REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije

(Politika SIMoD-PKI)

Verzija 2.0

NEURADNO PREČIŠČENO BESEDILO

Zgodovina sprememb in dopolnitev Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije:

Izdaja:	Spremembe glede na prejšnjo izdajo:
Neuradno prečiščeno besedilo Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije (Politika SIMoD-PKI)	Združeni so dokumenti Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, verzija 2.0, številka 382-5/2006-109, Pravila o spremembah Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, verzija 2.0, številka 386-6/2011-229 in Pravila o dopolnitvah Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, verzija 2.0, številka: 386-6/2011-304.
Pravila o dopolnitvah Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, verzija 2.0, številka: 386-6/2011-304, datum: 14.11.2011	Uvedena je možnost, da overitelj s svojimi pravili delovanja lahko določi načine preverjanja istovetnosti in postopke obdelave zahtevka za ponovno izdajo digitalnih potrdil v izjemnih primerih, ki so različni od načinov oziroma postopkov predpisanih s Pravili delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije.
Pravila o spremembah Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, verzija 2.0, številka: 386-6/2011-229, datum: 08.09.2011	• odstranjene so vrednosti parametrov v povezavi z digitalnimi potrdili (dolžine in obdobje veljavnosti ključev) in • poenostavljen je postopek oddaje vloge za preklic digitalnega potrdila.

Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, verzija 2.0, številka: 382-5/2006-109, datum: 24.08.2010	• pristojnost sprejemanja pravil delovanja posameznih overiteljev je prenesena na Svet za upravljanje z infrastrukturo javnih ključev na MO, • spremenjeno je pravilo za določanje identifikacijskih oznak politik digitalnih potrdil, • razširjen je nabor imetnikov potrdil z organizacijskimi in funkcijskimi vlogami, • vpeljana so kvalificirana digitalna potrdila v skladu z ZEPEP in priporočili ETSI, • podrobneje so definirane zahteve za kvalificirana digitalna potrdila, • dodana so polja v kvalificiranih digitalnih potrdilih, • dodana je NIZKA stopnja zaupanja v digitalno potrdilo, • predpisani so postopki za izdajo digitalnih potrdil z obvezno uporabo pametne kartice, kjer overitelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, • predvidena je možnost ponovne izdaje digitalnega potrdila z uporabo PKCS#10 protokola brez osebnega preverjanja istovetnosti imetnika, če je elektronski zahtevek za ponovno izdajo podpisan z veljavnim digitalnim potrdilom, • poenostavljen je postopek prve registracije za digitalna potrdila NIZKE stopnje zaupanja.
Spremembe in dopolnitve Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije (Politika SIMoD-PKI), številka: 382-5/2006-42, datum: 27.12.2007	• spremenjena so polja v digitalnih potrdilih, • spremenjeno je pravilo za določanje identifikacijskih oznak politik digitalnih potrdil.
Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije (Politika SIMoD-PKI), šifra: 382-5/2006-11, datum: 17.7.2006	vpeljan je hiearalhični model infrastrukture javnih ključev.
Pravila overitelja digitalnih potrdil na Ministrstvu za obrambo Republike Slovenije – javni del notranjih pravil, šifra 471-01-6/2002-47, datum: 29.07.2005.	

KAZALO

1. UVOD 9

1.1. Pregled 9
1.2. Identifikacijske oznake politik delovanja 10
1.3. Udeleženci infrastrukture javnih ključev 11
1.3.1. Overitelji 11
1.3.1.1. Svet za upravljanje z infrastrukturo javnih ključev na MO 11
1.3.1.2. Operativno osebje overiteljev SIMoD-PKI 11
1.3.2. Prijavna služba 12
1.3.3. Imetniki digitalnih potrdil 12
1.3.4. Tretje osebe 12
1.3.5. Posredno odgovorni organi 13
1.4. Namen uporabe digitalnih potrdil 13
1.4.1. Dovoljena uporaba digitalnih potrdil 14
1.4.1.1. Stopnja zaupanja v digitalno potrdilo 14
1.4.1.2. Uporaba digitalnih potrdil VISOKE in SREDNJE stopnje zaupanja 15
1.4.1.3. Uporaba digitalnih potrdil NIZKE stopnje zaupanja 15
1.4.2. Nedovoljena uporaba digitalnih potrdil 15
1.5. Upravljanje s Politiko SIMoD-PKI 15
1.5.1. Organ, ki upravlja s tem dokumentom 15
1.5.2. Kontaktna oseba 15
1.5.3. Odgovorni organ za odobritev pravil delovanja overitelja 16
1.5.4. Postopek odobritve Pravil delovanja overitelja 16
1.6. Pojmi in kratice 16

2. ODGOVORNOST ZA OBJAVE IN IMENIK 20

2.1. Objave dokumentov in imenik 20
2.2. Objave informacij o digitalnih potrdilih 20
2.3. Čas in pogostost objav 21
2.4. Dostop do podatkov v imeniku in na spletni strani 21

3. PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI 22

3.1. Določanje imen 22
3.1.1. Vrste imen 22
3.1.2. Potreba po smiselnosti imen 22
3.1.3. Anonimnost imetnikov in uporaba psevdonimov 22
3.1.4. Pravila za interpretacijo različnih oblik imen 22
3.1.5. Edinstvenost imen 22
3.1.6. Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk 22
3.2. Preverjanje istovetnosti imetnikov ob prvi registraciji 23
3.2.1. Metode dokazovanja lastništva zasebnega ključa 23
3.2.2. Preverjanje istovetnosti za imetnike, ki niso fizične osebe 23
3.2.2.1. Digitalna potrdila za organizacijske enote MO in institucije, ki opravljajo naloge povezane z obrambo države 23
3.2.2.2. Digitalna potrdila za organizacijske ali funkcijske vloge 23
3.2.2.3. Digitalna potrdila za strežnike, drugo strojno in programsko opremo, izdajatelje varnih časovnih žigov ter druge ponudnike storitev overjanja 23
3.2.3. Preverjanje istovetnosti za fizične osebe 24
3.2.3.1. Zaposleni v MO in institucijah, ki opravljajo naloge povezane z obrambo države 24
3.2.3.2. Digitalna potrdila za vojaške dolžnosti v SV 24
3.2.4. Podatki o naročniku, ki se ne preverjajo 24
3.2.5. Preverjanje pooblastil 24
3.2.6. Merila za medsebojno povezovanje 25
3.3. Preverjanje imetnikov za ponovno izdajo digitalnega potrdila 25
3.3.1. Preverjanje istovetnosti pri rutinski ponovni izdaji digitalnih potrdil 25
3.3.2. Preverjanje istovetnosti za ponovno izdajo digitalnega potrdila po preklicu 25
3.4. Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila 25

4. UPRAVLJANJE Z DIGITALNIMI POTRDILI 26

4.1. Pridobitev digitalnega potrdila 26

4.1.1. Kdo lahko zaprosi za izdajo digitalnega potrdila 26
4.1.2. Postopek bodočega imetnika za pridobitev digitalnega potrdila in odgovornosti 26
4.2. Obdelava zahtevka za izdajo digitalnega potrdila 26
4.2.1. Preverjanje istovetnosti bodočega imetnika 26
4.2.2. Odobritev ali zavrnitev izdaje digitalnega potrdila 26
4.2.3. Čas za obdelavo zahtevka za izdajo digitalnega potrdila 27
4.3. Izdaja digitalnega potrdila 27
4.3.1. Postopki overiteljev SIMoD-PKI ob izdaji potrdil 27
4.3.1.1. Dostava zasebnega ključa imetniku 27
4.3.1.2. Dostava overiteljevega javnega ključa imetniku 28
4.3.2. Obvestilo naročnikom o izdaji digitalnega potrdila 28
4.4. Prevzem digitalnega potrdila 28
4.4.1. Postopek prevzema digitalnega potrdila 28
4.4.2. Objava digitalnega potrdila 28
4.4.3. Obveščanje drugih udeležencev o izdaji digitalnega potrdila 29
4.5. Uporaba ključev in digitalnih potrdil 29
4.5.1. Uporaba ključev in digitalnih potrdil imetnikov 29
4.5.1.1. Zasebni ključi in digitalna potrdila overiteljev 29
4.5.1.2. Zasebni ključi in digitalna potrdila prijavne službe 29
4.5.1.3. Uporabniški zasebni ključi in digitalna potrdila 29
4.5.2. Uporaba digitalnih potrdil s strani tretjih oseb 30
4.6. Ponovna izdaja digitalnega potrdila brez spremembe javnega ključa 30
4.7. Ponovna izdaja digitalnih potrdil 30
4.7.1. Razlogi za ponovno izdajo digitalnega potrdila 30
4.7.2. Kdo lahko zahteva ponovno izdajo digitalnega potrdila 30
4.7.3. Obdelava zahtevkov za ponovno izdajo digitalnega potrdila 30
4.7.4. Obvestilo imetniku o izdaji novega digitalnega potrdila 31
4.7.5. Postopek potrditve prevzema novega digitalnega potrdila 31
4.7.6. Objava novega digitalnega potrdila 31
4.7.7. Obveščanje drugih udeležencev o izdaji digitalnega potrdila 31
4.8. Sprememba digitalnega potrdila 31
4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila 31
4.9.1. Okoliščine preklica 31
4.9.1.1. Okoliščine preklica imetniških digitalnih potrdil 31
4.9.1.2. Okoliščine preklica digitalnega potrdila korenskega overitelja 32
4.9.1.3. Okoliščine preklica digitalnega potrdila o priznavanju drugega overitelja 32
4.9.1.4. Okoliščine preklica digitalnega potrdila podrejenega overitelja 32
4.9.2. Kdo lahko zahteva preklic 32
4.9.2.1. Kdo lahko zahteva preklic digitalnega potrdila imetnika 32
4.9.2.2. Kdo lahko zahteva preklic digitalnega potrdila korenskega overitelja 33
4.9.2.3. Kdo lahko zahteva preklic digitalnega potrdila o priznavanju drugega overitelja 33
4.9.2.4. Kdo lahko zahteva preklic digitalnega potrdila podrejenega overitelja 33
4.9.3. Postopki za preklic 33
4.9.3.1. Postopki preklica digitalnih potrdil imetnikov 33
4.9.3.2. Postopki preklica digitalnega potrdila korenskega overitelja 33
4.9.3.3. Postopki preklica digitalnega potrdila o priznavanju drugega overitelja 34
4.9.3.4. Postopki preklica digitalnega potrdila podrejenega overitelja 34
4.9.4. Čas za posredovanje zahtevka za preklic 34
4.9.5. Čas od prejema zahtevka za preklic do preklica 34
4.9.5.1. Čas za preklic digitalnega potrdila imetnika 34
4.9.5.2. Čas za preklic digitalnega potrdila korenskega overitelja 35
4.9.5.3. Čas za preklic digitalnega potrdila o priznavanju drugega overitelja 35
4.9.5.4. Čas za preklic digitalnega potrdila podrejenega overitelja 35
4.9.6. Obveza preverjanja registra preklicanih potrdil 35
4.9.7. Pogostost objav registrov preklicanih potrdil 35
4.9.8. Dovoljene zakasnitve pri objavi registrov preklicanih potrdil 36
4.9.9. Storitev sprotnega preverjanje statusa digitalnih potrdil 36
4.9.10. Obveza sprotnega preverjanja statusa preklicanih potrdil 36
4.9.11. Ostale oblike objavljanja preklicanih digitalnih potrdil 36
4.9.12. Posebne zahteve glede zlorabe ključa 36
4.9.13. Okoliščine za začasno ukinitev veljavnosti 36
4.9.14. Kdo lahko zahteva začasno ukinitev veljavnosti 36

