating request from [<ip naslov>] using Digest HTTP authentication.

Reason: <opis napake>«

WARN: »Internal error authenticating request from [<ip naslov>] using Digest HTTP authentication.«

Pri poskusu prijave uporabnika na administracijski modul strežnika IMiS®/ARChive Server je prišlo do napake (najverjetneje napačno uporabniško ime ali geslo).

WARN: »AAAConfiguration: Unable to parse initialization data. Reason: '<opis napake>'«

WARN: »AAAConfiguration: Unable to address required 'AAAConfiguration' node. Reason: '<opis napake>'«

WARN: »User field value '<vrednost>' is not present in a list of supported fields, skipping...«

WARN: »'SyncUserFields' tag is missing in AAA directory configuration '<id uporabnika ali skupine>', all fields will be used for synchronization«

WARN: »'SyncGroupFields' tag is missing in AAA directory configuration '<id uporabnika ali skupine>', all fields will be used for synchronization«

WARN: »Group field value '<vrednost>' is not present in a list of supported fields, skipping...«

Opozorila se pojavijo ob inicializaciji konfiguracije za avtentikacijo in avtorizacijo strežnika IMiS®/ARChive Server. Ne gre za kritične napake, vendar je priporočljivo, da konfiguracijo pregleda strokovnjak proizvajalca.

WARN: »AuditLogConfiguration: Attribute '<ime atributa>' missing. Using default value of '<vrednost>'...«

WARN: »AuditLogConfiguration: Attribute's '<ime atributa>' value is empty. Using default value of '<vrednost>'...«

WARN: »AuditLogConfiguration: Attribute's '<ime atributa>' value '<vrednost>' does not translate to a valid boolean value. Using default value of '<vrednost>'...«

WARN: »Audit log profile '<id profila>' contains node '<ime>' which is not recognized, ignoring...«

WARN: »Global audit log does not have scope and/or template filters, ignoring...«

WARN: »Global signature node is missing, state of all profiles will be serialized to audit log«

WARN: »Error occurred while resolving scope entity '<tip>' '<identifikator>' for audit log profile '<id profila>'. Reason: '<opis napake>'«



WARN: »Template '<ime\_predloge<' cannot be found in template map and will not be used as template filter on audit log profile '<id\_profila>'

Opozorila se pojavijo ob inicializaciji konfiguracije za revizijsko sled. Ne gre za kritične napake, vendar je za pravilno delovanje zapisa revizijske sledi potreben pregled strokovnjaka proizvajalca.

WARN: »CertificateStoreConfiguration: Configuration not found, default settings will be used«

WARN: »CertificateStoreConfiguration: Proxy port value '<vrednost>' is invalid (reason: '<opis napake>'), skipping...«

WARN: »CertificateStoreConfiguration: Unknown configuration parameter '<ime>' encountered. Skipping...«

WARN: »CertificateStoreConfiguration: Missing attribute '<ime>' from '<ime>' tag. Skipping...«

WARN: »CertificateStoreConfiguration: Unknown configuration parameter '<ime>' encountered. Skipping...«

Opozorila se pojavijo ob inicializaciji konfiguracije shrambe digitalnih potrdil. Ne gre za kritične napake, vendar je za pravilno delovanje shrambe digitalnih potrdil in odjemalca za pridobivanje podatkov o preklicih potreben pregled strokovnjaka proizvajalca.

WARN: »ContentConfiguration: <opis napake>«

WARN: »ContentConfiguration[Filter]: <opis napake>«

WARN: »ContentConfiguration[Filter/Mime]: <opis napake>«

WARN: »ContentConfiguration[FullTextIndex]: <opis napake>«

WARN: »ContentConfiguration[DigitalSignature/Verification]: <opis napake>«

WARN: »ContentConfiguration[Parser]: <opis napake>«

WARN: »ContentConfiguration[Converter]: <opis napake>«

WARN: »Converter: <opis napake>«

Opozorila se pojavijo ob inicializaciji konfiguracije za obdelavo vsebine. Ne gre za kritične napake, vendar je za pravilno delovanje sistema za upravljanje z vsebinami (indeksiranje, pretvorba, preverjanje digitalnih podpisov, ... ) potreben pregled strokovnjaka proizvajalca.

WARN: »Configuration[LegacyArchival/Traverse]: <opis napake>«

WARN: »Configuration[LegacyArchival/ObjectContainer]: <opis napake>«

WARN: »Configuration[LegacyArchival/MimeAlias]: <opis napake>«

WARN: »Legacy Archival option DISABLED. Reason: '<opis napake>'«

Opozorila se pojavijo ob inicializaciji konfiguracije za starejše odjemalce. Ne gre za kritične napake, vendar je za pravilno delovanje starejših odjemalcev potreben pregled strokovnjaka proizvajalca.

WARN: »FullTextIndexAsioJob[QueueWorker]: <opis napake>«

WARN: »FullTextIndexService[QueueWorker]: <opis napake>«

Opozorila se pojavijo v primeru napak pri indeksiranju vsebine. Taka vsebina posledično ne bo dostopna pri iskanju po vsebini. Za razrešitev napake je potreben pregled strokovnjaka proizvajalca.

WARN: »Configuration[EntityIdentification]: <opis napake>«

WARN: »Configuration[EntityIdentification/Identifier]: <opis napake>«

WARN: »Configuration[EntityIdentification/LevelDelimiter]: <opis napake>«

Opozorila se pojavijo v primeru napak pri inicializaciji števecv za samodejno ustvarjanje klasifikacijskih oznak. Za vzpostavitev pravilnega delovanja števecv je potreben pregled strokovnjaka proizvajalca.

WARN: »No listening ports activated for Administration requests. Service disabled.«

WARN: »No listening ports activated for Client I/O requests. Service disabled.«

Opozorilo se pojavi pri zagonu strežnika v primeru napačne konfiguracije v datoteki iarc.conf ter posledično onemogočenim administracijskim servisom ali servisom za odjemalce.

Za vzpostavitev pravilnega delovanja je potrebno popraviti konfiguracijo ter ponovno zagnati strežnik IMiS®/ARChive Server.

WARN: »User '<uporabniško ime>' from '<ime računalnika>' did not authenticate with Audit Log Query permissions. Query denied.«

Opozorilo se pojavi v primeru, ko hoče uporabnik izvesti vpogled v revizijsko sled, vendar nima pravice za izvajanje operacije.

WARN: »Unknown stream handle <šestnajstiška vrednost>. Ignoring request.«

Opozorilo se pojavi v primeru, ko odjemalec posreduje neveljavno oznako za dostop do toka podatkov. Gre za napako odjemalca.

WARN: »Service '<ime storitve>' cannot be resolved to a discreet port number (error: <systemski opis napake>).«

WARN: »Service '<ime storitve>' cannot be resolved to a discreet port number (error: <systemski opis napake>). Falling back to default service '<ime storitve>'...«

WARN: »Service '<ime storitve>' resolves to an unsupported protocol family.«

WARN: »Service '<ime storitve>' resolves to a unsupported protocol family. Falling back to default service '<ime storitve>'...«

Opozorila pomenijo napako pri inicializaciji sistema za omrežne povezave. Vzrok za napako je lahko napačna konfiguracija strežnika IMiS®/ARChive Server ali nepravilno delovanje operacijskega sistema.

WARN: »Description expression '<formula za opis vsebine>' failed to process, original description '<vrednost opisa>' will be used.«

Opozorilo pomeni napako v konfiguraciji za pretvarjanje vsebine. Gre za napako v atributu '*descriptionExpression*' v znački '*Output*'.