4.9.15. Postopki za začasno ukinitev veljavnosti *36*
4.9.16. Omejitve obdobja začasne ukinitve veljavnosti *36*
4.10. Storitve preverjanja statusa digitalnih potrdil 36
4.10.1. Tehnične lastnosti storitve *36*
4.10.2. Razpoložljivost storitve *36*
4.10.3. Dodatne možnosti *36*
4.11. Predčasna prekinitev veljavnosti digitalnih potrdil 37
4.12. Varnostno kopiranje in odkrivanje zasebnega ključa 37
4.12.1. Povrnitev zgodovine ključev za dešifriranje *37*
4.12.2. Odkrivanje kopije ključev za dešifriranje *37*
4.12.3. Zaščita odkritega zasebnega ključa in postopek prenosa *38*

5. FIZIČNO VAROVANJE, ORGANIZACIJSKI VARNOSTNI UKREPI IN ZAHTEVE ZA OSEBJE 39

5.1. Fizično varovanje 39
5.1.1. Lokacija in konstrukcija prostorov ter fizični dostop *39*
5.1.2. Fizični dostop *39*
5.1.3. Napajanje in klimatske naprave *39*
5.1.4. Zaščita pred poplavo *39*
5.1.5. Zaščita pred ognjem *39*
5.1.6. Shranjevanje medijev *39*
5.1.7. Odstranjevanje odpadkov *40*
5.1.8. Hranjenje na oddaljeni lokaciji *40*
5.2. Organizacijski varnostni ukrepi 40
5.2.1. Organizacija upravljanja overitelja *40*
5.2.1.1. Operativno osebje overiteljev SIMoD-PKI 40
5.2.1.2. Prijavna služba 41
5.2.1.3. Druge funkcije 41
5.2.2. Število oseb, potrebnih za izvedbo postopkov *41*
5.2.3. Preverjanje istovetnosti operativnega osebja *42*
5.3. Zahteve za osebje overiteljev 42
5.3.1. Kvalifikacije, izkušnje in varnostno preverjanje *42*
5.3.2. Dovoljenja za dostop do tajnih podatkov *42*
5.3.3. Usposabljanje osebja *42*
5.3.3.1. Usposabljanje osebja overiteljev 42
5.3.3.2. Usposabljanje osebja za pomoč uporabnikom 42
5.3.4. Pogostost dodatnih usposabljanj *42*
5.3.5. Kroženje med delovnimi mesti *43*
5.3.6. Ukrepi ob kršitvah pooblastil *43*
5.3.7. Zunanji izvajalci *43*
5.3.8. Dokumentacija za osebje overiteljev *43*
5.4. Postopki varnostnih pregledov sistema 43
5.4.1. Vrste beleženih dogodkov *43*
5.4.2. Pogostost pregleda dnevnikov beleženih dogodkov *43*
5.4.3. Obdobje hranjenja dnevnikov beleženih dogodkov *44*
5.4.4. Zaščita dnevnikov beleženih dogodkov *44*
5.4.5. Varnostne kopije dnevnikov beleženih dogodkov *44*
5.4.6. Način zbiranja beleženih dogodkov *44*
5.4.7. Obveščanje povzročitelja dogodka *44*
5.4.8. Ocena in odprava ranljivosti *44*
5.5. Arhiviranje podatkov 44
5.5.1. Vrste arhiviranih podatkov *44*
5.5.2. Obdobje hranjenja arhiva *45*
5.5.3. Zaščita arhiva *45*
5.5.4. Varnostna kopija arhiva *45*
5.5.5. Časovno žigosanje zapisov *45*
5.5.6. Način arhiviranja *45*
5.5.7. Postopek vpogleda v in verifikacije arhiva *45*
5.6. Zamenjava ključev overiteljev 46
5.6.1. Obnova potrdila korenskega overitelja *46*
5.6.2. Obnova potrdil podrejenih overiteljev *46*

5.7. Okrevalni načrt 46
5.7.1. Postopki v primeru okvar in zlorab 46
5.7.2. Uničenje programske, strojne opreme ali podatkov overitelja 46
5.7.3. Zloraba zasebnega ključa overitelja 47
5.7.4. Zagotavljanje kontinuitete delovanja po nesrečah 47
5.8. Prenehanje delovanja overitelja 47
6. TEHNIČNE VARNOSTNE ZAHTEVE 48
6.1. Generiranje in namestitev para ključev 48
6.1.1. Generiranje para ključev 48
6.1.2. Dostava zasebnega ključa imetniku 48
6.1.3. Dostava imetnikovega javnega ključa overitelju 48
6.1.4. Dostava overiteljevega javnega ključa uporabnikom 48
6.1.5. Dolžina ključev 48
6.1.6. Parametri za generiranje javnih ključev in preverjanje parametrov 49
6.1.7. Namen uporabe ključev 49
6.2. Zaščita zasebnih ključev in zahteve za kriptografske module 49
6.2.1. Standardi za kriptografske module 49
6.2.2. Nadzor zasebnega ključa z več pooblaščenimi osebami 50
6.2.3. Odkrivanje zasebnega ključa 50
6.2.4. Varnostno kopiranje zasebnih ključev 50
6.2.5. Arhiviranje zasebnega ključa 50
6.2.6. Zapis zasebnega ključa v kriptografski modul in iz njega 50
6.2.7. Hranjenje zasebnega ključev v kriptografskem modulu 50
6.2.8. Postopek za aktiviranje zasebnega ključa 51
6.2.9. Postopek za deaktiviranje zasebnega ključa 51
6.2.10. Postopek za uničenje zasebnega ključa 51
6.2.11. Stopnja varnosti kriptografskih modulov 51
6.3. Ostali vidiki upravljanja s pari ključev 51
6.3.1. Arhiviranje javnega ključa 51
6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil 51
6.4. Gesla za dostop do zasebnih ključev 52
6.4.1. Določanje gesel za dostop do zasebnih ključev v kriptografskih modulih 52
6.4.2. Zaščita gesel 52
6.4.3. Druge zahteve za gesla 52
6.5. Varnostne zahteve za računalnike 52
6.5.1. Specifične tehnične varnostne zahteve za računalnike 52
6.5.2. Raven varnostne zaščite računalnikov 52
6.6. Tehnični nadzor življenjskega cikla overitelja 53
6.6.1. Nadzor razvoja sistema 53
6.6.2. Upravljanje varnosti 53
6.6.3. Upravljanje varnosti čez življenjski cikel 53
6.7. Varnostne kontrole na ravni računalniškega omrežja 53
6.8. Časovno žigosanje 53
7. PROFIL DIGITALNIH POTRDIL IN REGISTROV PREKLICANIH POTRDIL 54
7.1. Profil digitalnih potrdil 54
7.1.1. Verzija digitalnih potrdil 54
7.1.2. Razširitvena polja 54
7.1.3. Identifikacijske oznake algoritmov 55
7.1.4. Oblike imen 55
7.1.5. Omejitve imen 55
7.1.6. Identifikacijske oznake politik 55
7.1.7. Način uporabe razširitvenega polja za omejitev uporabe politik 55
7.1.8. Specifični podatki o politiki 55
7.1.9. Procesiranje oznake kritičnosti razširitvenih polj 56
7.2. Profil registrov preklicanih potrdil 56
7.2.1. Verzija registrov preklicanih potrdil 56
7.2.2. Razširitvena polja registrov preklicanih potrdil 56
7.3. Profil OSCP 57
7.3.1. Verzija OSCP 57

7.3.2. Razširitve OSCP 57

8. PREVERJANJE SKLADNOSTI IN OSTALE OBLIKE NADZORA 58

8.1. Pogostost inšpekcije 58
8.2. Pogoji za inšpektorja 58
8.3. Relacija med inšpektorjem in overitelji SIMoD-PKI 58
8.4. Področja inšpekcije 58
8.5. Postopki po opravljeni inšpekciji 58
8.6. Prejemniki ugotovitev o inšpekciji 59

9. OSTALE POSLOVNE IN PRAVNE ZADEVE 60

9.1. Cenik 60
9.1.1. Cena prve in ponovne izdaje digitalnega potrdila 60
9.1.2. Cena dostopa do digitalnega potrdila 60
9.1.3. Cena dostopa do podatka o statusu in preklicu potrdila 60
9.1.4. Cene drugih storitev 60
9.1.5. Povračilo stroškov 60
9.2. Finančna odgovornost 60
9.2.1. Višina zavarovanja 60
9.2.2. Druge oblike zavarovanja 60
9.2.3. Zavarovanje ali jamstva za končne uporabnike 60
9.3. Zaupnost poslovnih informacij 60
9.3.1. Obseg zaupnih poslovnih informacij 60
9.3.2. Informacije izven obsega zaupnih poslovnih informacij 60
9.3.3. Odgovornost za zagotavljanje zaupnosti poslovnih informacij 61
9.4. Zaupnost osebnih podatkov 61
9.4.1. Načrt zagotavljanja zaupnosti osebnih podatkov 61
9.4.2. Obseg osebnih podatkov, ki se obravnavajo kot zaupni 61
9.4.3. Osebni podatki, ki se ne obravnavajo kot zaupni 61
9.4.4. Odgovornost glede varovanja osebnih podatkov 61
9.4.5. Dovoljenje za uporabo osebnih podatkov 61
9.4.6. Posredovanje osebnih podatkov v sodnih in upravnih postopkih 61
9.4.7. Druge okoliščine posredovanja osebnih podatkov 61
9.5. Zaščita intelektualne lastnine 61
9.6. Odgovornosti in jamstva 62
9.6.1. Odgovornosti in jamstva overitelja 62
9.6.2. Odgovornost in jamstva prijavne službe 62
9.6.3. Odgovornost in jamstva imetnikov digitalnih potrdil 62
9.6.4. Odgovornost in jamstva tretjih oseb 62
9.6.5. Odgovornost in jamstva drugih udeležencev 62
9.7. Zanikanje odgovornosti overitelja 62
9.8. Omejitve odgovornosti overiteljev SIMoD-PKI 63
9.9. Zavarovanje pred škodo zaradi neizpolnjevanja obveznosti 63
9.10. Začetek in prenehanje veljavnosti 63
9.10.1. Začetek veljavnosti 63
9.10.2. Prenehanje veljavnosti 63
9.10.3. Posledice prenehanja veljavnosti 63
9.11. Obvestila in komuniciranje z udeleženci 63
9.12. Spreminjanje dokumenta 64
9.12.1. Postopek uveljavitve spremembe 64
9.12.2. Postopek in roki obveščanja 64
9.12.3. Spremembe, ki zahtevajo novo identifikacijsko oznako politike 64
9.13. Reševanje sporov 64
9.14. Veljavna zakonodaja 64
9.15. Ostala relevantna zakonodaja 65
9.16. Razne določbe 65
9.17. Ostale določbe 65

1. UVOD

1.1. Pregled

Ministrstvo za obrambo Republike Slovenije (v nadaljnjem besedilu: MO) upravlja z infrastrukturo javnih ključev na MO (ang. **S**loveni**i**an **M**inistry **o**f **D**efence **P**ublic **K**ey **I**nfrastructure, SIMoD-PKI) za potrebe obrambe države.

V okviru SIMoD-PKI deluje korenski overitelj in podrejeni overitelji digitalnih potrdil, v nadaljevanju overitelji SIMoD-PKI.

Ta dokument, Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, imenujemo tudi Politika SIMoD-PKI.

Politika SIMoD-PKI predpisuje pogoje, ki jih morajo izpolnjevati overitelji za zagotavljanje zaupanja v digitalna potrdila izdana po tej politiki. Politika SIMoD-PKI predpisuje splošne zahteve za digitalna potrdila, minimalne zahteve za tehnične lastnosti in raven varnosti infrastrukture overiteljev, postopke za upravljanje z digitalnimi potrdili, obveznosti in odgovornosti, ki jih morajo izpolnjevati overitelji, imetniki in tretje osebe, ki se zanašajo na digitalna potrdila, ter drugi overitelji, ki se želijo povezovati z infrastrukturo javnih ključev na MO.

Politika SIMoD-PKI predpisuje izdajanje in upravljanje digitalnih potrdil za zagotavljanje naslednjih varnostnih storitev:

- digitalno podpisovanje podatkov,
- zagotavljanje zaupnosti pri hranjenju in prenosu podatkov,
- selektivno omejevanje dostopa do podatkov,
- zagotavljanje celovitosti datotek, sporočil in elektronskih obrazcev,
- prepoznavanje in preverjanje istovetnosti oseb in gradnikov informacijske infrastrukture kot so strežniki, usmerjevalniki, požarne pregrade in imeniki ter
- nezanikanje oddaje ali sprejema sporočil.

Digitalna potrdila se med seboj ločijo glede na stopnjo zaupanja v digitalno potrdilo, namen uporabe, zahtevnost postopka preverjanja istovetnosti bodočega imetnika digitalnega potrdila in način hranjenja zasebnih ključev.

Overitelji SIMoD-PKI izdajajo nekvalificirana in kvalificirana digitalna potrdila. Kvalificirana so tista digitalna potrdila, za katera sta poleg splošnih zahtev po Politiki SIMoD-PKI izpolnjena naslednja pogoja:

- zasebni ključ se hrani izključno pri imetniku in je izključno pod njegovim nadzorom in
- ob prvi registraciji se preverja istovetnost bodočega imetnika v prijavni službi.

Politika SIMoD-PKI zagotavlja, da so kvalificirana potrdila skladna z [1] ZEPEP, [5] EU Direktiva o elektronskem podpisu, [3] ETSI TS 101 456 in [4] ETSI TS 101 862.

Overitelji v okviru infrastrukture javnih ključev na MO so dolžni objaviti pravila delovanja, ki morajo biti v skladu s Politiko SIMoD-PKI.

Overitelji SIMoD-PKI delujejo v zasebnem komunikacijsko informacijskem sistemu MO in SV (v nadaljnjem besedilu: KIS MO in SV).

SIMoD-PKI deluje po priporočilih zveze NATO, Evropske skupnosti in v skladu s predpisi, ki urejajo področje elektronskega podpisa v Republiki Sloveniji.

1.2. Identifikacijske oznake politik delovanja

Identifikacijske oznake politik delovanja overiteljev SIMoD-PKI (ang. Policy Object Identifiers; Policy OIDs) so določene po naslednjem pravilu: *osnova.p1.p2.p3.p4.p5.p6*

Del identifikacijske oznake	Vrednost	
Osnova OID	1.3.6.1.4.1.22295.10	
Klasifikacija KIS (p1)	1	brez stopnje tajnosti, javna omrežja + INTERNO
	2	TAJNO
	…	
Ob prvi registraciji obvezno preverjanje istovetnosti v prijavni službi (p2)	1	DA
	2	NE
Obvezna uporaba sredstva za varno elektronsko podpisovanje[1] (p3)	1	DA
	2	NE
Imetnik digitalnega potrdila (p4)	1	fizična oseba
	2	funkcijska ali organizacijska vloga
	3	organizacijska enota MO ali institucija, ki opravlja naloge povezane z obrambo
	4	strežnik ali druga strojna oziroma programska oprema
	5	izdajatelj varnih časovnih žigov
	…	
Namen uporabe ključev (p5)	1	preverjanje digitalnega podpisa
	2	šifriranje s hranjenjem kopije zasebnega ključa pri overitelju
	3	preverjanje digitalnega podpisa in šifriranje
	…	
Verzija (p6)	zaporedna številka izdaje politike	

Overitelji označijo, pod katero politiko izdajajo digitalna potrdila, v razširitvenih poljih, kot je določeno v poglavju 7.1.2 Razširitvena polja.

Overitelji SIMoD-PKI lahko izdajajo eno ali več vrst digitalnih potrdil, kar morajo jasno označiti v svojih pravilih delovanja in digitalnih potrdilih z navedbo identifikacijske oznake politike v razširitvenem polju *Certificate Policies*. Overitelji lahko digitalnim potrdilom, ki jih izdajajo po eni od SIMoD-PKI politik, dodelijo svojo identifikacijsko oznako. V tem primeru mora biti v razširitvenem polju *Certificate Policies* identifikacijska oznaka po politiki SIMoD-PKI in overiteljeva identifikacijska oznaka.

Overitelji SIMoD-PKI lahko poleg digitalnih potrdil določenih v tej politiki izdajajo tudi druga digitalna potrdila, kar morajo jasno označiti v svojih pravilih delovanja in digitalnih potrdilih z navedbo identifikacijske oznake politike v razširitvenem polju C*ertificate Policies*. Digitalna potrdila, ki niso izdana v skladu z eno od identifikacijskih oznak oziroma politik digitalnih potrdil določenih v Politiki SIMoD-PKI, ne smejo vsebovati identifikacijske oznake SIMoD-PKI.

Kvalificirana digitalna potrdila morajo v skladu z [1] ZEPEP vsebovati navedbo, da so kvalificirana potrdila.

Kvalificirana digitalna potrdila skladna z [3] ETSI TS 101 456 morajo v razširitvenem polju *Certificate Policies* vsebovati poleg oznake politike po Politiki SIMoD-PKI še oznako politike *0.4.0.1456.1.2*, kar pomeni skladnost z ETSI politiko za kvalificirana potrdila; kvalificirana potrdila z obvezno uporabo sredstva za varno podpisovanje pa še oznako politike

[1] Primera sredstev za varno elektronsko podpisovanje: strojni kriptografski modul in pametna kartica

0.4.0.1456.1.1, kar pomeni skladnost z ETSI politiko za kvalificirana potrdila z uporabo sredstva za varno elektronsko podpisovanje.

Kvalificirana digitalna potrdila skladna z [3] ETSI TS 101 456 morajo vsebovati razširitveno polje *qcStatement* z vrednostjo *QcCompliance statement*; kvalificirana potrdila z obvezno uporabo sredstva za varno podpisovanje pa še vrednost *QcSSCD statement.*

1.3. Udeleženci infrastrukture javnih ključev

1.3.1. Overitelji

V okviru SIMoD-PKI deluje korenski overitelj in podrejeni overitelji.

Overitelji posedujejo strojno in programsko opremo, zaposlujejo osebje in izvajajo predpisane postopke ter ukrepe, ki zagotavljajo varno in zanesljivo poslovanje infrastrukture javnih ključev na MO (v nadaljevanju SIMoD-PKI). Overitelje, ki delujejo v okviru SIMoD-PKI, zastopa Svet za upravljanje z infrastrukturo javnih ključev na MO.

1.3.1.1. Svet za upravljanje z infrastrukturo javnih ključev na MO

Svet za upravljanje z infrastrukturo javnih ključev na MO upravlja z infrastrukturo javnih ključev na MO, jo zastopa (glej poglavje 1.5.2 Kontaktna oseba) in ima v zvezi s tem naslednje obveznosti:

- nadzira izdelavo, vodi postopek potrditve, ocenjuje predlagane spremembe, predlaga uveljavitve sprememb in načrtuje postopek uveljavitve sprememb Politike SIMoD-PKI,
- ocenjuje in potrjuje skladnost pravil delovanja posameznega overitelja s Politiko SIMoD-PKI,
- sprejema pravila delovanja overiteljev SIMoD-PKI,
- imenuje operativno osebje overiteljev SIMoD-PKI,
- operativnemu osebju daje usmeritve za odpravljanje pomanjkljivosti, ugotovljenih ob inšpekcijskem in drugih oblikah nadzora ter uveljavlja druge ukrepe, kot je npr. preklic overiteljevega potrdila,
- ocenjuje ustreznost politik digitalnih potrdil drugih overiteljev v postopku medsebojnega priznavanja ter usmerja postopke in ukrepe formalnega medsebojnega priznavanja z drugimi overitelji.

Svet za upravljanje z infrastrukturo javnih ključev na MO sestavlja 7 članov:

- vodja organizacijske enote MO pristojne za informatiko in telekomunikacije, ki je vodja sveta,
- vodja organizacijske enote MO pristojne za obveščevalno varnostne zadeve,
- vodja organizacijske enote MO pristojne za pravne zadeve,
- prvi varnostni inženir iz skupine za upravljanje z digitalnimi potrdili korenskega overitelja,
- prvi administrator overitelja iz skupine za upravljanje z informacijskim sistemom korenskega overitelja,
- dva člana Sveta sta strokovna sodelavca iz organizacijske enote MO pristojne za informatiko in telekomunikacije, ki ju predlaga vodja sveta.

Svet za upravljanje z infrastrukturo javnih ključev na MO je za svoje delo odgovoren ministru.

1.3.1.2. Operativno osebje overiteljev SIMoD-PKI

Operativno osebje overiteljev SIMoD-PKI so zaposleni notranje organizacijske enote MO, pristojne za informatiko in telekomunikacije, ki opravljajo naloge izdajanja in upravljanja z digitalnimi potrdili ter zagotavljanja varnega in zanesljivega delovanja komunikacijsko informacijske infrastrukture overiteljev.

1.3.2. Prijavna služba

Prijavna služba sprejema zahtevke in preverja točnost podatkov naročnikov digitalnih potrdil. Naloge prijavne službe opravlja organizacijska enota MO, pristojna za kadrovske zadeve. Osebje prijavne službe imenuje vodja organizacijske enote MO, pristojne za kadrovske zadeve.

1.3.3. Imetniki digitalnih potrdil

Imetniki digitalnih potrdil so:

- fizične osebe - zaposleni v MO,
- fizične osebe - zaposleni v institucijah, ki opravljajo naloge povezane z obrambo,
- organizacijske enote in organi v sestavi MO (v nadaljevanju organizacijske enote MO),
- institucije, ki opravljajo naloge povezane z obrambo,
- vojaške dolžnosti v SV,
- funkcijske in organizacijske vloge, povezane z opravljanjem vojaških nalog ali drugih nalog s področja obrambe,
- strežniki in druga strojna ter programska oprema in
- izdajatelji varnih časovnih žigov in drugi ponudniki storitev overjanja.

Odgovorna oseba za digitalno potrdilo za organizacijske enote MO je vodja organizacijske enote MO, ki ima glede digitalnega potrdila enake obveznosti kot fizična oseba.

Odgovorna oseba za digitalno potrdilo za institucije, ki opravljajo naloge povezane z obrambo, je predstojnik institucije, ki ima glede digitalnega potrdila enake obveznosti kot fizična oseba.

Odgovorna oseba za digitalno potrdilo za vojaške dolžnosti v SV je fizična oseba - nosilec vojaške dolžnosti (npr, poveljnik enote) oziroma v primeru, ko opravlja isto vojaško dolžnost več oseb (npr. dežurni poveljstva), poveljnik enote SV, v okviru katere je vzpostavljena vojaška dolžnost.

Odgovorna oseba za digitalno potrdilo za funkcijsko ali organizacijsko vlogo je nosilec, skrbnik ali administrator vloge. Glede digitalnega potrdila ima enake obveznosti kot fizična oseba.

Odgovorna oseba za digitalno potrdilo za strežnike in drugo strojno ter programsko opremo je skrbnik strežnika, druge strojne ali programske opreme. Odgovorna oseba ima glede digitalnega potrdila za strežnik, drugo strojno ali programsko opremo enake obveznosti kot fizična oseba.

Odgovorna oseba za digitalno potrdilo za izdajatelje časovnih žigov in druge ponudnike storitev overjanja je vodja notranje organizacijske enote MO, ki upravlja z izdajateljem časovnega žiga ali drugim ponudnikom storitev overjanja. Odgovorna oseba ima glede digitalnega potrdila za izdajatelja časovnega žiga ali podobnega ponudnika storitev overjanja enake obveznosti kot fizična oseba.

Overitelj ali medsebojno priznani drugi overitelj je s tehničnega stališča tudi imetnik digitalnega potrdila, vendar se v tem dokumentu oznaka “imetnik” uporablja za tiste lastnike digitalnih potrdil, ki uporabljajo digitalna potrdila za namene, različne od podpisovanja in izdajanja digitalnih potrdil ter podpisovanja registra preklicanih potrdil.

1.3.4. Tretje osebe

Tretje osebe so osebe, ki zaupajo digitalnim potrdilom oziroma povezavi med imetnikovim imenom in javnim ključem v digitalnem potrdilu. Zaupanje izhaja iz zaupanja v overitelja.

Tretje osebe so:

- imetniki digitalnih potrdil overiteljev SIMoD-PKI,
- imetniki digitalnih potrdil overiteljev, ki so medsebojno priznani s SIMoD-PKI,

- podrejeni overitelji in
- subjekti, ki nimajo digitalnega potrdila overitelja SIMoD-PKI, a se zanašajo na digitalna potrdila, ki so jih je izdali overitelji SIMoD-PKI.

1.3.5. Posredno odgovorni organi

Overitelji SIMoD-PKI delujejo v KIS MO in SV in obratujejo v skladu s predpisi MO za področje KIS MO in SV. Posredno odgovorni organi so tudi organizacijske enote MO, ki so pristojne za področje varovanja ter nadzora KIS MO in SV.

1.4. Namen uporabe digitalnih potrdil

Namen uporabe digitalnih potrdil je določen z namenom uporabe pripadajočih ključev (poglavje 6.1.7 Namen uporabe ključev). Namen uporabe javnih in zasebnih ključev za določeno digitalno potrdilo je naveden v spodnji tabeli:

Vrsta digitalnega potrdila	Namen uporabe zasebnega ključa	Namen uporabe javnega ključa oziroma digitalnega potrdila
digitalno potrdilo korenskega overitelja	digitalno podpisovanje potrdil podrejenih overiteljev in medsebojno priznanih overiteljev ter registrov preklicanih overiteljev	preverjanje digitalnega podpisa na potrdilih podrejenih overiteljev in medsebojno priznanih overiteljev ter registrih preklicanih overiteljev
digitalno potrdilo podrejenega overitelja	digitalno podpisovanje digitalnih potrdil in registrov preklicanih potrdil	preverjanje digitalnega podpisa na digitalnih potrdilih in registrih preklicanih potrdil
digitalno potrdilo za preverjanje digitalnega podpisa	digitalno podpisovanje	preverjanje digitalnega podpisa
digitalno potrdilo za šifriranje	dešifriranje[2]	šifriranje[3]
digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje	digitalno podpisovanje in dešifriranje	preverjanje digitalnega podpisa in šifriranje
digitalno potrdilo za izdajatelja varnih časovnih žigov	digitalno podpisovanje varnih časovnih žigov	preverjanje varnih časovnih žigov
digitalno potrdilo za ponudnike storitev overjanja	digitalno podpisovanje podatkov ponudnika storitev overjanja	preverjanje podatkov ponudnika storitev overjanja

Digitalna potrdila overiteljev SIMoD-PKI se morajo uporabljati v skladu s Politiko SIMoD-PKI in pravili delovanja overitelja. Digitalna potrdila overiteljev SIMoD-PKI so namenjena izključno službeni uporabi v MO. V drugih institucijah pa je namen omejen na opravljanje nalog povezanih z obrambo države.

Infrastruktura javnih ključev na MO omogoča pet osnovnih varnostnih storitev:

- **zaupnost**, kot lastnost podatkov v elektronski obliki, da so nerazumljivi ali nerazpoložljivi neavtoriziranim osebam,
- **celovitost** (tudi pristnost), kot lastnost podatkov v elektronski obliki, da se niso spremenili na način, ki ga ne bi bilo moč ugotoviti,
- **nezanikanje**, kot lastnost oz. mehanizem, ki onemogoča zanikanje izvršenega dejanja (npr. elektronske transakcije) oz. lastništva e-podatkov,
- **preverjanje istovetnosti**, kot mehanizem za preverjanje identitete v elektronski obliki in

[2] Zasebni ključ se uporablja za dešifriranje dejanskih simetričnih šifrirnih ključev.
[3] Javni ključ se uporablja za šifriranje dejanskih simetričnih šifrirnih ključev.

- **selektivno omejevanje dostopa**, v smislu, da so šifrirani podatki nerazumljivi ali nerazpoložljivi neavtoriziranim osebam.

Infrastruktura javnih ključev na MO zagotavlja zgoraj navedene varnostne storitve prepoznavanja oziroma preverjanja istovetnosti, celovitosti in nezanikanja z varnostnim mehanizmom digitalnega podpisa, zaupnost in omejevanje dostopa pa z mehanizmi izmenjave ključev kot podporo simetričnim šifrirnim algoritmom. Te osnovne varnostne storitve omogočajo dolgoročno celovitost podatkov, vendar same zase včasih ne zagotavljajo celovitosti v vseh primerih. Če obstaja zahteva po zagotavljanju verodostojnosti podpisa v časovnem obdobju, ki presega veljavnost potrdila za overjanje podpisa, je zahtevana dodatna storitev časovnega žigosanja. Ta storitev mora biti predpisana z ustreznimi politikami delovanja izdajateljev varnih časovnih žigov.

1.4.1. Dovoljena uporaba digitalnih potrdil

1.4.1.1. Stopnja zaupanja v digitalno potrdilo

Digitalno potrdilo nedvoumno povezuje imetnika digitalnega potrdila z njegovim javnim ključem. Celovitost in varnost povezave med imetnikom in njegovim javnim ključem je ocenjena s stopnjo zaupanja v digitalno potrdilo. Stopnja zaupanja je odvisna od strogosti registracijskih postopkov, postopkov pri upravljanju z digitalnimi potrdili in pripadajočimi zasebnimi ključi, zahtev glede osebja, fizičnega in tehničnega varovanja infrastrukture javnih ključev ter varovanja zasebnih ključev.

Stopnje zaupanja v digitalna potrdila overiteljev SIMoD-PKI so določene z izpolnjevanjem naslednjih pogojev:

Pogoj:						
Ob prvi registraciji obvezno preverjanje identitete v prijavni službi	DA	DA	DA	DA	NE	NE
Obvezna uporaba sredstva za varno elektronsko podpisovanje	DA	DA	NE	NE	NE	NE
Zasebni ključ se hrani in je pod izključno kontrolo imetnika	DA	NE	DA	NE	DA	NE
Stopnja zaupanja:	VISOKA	VISOKA	SREDNJA	SREDNJA	NIZKA	NIZKA
Identifikacija digitalnega potrdila po ETSI TS 101 456:	QCP public + SSCD[4]		QCP public[5]			

V nadaljevanju so podane smernice za uporabo digitalnih potrdil različnih stopenj zaupanja Odločitev o uporabi digitalnega potrdila ustrezne stopnje zaupanja mora biti rezultat konkretne študije, ki upošteva konkretno okolje uporabe in vključuje obvladovanje tveganj. Študija upošteva dejstvo ali gre za tajne, osebne ali druge podatke, ki glede na pomembnost, zahtevo po celovitosti in razpoložljivosti, zahtevajo uporabo digitalnih potrdil določene stopnje zaupanja. Ustreznost odločitve potrdi odgovorni organ, ki izda dovoljenje za obratovanje informacijske rešitve.

Uporaba digitalnih potrdil oziroma varnostnih storitev infrastrukture javnih ključev MO ne povečuje ravni zaščite KIS MO in SV, povečuje pa varnost konkretne aplikacije oziroma informacijske rešitve. Izjemoma je dopustna uporaba digitalnih potrdil za zagotavljanje tajnosti, kjer se omrežje z nizko ravnjo zaščite uporablja samo kot prenosni medij (npr. podatki stopnje tajnosti INTERNO se prenašajo preko javnega Internet omrežja). Digitalna potrdila se uporabljajo v okviru KIS MO in SV za implementacijo varnostnih storitev, ki jih KIS MO in SV sam ne nudi.

[4] kvalificirano potrdilo z obvezno uporabo sredstva za varno elektronsko podpisovanje
[5] kvalificirano potrdilo

1.4.1.2. Uporaba digitalnih potrdil VISOKE in SREDNJE stopnje zaupanja

Uporaba digitalnih potrdil VISOKE in SREDNJE stopnje zaupanja zagotavlja:

- celovitost, preverjanje istovetnosti in nezanikanje podatkov vseh stopenj tajnosti,
- zaupnost podatkov do stopnje tajnosti vključno INTERNO,
- selektivno omejevanje dostopa do podatkov do stopnje tajnosti vključno TAJNO,
- upravljanje z varnostnimi parametri v KIS; upravljanje s šifrirnimi ključi naprav v KIS (usmerjevalniki, šifrirne naprave), daljinski nadzor in upravljanje z napravami in
- preverjanje istovetnosti naprav v KIS.

Pri prenosu podatkov stopnje tajnosti ZAUPNO in višje v nevarovanem KIS ni dovoljeno uporabljati digitalnih potrdil za šifriranje kot edinega varnostnega mehanizma za zagotavljanje zaupnosti teh podatkov.

1.4.1.3. Uporaba digitalnih potrdil NIZKE stopnje zaupanja

V vseh primerih, kjer se uporabljajo potrdila z NIZKO stopnjo zaupanja, se lahko uporabljajo tudi potrdila SREDNJE in VISOKE stopnje zaupanja.

Uporaba digitalnih potrdil NIZKE stopnje zaupanja zagotavlja:

- celovitost, preverjanje istovetnosti, selektivno omejevanje dostopa, zaupnost in nezanikanje za podatke brez stopnje tajnosti (npr. spletni dostop po protokolu SSL),
- zaupnost podatkov, ki niso tajni podatki po [10] ZTP, npr. osebni podatki,
- upravljanje z varnostnimi parametri v KIS; upravljanje s šifrirnimi ključi naprav v KIS (usmerjevalniki, šifrirne naprave), daljinski nadzor in upravljanje z napravami; predpogoj je ustrezno fizično varovanje naprav, da je možnost zlorabe digitalnih potrdil majhna in
- preverjanje istovetnosti naprav v KIS, če so naprave fizično varovane, da je možnost zlorabe potrdil majhna.

1.4.2. Nedovoljena uporaba digitalnih potrdil

Ni relevantno.

1.5. Upravljanje s Politiko SIMoD-PKI

1.5.1. Organ, ki upravlja s tem dokumentom

Svet za upravljanje z infrastrukturo javnih ključev na MO nadzira izdelavo, vodi postopek potrditve in ocenjuje, predlaga ter načrtuje uveljavitev sprememb Politike SIMoD-PKI.

Operativno osebje overiteljev SIMoD-PKI predlaga Svetu za upravljanje z infrastrukturo javnih ključev na MO spremembe Politike SIMoD-PKI.

1.5.2. Kontaktna oseba

Naslov:	Ministrstvo za obrambo Sekretariat generalnega sekretarja Služba za informatiko in komunikacije Svet za upravljanje z infrastrukturo javnih ključev na MO Vojkova cesta 55, 1000 Ljubljana
Telefon:	01 230 5314
Faks:	01 471 2701
Spletni naslov:	http://www.simod-pki.mors.si
Naslov elektronske pošte:	simod-pki@mors.si

1.5.3. Odgovorni organ za odobritev pravil delovanja overitelja

Odgovorni organ za odobritev skladnosti pravil delovanja overitelja z Politiko SIMoD-PKI je Svet za upravljanje z infrastrukturo javnih ključev na MO.

1.5.4. Postopek odobritve Pravil delovanja overitelja

Overitelj mora Svetu za upravljanje z infrastrukturo javnih ključev na MO predložiti pravila delovanja. Svet za upravljanje z infrastrukturo javnih ključev na MO preveri:

- skladnost pravil delovanja overitelja z zahtevami Politike SIMoD-PKI,
- overiteljevo infrastrukturo in postopke.

Izdaja digitalnega potrdila overitelju je hkrati tudi potrditev skladnosti s Politiko SIMoD-PKI.

Svet za upravljanje z infrastrukturo javnih ključev na MO lahko za izvedbo postopka preverjanja skladnosti pooblasti zunanjo inšpekcijsko službo oziroma organizacijo z ustreznim znanjem in izkušnjami s področja infrastrukture javnih ključev.

1.6. Pojmi in kratice

Pojem	Definicija
Časovni žig	Elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času.
Digitalni podpis	Dodan podatek ali kriptografsko preoblikovanje, ki omogoča, da prejemnik podatkov preveri njihov izvor in integriteto, ter s tem prepreči poneverbo.
Digitalno potrdilo	Potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto.
Digitalno potrdilo izdajatelja časovnih žigov	Digitalno potrdilo, s katerim izdajatelj časovnih žigov izdaja časovne žige.
Digitalno potrdilo za preverjanje podpisa	Digitalno potrdilo, ki se uporablja za verifikacijo digitalnega podpisa, preverjanje istovetnosti uporabnikov in preverjanje celovitosti podatkov v elektronski obliki.
Digitalno potrdilo za šifriranje	Digitalno potrdilo, ki se uporablja za izmenjavo simetričnih šifrirnih ključev pri zagotavljanju tajnosti podatkov v elektronski obliki.
Elektronski podpis	Niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika.
Elektronsko sporočilo	Niz podatkov, ki so poslani ali prejeti na elektronski način, kar vključuje predvsem elektronsko izmenjavo podatkov in elektronsko pošto.
Imenik	Podatkovna struktura, ki vsebuje objekte z določenimi lastnosti in pripadajočimi vrednostmi. Imenik, ki vsebuje digitalna potrdila je običajno v skladu s standardom X.500 oziroma razširjenim standardom X.509 ver.3.
Imetnik potrdila	Fizična oseba, navedena v digitalnem potrdilu v polju »Subject« kot lastnik zasebnega ključa, ki ustreza javnemu ključu, vsebovanem v digitalnem potrdilu oziroma odgovorna oseba za uporabo digitalnega potrdila.
Informacijski sistem	Skupek naprav in postopkov, ki omogočajo obdelavo informacij oziroma nudijo informacijske storitve. Združuje računalniško strojno in programsko opremo, računalniške nosilce podatkov, podatkovne zbirke in druge naprave ter identifikacijske, avtorizacijske, upravljavske in nadzorne postopke v funkcionalno celoto.
Javni ključ	Ključ iz para ključev, ki je lahko javno objavljen.
Javni komunikacijsko informacijski sistem	Je komunikacijsko informacijski sistem, katerega storitve so namenjene javni uporabi.

Komunikacijski sistem	Skupek naprav in postopkov, ki omogočajo prenos informacij. Primeri takih sistemov so telekomunikacijski sistemi in računalniška omrežja.
Komunikacijsko informacijski sistem	Skupen izraz za komunikacijski in informacijski sistem.
Kvalificirano digitalno potrdilo	Digitalno potrdilo, ki izpolnjuje zahteve iz 28. člena ZEPEP. Izda ga overitelj, ki deluje v skladu z zahtevami iz 28. do 36. člena ZEPEP.
Naročnik potrdila	Fizična ali pravna oseba, ki z zahtevkom zaprosi za izdajo digitalnega potrdila.
Oprema za elektronsko podpisovanje	Strojna ali programska oprema ali njune specifične sestavine, ki jo overitelj uporablja za storitve v zvezi z elektronskim podpisovanjem ali ki se uporabljajo za oblikovanje ali preverjanje elektronskih podpisov.
Overitelj digitalnih potrdil	Fizična ali pravna oseba, ki izdaja digitalna potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi.
Par ključev	Par asimetričnih kriptografskih ključev, ki ga sestavljata zasebni in javni ključ.
Podatki v elektronski obliki	Podatki, ki so oblikovani, shranjeni, poslani, prejeti ali izmenljivi na elektronski način.
Podatki za elektronsko podpisovanje	Edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa.
Podatki za preverjanje elektronskega podpisa	Edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa.
Podpisnik	Oseba, ki ustvari ali je v njenem imenu in v skladu z njeno voljo ustvarjen elektronski podpis.
Politika digitalnih potrdil	Nabor pravil, ki posledično definira uporabnost digitalnih potrdil v določeni skupini uporabnikov in/ali za določen nabor aplikacij s skupnimi varnostnimi zahtevami.
Pošiljatelj elektronskega sporočila	Oseba, ki je sama poslala elektronsko sporočilo ali pa je bilo sporočilo poslano v njenem imenu in v skladu z njeno voljo; posrednik elektronskega sporočila se ne šteje za pošiljatelja tega elektronskega sporočila.
Prejemnik elektronskega sporočila	Oseba, ki je prejela elektronsko sporočilo; posrednik elektronskega sporočila se ne šteje za prejemnika tega elektronskega sporočila.
Prijavna služba	Služba oziroma organizacija, ki po pooblastilu overitelja sprejema zahtevke in preverja istovetnosti bodočih imetnikov.
Selektivno omejevanje dostopa	Ločevanje dostopa glede na upravičen interes.
Sredstvo za elektronsko podpisovanje	Nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa.
Sredstvo za varno elektronsko podpisovanje	Sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve iz 37. člena ZEPEP.
Šifrirni (kriptografski) ključ	Niz znakov uporabljen za kriptografsko preoblikovanje (npr. šifriranje, dešifriranje, podpisovanje, ali preverjanje podpisa).
Tajni podatek	Dejstvo ali sredstvo iz delovnega področja organa, ki se nanaša na javno varnost, obrambne zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov določenih v ZTP zaščititi pred nepoklicanimi osebami, in ki je v skladu s ZTP določeno in označeno kot tajno.
Tajnost	Zaupnost v smislu ZTP.
Tretja oseba	Subjekt, ki ni aktivno udeležen v storitev, vendar zaupa izvajalcu in rezultatu storitve.
Uporabnik	Naročnik ali imetnik digitalnega potrdila.

Varen časovni žig	Elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času (2. člen ZEPEP). Varen časovni žig mora v skladu s 34. členom Uredbe vsebovati nedvoumne in pravilne podatke o datumu, točnem času najmanj na sekundo natančno in overitelju, ki je varni časovni žig ustvaril. Varni časovni žig je lahko dokumentu dodan ali priložen in z njim povezan, vendar morajo biti pri tem vedno izpolnjene enake zahteve kot za varen elektronski podpis s kvalificiranim digitalnim potrdilom.
Varen elektronski podpis	Je elektronski podpis, ki izpolnjuje naslednje zahteve: • povezan je izključno s podpisnikom, • iz njega je mogoče zanesljivo ugotoviti podpisnika, • ustvarjen je s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom, • povezan je s podatki, na katere se nanaša, tako, da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi.
Zasebni komunikacijsko informacijski sistem	Je komunikacijsko informacijski sistem, ki ni javen in je v lasti, upravljanju in pod nadzorom neke privatne, vladne ali nevladne organizacije.
Zasebni ključ	Ključ iz para ključev, ki mora ostati skriven, da se zagotovi zaupnost in celovitost podatkov v elektronski obliki.
Zloraba	Je razkritje tajnega podatka, izguba celovitosti ali razpoložljivosti podatka.

Kratica	Opis
CN	Splošno ime objekta v imeniku (ang. Common Name).
CRL	Register preklicanih potrdil (ang. Certificate Revocation List).
DN	Razločevalno ime objekta v imeniku, tudi polno ime objekta v imeniku (ang. Distinguished Name).
RDN	Kratko razločevalno ime objekta v imeniku, praviloma sestavljeno in splošnega imena (ang. Common Name, CN) in serijske številke (ang. serialNumber)
ETSI	Evropski inštitut za standardizacijo na področju telekomunikacij; izdaja serijo standardov s področja elektronskega podpisa in delovanja overiteljev (ang. European Telecommunications Standards Institute).
FIPS	Standardi za informacijske tehnologije, ki so v uporabi v ameriških zveznih institucijah. Izdaja jih ameriški nacionalni inštitut za standarde in tehnologijo (ang. Federal Information Processing Standards).
FIPS 140-2	Serija standardov FIPS za kriptografske module.
HTTP	Protokol za prenos podatkov v spletnem okolju (ang. Hypertext Transfer Protocol).
FQDN	Popolno ime naprave v domenskem sistemu (ang. Fully Qualified Domain Name).
IETF	Združenje strokovnjakov s področja Internetnih tehnologij. Izdelujejo serije priporočil (ang. Internet Engineering Task Force).
ISO	Mednarodna organizacija za standardizacijo (ang. International Standardization Organization).
ITU-T	Mednarodna organizacija za standardizacijo na področju telekomunikacij (ang. International Telecommunications Union - Telecommunication Standardization Sector).
KIS MO in SV	Komunikacijsko informacijski sistem MO in SV.
LDAP	Protokol, ki določa dostop do imenika in je specificiran po IETF (ang. Internet Engineering Task Force) priporočilu RFC 1777 (LDAP, ang. Leightweight Directory Access Protocol).
MO	Ministrstvo za obrambo
PKCS	Priporočila podjetja RSA Security za uporabo asimetričnih kriptografskih algoritmov (ang. Public Key Cryptographic Standards).

PKCS#1	Osnovna pravila za formatiranje podatkov ob implementaciji RSA funkcij. Predpisuje, kako se izračuna digitalni podpis, kako se formatirajo podatki, ki se podpisujejo in format podpisa. Predpisuje tudi sintakso javnega in zasebnega RSA ključa.
PKCS#10	Sintaksa zahtevka za digitalno potrdilo. Zahtevek za digitalno potrdilo vsebuje razločevalno ime, javni ključ in nabor drugih atributov, ki jih podpiše subjekt, ki zahteva potrditev. Daljše ime: PKCS#10 Certification Request Syntax Standard.
PKCS#7	Sintaksa za kriptografsko obdelane podatke, kot digitalni podpisi in digitalne ovojnice.
PKI	Infrastruktura javnih ključev; strojna in programska oprema ter varnostni mehanizmi za zaupanja vredno implementacijo varnostnih storitev, ki temeljijo na nesimetrični kriptografiji (ang. Public Key Infrastructure).
PKIX	Delovna skupina za področje infrastrukture javnih ključev v okviru IETF(ang. Internet Engineering Task Force). Izdala serijo priporočil za digitalna potrdila in registre preklicanih potrdil (ang. Public Key Infrastrukture X.509).
PKIX- CMP	Postopek izmenjave podatkov, ki se nanašajo na digitalna potrdila med subjekti infrastrukture overitelja (ang. PKIX Certificate Management Protocol). Vključuje PKCS#7 in PKCS#10.
RFC	Priporočila, ki jih izdaja IETF.
RFC 4210	Priporočilo, ki določa postopke za izmenjavo podatkov, ki se nanašajo na digitalna potrdila. Vsebuje PKIX-CMP.
RFC 3647	Priporočilo, ki določa elemente, ki naj bodo zajeti v politiki overitelja (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework). veljavno od novembra 2003 (je nadomestil RFC 2527).
RFC 3280	Priporočilo, ki določa elemente potrdil in registra preklicanih potrdil.
RSA	Eden prvih nesimetričnih kriptografskih sistemov, patentiran leta 1983, imenovan po odkriteljih: Rivest, Shamir in Adelman.
SIMoD-PKI	Infrastruktura javnih ključev Ministrstva za obrambo Republike Slovenije (ang. **S**loveni**i**an **M**inistry **o**f **D**efence **P**ublic **K**ey **I**nfrastructure - SIMoD-PKI)
SV	Slovenska vojska
QCP public + SSCD	Oznaka ETSI politike za kvalificirana potrdila z uporabo sredstva za varno elektronsko podpisovanje (ang. a certificate policy for qualified certificates issued to the public, requiring use of secure signature creation devices).
SSCD	Sredstvo za varno elektronsko podpisovanje (ang. secure signature creation device).
QCP public + SSCD	Oznaka ETSI politike za kvalificirana potrdila (ang. QCP public; a certificate policy for qualified certificates issued to the public).
X.501	Standard organizacij ITU-T in ISO, ki definira poimenovanje objektov v imeniku. Tudi del serije PKIX Part1.
X.509	Standard organizacij ITU-T in ISO, ki definira strukturo digitalnih potrdil. Eden izmed serije standardov ITU-ISO s področja imenikov. Tudi del RFC 3280.

2. ODGOVORNOST ZA OBJAVE IN IMENIK

2.1. Objave dokumentov in imenik

V okviru infrastrukture javnih ključev na MO se informacije o overiteljih in digitalnih potrdilih objavljajo v imenikih in na spletni strani http://www.simod-pki.mors.si.

Imenik mora biti stalno dostopen. V primeru odpovedi dostopa mora operativno osebje overitelja pristopiti k odpravljanju napake v najkrajšem možnem času, tudi če rezervna kopija imenika normalno deluje.

Stalna dostopnost imenika v okviru infrastrukture javnih ključev na MO je zagotovljena z več vstopnimi točkami v imenik oziroma več ekvivalentnimi imeniki, tako da je vsakemu uporabniku zagotovljen dostop do digitalnih potrdil in registrov preklicanih potrdil ne glede na njihov položaj v segmentiranem omrežju v KIS MO in SV. Zagotovljeno mora biti medsebojno usklajevanje imenikov z namenom, da imajo vsi uporabniki dostopen vsaj en ažuren imenik.

Razen v izjemnih primerih, ko je določeni omrežni segment zaradi trenutne napake ali nezmožnosti povezave izoliran, morajo biti digitalna potrdila in registri preklicanih potrdil dostopni uporabnikom.

Pri povezovanju z drugimi KIS, ki niso pod upravljanjem MO in SV, se morajo opredeliti tudi načini in postopki zagotavljanja dostopnosti do imenika in spletne strani SIMoD-PKI uporabnikom drugih KIS.

2.2. Objave informacij o digitalnih potrdilih

Na spletni strani http://www.simod-pki.mors.si so objavljeni naslednji podatki:

- Politika SIMoD-PKI in pravila delovanja overiteljev,
- digitalno potrdilo korenskega overitelja,
- digitalna potrdila podrejenih overiteljev,
- registri preklicih potrdil in
- druge javne objave overiteljev.

Overitelji v imenikih objavljajo naslednje podatke:

- digitalna potrdila imetnikov in
- registre preklicanih potrdil:
    - delne registre ter
    - celotni register.

Imeniki so dostopni po protokolu LDAP.

Celotni register preklicanih potrdil je dostopen tudi po protokolu HTTP na spletnem naslovu navedenem v razširitvenem polju digitalnega potrdila, kot je navedeno v poglavju 7.1.2 Razširitvena polja.

Overitelji SIMoD-PKI morajo objaviti navodila uporabnikom za varno uporabo digitalnih potrdil in zahtevke za pridobitev, preklic ter druge storitve v zvezi z digitalnimi potrdili. Overitelji SIMoD-PKI morajo svojih pravilih delovanja navesti spletni naslov, na katerem so dokumenti dostopni.

Overitelji SIMoD-PKI si lahko pridržijo pravico, da nekaterih podatkov ne objavijo v vseh imenikih.

2.3. Čas in pogostost objav

Overitelj objavi digitalno potrdilo takoj, ko ga izda. Overitelj uvrsti preklicano digitalno potrdilo v register preklicanih potrdil takoj po opravljenem preklicu. Objava registrov preklicanih potrdil je v skladu s poglavji 4.9.7 Pogostost objav registrov preklicanih potrdil in 4.9.8 Dovoljene zakasnitve pri objavi registrov preklicanih potrdil.

2.4. Dostop do podatkov v imeniku in na spletni strani

Vpogled v podatke iz poglavja 2.2. Objave informacij o digitalnih potrdilih je brez omejitev.

Imeniki in spletna stran http://www.simod-pki.mors.si imajo vzpostavljene mehanizme za zagotavljanje celovitosti in razpoložljivosti podatkov.

3. PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI

3.1. Določanje imen

3.1.1. Vrste imen

Vsako izdano X.509v3 digitalno potrdilo vsebuje polje *Subject* z edinstvenim razločevalnim imenom imetnika - X.501 DN (ang. Distinguished Name, DN) v skladu z RFC 3280. Razločevalno ime je v digitalno potrdilo zapisano v obliki X.501 UTF8String in ni nikdar prazno. Imetnik ima lahko tudi eno ali več alternativnih imen, ki so zapisana v razširitvenem polju *subjectAltName* digitalnega potrdila, v skladu z RFC 3280.

3.1.2. Potreba po smiselnosti imen

Kratko razločevalno ime (ang. Relative Distinguished Name, RDN) mora enolično določati imetnika potrdila.

Splošno ime (ang. Common Name, CN) v digitalnih potrdilih za zaposlene vsebuje priimek in ime osebe ter številko zaposlenega iz kadrovske evidence.

Splošno ime v digitalnih potrdilih, kjer je imetnik organizacijska enota MO, institucija, vojaška dolžnost, funkcijska ali organizacijska vloga, izdajatelj varnih časovnih žigov ali drug ponudnik overjanja, mora enolično in nedvoumno označevati imetnika.

Splošno ime v digitalnih potrdilih za strežnike, drugo strojno ali programsko opremo je praviloma polno domensko ime (ang. fully qualified domain name, FQDN), oziroma mora enolično in nedvoumno označevati storitev.

Predlog za splošno ime je del zahtevka za izdajo digitalnega potrdila. Prijavna služba in operativno osebje overitelja si pridržujejo pravico za zavrnitev imena, če je neprimerno oziroma žaljivo, zavajajoče za tretje osebe, oziroma pripada neki drugi pravni ali fizični osebi ali je v nasprotju z veljavnimi predpisi. V teh primerih prijavna služba in operativno osebje overitelja predlaga drugačno ime.

3.1.3. Anonimnost imetnikov in uporaba psevdonimov

Uporaba psevdonimov ni dovoljena. Izdaja digitalnih potrdil z zakrito identiteto imetnika oziroma mehanizmi zagotavljanja anonimnosti niso predvideni.

3.1.4. Pravila za interpretacijo različnih oblik imen

Imena se interpretirajo v skladu z definicijami v poglavju 3.1.1 Vrste imen in 3.1.2 Potreba po smiselnosti imen.

3.1.5. Edinstvenost imen

Edinstvenost kratkega imena se po potrebi zagotovi z oznako (na primer številke) dodano splošnemu imenu.

3.1.6. Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk

Uporaba zaščitenih znamk v imenih je dovoljena samo nosilcem zaščitenih znamk. Overitelji SIMoD-PKI ne smejo zavestno izdati digitalnega potrdila z imenom, ki vsebuje zaščiteno znamko naročniku, ki ni nosilec zaščitene znamke. Prijavna služba in operativno osebje niso dolžni preverjati pravic do uporabe zaščitenih znamk niti razčiščevati sporov glede zaščitenih znamk.

Bodočim imetnikom ni dovoljeno zahtevati imen, ki bi kršila intelektualne ali avtorske pravice drugih, čeprav se v okviru SIMoD-PKI tega ne preverja niti ne bo Svet za upravljanje z infrastrukturo javnih ključev na MO posredoval v takšnih sporih. Prijavna služba in operativno osebje si pridržujejo pravico zavrniti izdajo digitalnega potrdila ali preklicati izdana digitalna potrdila udeležencev spora.

3.2. Preverjanje istovetnosti imetnikov ob prvi registraciji

3.2.1. Metode dokazovanja lastništva zasebnega ključa

Overitelji SIMoD-PKI morajo v postopku izdaje potrdila zagotoviti preverjanje lastništva zasebnega ključa z uporabo PKIX-CMP protokola v skladu z RFC 4210 Internet X.509 Public Key Infrastructure (PKI) Certificate Management protocol (CMP) ali PKCS#10 v skladu z RSA PKCS#10 Certification Request Syntax Standard.

3.2.2. Preverjanje istovetnosti za imetnike, ki niso fizične osebe

3.2.2.1. Digitalna potrdila za organizacijske enote MO in institucije, ki opravljajo naloge povezane z obrambo države

Zahtevek za pridobitev digitalnega potrdila za splošne nazive oziroma organizacijske enote MO ali institucije, ki opravljajo naloge povezane z obrambo države, mora vsebovati uradni naziv organizacijske enote MO ali institucije, naslov in ime odgovorne osebe, ki je praviloma vodja organizacijske enote MO oziroma predstojnik institucije. Za pravilnost podatkov jamči odgovorna oseba s podpisom na zahtevku.

Za zahtevke za pridobitev digitalnih potrdil SREDNJE in VISOKE stopnje zaupanja prijavna služba preveri podatke o odgovorni osebi v kadrovski evidenci; če je bodoči imetnik institucija, ki opravlja naloge povezane z obrambo države, lahko prijavna služba zahteva dodatna dokazila. Nato izvede osebno identifikacijo odgovorne osebe na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list ali vozniško dovoljenje).

Za zahtevke za pridobitev digitalnih potrdil NIZKE stopnje zaupanja preverjanje podatkov in osebna identifikacija ni obvezna. Zahtevke prejme in obdela operativno osebje overitelja.

3.2.2.2. Digitalna potrdila za organizacijske ali funkcijske vloge

Zahtevek za pridobitev digitalnega potrdila za organizacijsko ali funkcijsko vlogo podpišeta nosilec, skrbnik ali administrator vloge in njegov nadrejeni poveljnik oziroma vodja ustrezne organizacijske enote MO. Za pravilnost podatkov jamči poveljnik oziroma vodja s podpisom na zahtevku.

Za zahtevke za pridobitev digitalnih potrdil SREDNJE in VISOKE stopnje zaupanja, prijavna služba preveri pristnost podatkov nosilca, skrbnika ali administratorja vloge v kadrovski evidenci in izvede njegovo osebno identifikacijo na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list, ali vozniško dovoljenje).

Za zahtevke za pridobitev digitalnih potrdil NIZKE stopnje zaupanja preverjanje podatkov in osebna identifikacija ni obvezna. Zahtevke prejme in obdela operativno osebje overitelja.

3.2.2.3. Digitalna potrdila za strežnike, drugo strojno in programsko opremo, izdajatelje varnih časovnih žigov ter druge ponudnike storitev overjanja

Zahtevek za pridobitev digitalnega potrdila za strežnike, drugo strojno in programsko opremo, izdajatelje varnih časovnih žigov ter druge ponudnike storitev overjanja izpolnita in podpišeta skrbnik strežnika, druge strojne ali programske opreme, izdajatelja varnih časovnih žigov, drugega ponudnika storitve overjanja ter vodja ustrezne organizacijske enote MO ali institucije, ki opravlja naloge povezane z obrambo države.

Za zahtevke za pridobitev digitalnih potrdil SREDNJE in VISOKE stopnje zaupanja prijavna služba preveri podatke skrbnika v kadrovski evidenci; v primeru institucije, ki opravlja naloge povezane z obrambo države, pa lahko zahteva dodatna dokazila, da je bodoči skrbnik zaposlen v instituciji. Nato izvede osebno identifikacijo na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list, ali vozniško dovoljenje).

Za zahtevke za pridobitev digitalnih potrdil NIZKE stopnje zaupanja preverjanje podatkov in osebna identifikacija ni obvezna. Zahtevke prejme in obdela operativno osebje overitelja.

3.2.3. Preverjanje istovetnosti za fizične osebe

3.2.3.1. Zaposleni v MO in institucijah, ki opravljajo naloge povezane z obrambo države

Zahtevek za pridobitev digitalnega potrdila za zaposlene v MO in v institucijah, ki opravljajo naloge povezane z obrambo države, izpolnita in podpišeta bodoči imetnik in vodja njegove organizacijske enote oziroma predstojnik institucije. Za pravilnost podatkov jamči vodja organizacijske enote oziroma predstojnik institucije s podpisom na zahtevku.

Za zahtevek za pridobitev digitalnih potrdil SREDNJE in VISOKE stopnje zaupanja prijavna služba preveri podatke o bodočem imetniku v kadrovski evidenci; če je bodoči imetnik zaposlen v instituciji, ki opravlja naloge povezane z obrambo države, lahko prijavna služba zahteva dodatna dokazila, da je bodoči imetnik zaposlen v instituciji. Nato izvede osebno identifikacijo na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list ali vozniško dovoljenje).

Za zahtevke za pridobitev digitalnih potrdil NIZKE stopnje zaupanja preverjanje podatkov in osebna identifikacija ni obvezna. Zahtevke prejme in obdela operativno osebje overitelja.

3.2.3.2. Digitalna potrdila za vojaške dolžnosti v SV

Zahtevek za pridobitev digitalnega potrdila za vojaške dolžnosti v SV podpišeta nosilec vojaške dolžnosti v SV in njegov nadrejeni poveljnik oziroma, ko opravlja isto vojaško dolžnost več oseb, poveljnik enote. Za pravilnost podatkov jamči poveljnik s podpisom na zahtevku.

Za zahtevke za pridobitev digitalnih potrdil SREDNJE in VISOKE stopnje zaupanja prijavna služba preveri pristnost podatkov nosilca vojaške dolžnosti v SV oziroma, ko opravlja isto vojaško dolžnost več oseb poveljnika enote, v kadrovski evidenci in izvede njegovo osebno identifikacijo na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list, ali vozniško dovoljenje).

Za zahtevke za pridobitev digitalnih potrdil NIZKE stopnje zaupanja preverjanje podatkov in osebna identifikacija ni obvezna. Zahtevke prejme in obdela operativno osebje overitelja.

3.2.4. Podatki o naročniku, ki se ne preverjajo

Prijavna služba ne preverja naslednjih podatkov, ki bodo vsebovani v digitalnem potrdilu:

- splošni naziv oziroma ime organizacijske enote MO ali institucije,
- obstoj funkcijske ali organizacijske vloge ali vojaške dolžnosti v SV,
- ali je naročnik res nosilec vojaške dolžnosti v SV,
- naziv strežnika in druge strojne ali programske opreme in
- naziv izdajatelja varnih časovnih žigov ali drugega ponudnika overjanja.

Za pravilnost zgoraj navedenih podatkov jamči vodja organizacijske enote, predstojnik institucije oziroma poveljnik enote SV.

3.2.5. Preverjanje pooblastil

Vodja organizacijske enote MO ali predstojnik institucije, ki opravlja naloge povezane z obrambo, oziroma poveljnik enote SV s podpisom na zahtevku za pridobitev digitalnega

potrdila jamči, da želi za določeno osebo, da le-ta pridobi digitalno potrdilo zase, za organizacijsko enoto MO, institucijo, vojaško dolžnost, funkcijsko ali organizacijsko vlogo, strežnik, drugo strojno ali programsko opremo, izdajatelja varnih časovnih žigov ali ponudnika storitve overjanja.

3.2.6. Merila za medsebojno povezovanje

Medsebojno povezovanje je mogoče samo na nivoju korenskega overitelja. Način in pogoji medsebojnega povezovanja bodo določeni s pogodbo o medsebojnem zaupanju overiteljev. Pogodba o medsebojnem zaupanju overiteljev je obvezna za vse možne načine medsebojnega povezovanja.

Minimalni pogoji za medsebojno povezovanje:

- pogodba o medsebojnem zaupanju,
- zadostno ujemanje politik digitalnih potrdil, za katere velja medsebojno zaupanje, ki ga ugotavlja Svet za upravljanje z infrastrukturo javnih ključev na MO in
- dokazilo overitelja, s katerim se vzpostavlja medsebojno zaupanje, da res izvaja postopke v skladu s politiko digitalnih potrdil, za katero se vzpostavlja medsebojno zaupanje, pred vzpostavitvijo medsebojnega zaupanja in vsaj enkrat letno.

3.3. Preverjanje imetnikov za ponovno izdajo digitalnega potrdila

3.3.1. Preverjanje istovetnosti pri rutinski ponovni izdaji digitalnih potrdil

Ob rutinski ponovni izdaji digitalnih potrdil, ki so bila izdana po protokolu PKIX-CMP, imetnik izkaže svojo istovetnost s posedovanjem še veljavnega zasebnega ključa.

Rutinska ponovna izdaja digitalnih potrdil izdanih z uporabo PKCS#10 protokola ni možna. Dovoljena je ponovna izdaja digitalnega potrdila brez osebnega preverjanja istovetnosti imetnika, če je elektronski zahtevek za ponovno izdajo podpisan z veljavnim digitalnim potrdilom. Imetnik izkaže svojo istovetnost s posedovanjem še veljavnega zasebnega ključa.

3.3.2. Preverjanje istovetnosti za ponovno izdajo digitalnega potrdila po preklicu

Za ponovno pridobitev digitalnega potrdila po preklicu je potrebno ponoviti postopek v skladu s poglavjem 3.2. Preverjanje istovetnosti imetnikov ob prvi registraciji.

S pravili delovanja posameznega overitelja so lahko določeni drugačni načini preverjanja istovetnosti za ponovno izdajo digitalnega potrdila v izjemnih primerih.

3.4. Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila

Oseba, ki želi preklicati digitalno potrdilo, se identificira:

- z veljavnim digitalnim podpisom na zahtevku za preklic digitalnega potrdila,
- z lastnoročnim podpisom na zahtevku za preklic digitalnega potrdila ali
- ob telefonski zahtevi za preklic s skrivnim geslom, ki ga je imetnik izbral ob oddaji zahtevka za izdajo digitalnega potrdila.

Osebna identifikacija ni obvezna.

4. UPRAVLJANJE Z DIGITALNIMI POTRDILI

4.1. Pridobitev digitalnega potrdila

4.1.1. Kdo lahko zaprosi za izdajo digitalnega potrdila

Zahtevek za pridobitev digitalnega potrdila za fizične osebe lahko oddajo zaposleni v MO in v institucijah, ki opravljajo naloge povezane z obrambo.

Zahtevek za pridobitev digitalnega potrdila za organizacijske enote MO ali institucije, ki opravljajo naloge povezane z obrambo države, oddajo predstojniki organizacijske enote vsaj na ravni vodje sektorja za organizacijske enote MO oziroma predstojniki institucij.

Zahtevek za pridobitev digitalnega potrdila za vojaške dolžnosti lahko oddajo nosilci vojaških dolžnosti oziroma v primeru, ko opravlja isto vojaško dolžnost več oseb (npr. dežurni poveljstva), poveljnik enote SV, v okviru katere je vzpostavljena vojaška dolžnost.

Zahtevek za pridobitev digitalnega potrdila za funkcijske ali organizacijske vloge lahko oddajo nosilci, skrbniki ali administratorji vloge.

Zahtevek za pridobitev digitalnih potrdil za strežnike, drugo strojno in programsko opremo, izdajatelje varnih časovnih žigov ali drugih ponudnikov storitev overjanja, oddajo skrbniki opreme.

4.1.2. Postopek bodočega imetnika za pridobitev digitalnega potrdila in odgovornosti

Zahtevki za pridobitev digitalnega potrdila in navodila za izpolnjevanje ter oddajo zahtevkov so dostopni na spletni strani: http://www.simod-pki.mors.si.

Naročnik odda izpolnjen in podpisan zahtevek za pridobitev digitalnega potrdila SREDNJE in VISOKE stopnje zaupanja v prijavno službo osebno. Prijavna služba deluje v okviru rednega delovnega časa oziroma uradnih ur.

Naročnik posreduje izpolnjen in podpisan zahtevek za izdajo digitalnega potrdila NIZKE stopnje zaupanja operativnemu osebju ustreznega overitelja SIMoD-PKI.

4.2. Obdelava zahtevka za izdajo digitalnega potrdila

4.2.1. Preverjanje istovetnosti bodočega imetnika

Prijavna služba preveri zahtevek za izdajo digitalnega potrdila SREDNJE in VISOKE stopnje zaupanja in preveri istovetnost naročnika v skladu s poglavji 3.2.2 Preverjanje istovetnosti za imetnike, ki niso fizične osebe in 3.2.3 Preverjanje istovetnosti za fizične osebe.

Za digitalna potrdila NIZKE stopnje zaupanja se istovetnost naročnika ne preverja.

4.2.2. Odobritev ali zavrnitev izdaje digitalnega potrdila

Zahtevek za pridobitev digitalnega potrdila overitelja ne obvezuje k izdaji digitalnega potrdila.

V primeru pomanjkljivih podatkov, neupravičenosti do digitalnega potrdila ali neuspešnega preverjanja istovetnosti prijavna služba zavrne izdajo digitalnega potrdila SREDNJE ali VISOKE stopnje zaupanja.

V primeru pomanjkljivih podatkov ali neupravičenosti do digitalnega potrdila NIZKE stopnje zaupanja operativno osebje overitelja zavrne izdajo digitalnega potrdila.

Odobritev ali zavrnitev izdaje digitalnega potrdila SREDNJE ali VISOKE stopnje zaupanja je odgovornost in pravica prijavne službe. Obvestilo o zavrnitvi pošlje prijavna služba naročniku po elektronski pošti, odobritev zahtevka pa prijavna služba na varen način (v zapečateni kuverti) posreduje operativnemu osebju ustreznega overitelja.

Odobritev ali zavrnitev izdaje digitalnega potrdila NIZKE stopnje zaupanja je odgovornost in pravica operativnega osebja overitelja. Obvestilo o zavrnitvi pošlje operativno osebje overitelja naročniku po elektronski pošti.

Naročnik je o odobritvi izdaje digitalnega potrdila obveščen hkrati s prejemom aktivacijskih podatkov ali pametne kartice z digitalnim potrdilom.

4.2.3. Čas za obdelavo zahtevka za izdajo digitalnega potrdila

Največji dopusten čas od sprejema zahtevka za pridobitev digitalnega potrdila in izdajo aktivacijskih podatkov, ki jih bodoči imetnik potrebuje za generiranje ključev, je enaindvajset (21) dni.

4.3. Izdaja digitalnega potrdila

4.3.1. Postopki overiteljev SIMoD-PKI ob izdaji potrdil

Operativno osebje overitelja začne s postopki izdajanja digitalnega potrdila SREDNJE in VISOKE stopnje zaupanja po prejemu odobrenega zahtevka od prijavne službe.

Operativno osebje overitelja začne s postopki izdajanja digitalnega potrdila NIZKE stopnje zaupanja po prejemu in odobritvi zahtevka.

Operativno osebje overitelja preveri pravilnost in veljavnost naslovov elektronske pošte bodočega imetnika. V primeru nepravilnega ali neveljavnega elektronskega naslova zadrži postopek izdajanja digitalnega potrdila dokler se problem ne razreši. Če v roku iz poglavja 4.2.3 Čas za obdelavo zahtevka za izdajo digitalnega potrdila problem ni odpravljen, se izdaja digitalnega potrdila zavrne.

Operativno osebje overitelja po uspešnem preverjanju veljavnosti naslovov elektronske pošte izvede rezervacijo razločevalnega imena in generiranje aktivacijskih podatkov.

Operativno osebje overitelja pošlje bodočemu imetniku obvestilo o odobritvi izdaje digitalnega potrdila in aktivacijske podatke, razdeljene v dva dela; referenčno številko po elektronski pošti, avtorizacijsko kodo pa v kuverti, zaščiteni pred nepooblaščenim pregledovanjem, po pošti s potrdilom o prevzemu.

Za digitalna potrdila z obvezno uporabo pametne kartice, kjer overitelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, overitelj bodočemu imetniku ne pošilja aktivacijskih podatkov.

4.3.1.1. Dostava zasebnega ključa imetniku

Ko bodoči imetnik sam generira ključe, kot je to v primeru ključev za podpisovanje, ni potrebe po prenašanju zasebnih ključev. Zasebni ključ za podpisovanje se mora obvezno generirati pri imetniku in mora biti vedno pod kontrolo imetnika. Overitelj v nobenem trenutku ne poseduje in ne hrani kopije zasebnih ključev za podpisovanje.

Ko overitelj generira zasebne ključe, kot je to v primeru dešifrirnih ključev s podporo za povrnitev zgodovine ključev, poteka prenos zasebnega ključa z uporabo protokola PKIX-CMP in je integralni del postopka za prevzem digitalnega potrdila.

Za digitalna potrdila z obvezno uporabo pametne kartice, kjer overitelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, generira ključe overitelj.

4.3.1.2. Dostava overiteljevega javnega ključa imetniku

Javni ključ overitelja oziroma overiteljevo digitalno potrdilo, ki vsebuje overiteljev javni ključ, se pošlje bodočim imetnikom digitalnih potrdil, ki se prevzemajo po PKIX-CMP protokolu, v sklopu PKIX-CMP protokola kot integralni del postopka za prevzem digitalnega potrdila.

Javni ključ overitelja oziroma overiteljevo digitalno potrdilo, ki vsebuje overiteljev javni ključ, se pošlje bodočim imetnikom digitalnih potrdil, ki se izdajajo na osnovi PKCS#10 zahtevka, po protokolu PKCS#7 kot integralni del postopka za prevzem digitalnega potrdila.

Overiteljevo digitalno potrdilo lahko uporabniki pridobijo tudi kadarkoli iz imenika, vendar morajo preveriti istovetnost overitelja in celovitost overiteljevega digitalnega potrdila.

4.3.2. Obvestilo naročnikom o izdaji digitalnega potrdila

Operativno osebje overitelja obvesti bodočega imetnika o odobritvi izdaje digitalnega potrdila z istim elektronskim sporočilom, s katerim mu pošilja referenčno številko, in z obvestilom po pošti, s katerim mu pošilja avtorizacijsko kodo.

Za digitalna potrdila z obvezno uporabo pametne kartice, kjer overitelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, velja, da je bodoči imetnik prejel obvestilo o izdaji potrdila, ko prevzeme pametno kartico z digitalnim potrdilom.

Digitalno potrdilo je izdano, ko ga overitelj objavi v imeniku iz poglavja 2.2. Objave informacij o digitalnih potrdilih.

4.4. Prevzem digitalnega potrdila

4.4.1. Postopek prevzema digitalnega potrdila

V okviru SIMoD-PKI sta izdaja in prevzem digitalnega potrdila neločljivo povezana. Bodoči imetnik lahko prevzame digitalno potrdilo samo z ustreznimi aktivacijskimi podatki: referenčno številko in avtorizacijsko kodo.

Veljavnost aktivacijskih podatkov je šestdeset (60) dni od izdaje aktivacijskih podatkov.

Postopek prevzema je odvisen od strojne in programske opreme na strani uporabnika in posameznega overitelja. Overitelji morajo v svojih pravilih delovanja opisati postopek prevzema oziroma objaviti uporabniška navodila za prevzem digitalnih potrdil.

Za digitalna potrdila z obvezno uporabo pametne kartice, kjer overitelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, opravi prevzem digitalnega potrdila overitelj. Overitelj nato pametno kartico s prevzetim digitalnim potrdilom na varen način posreduje imetniku.

Ob prevzemu digitalnega potrdila je imetnik dolžan preveriti vsebino digitalnega potrdila, ali je digitalno potrdilo podpisal pravi overitelj ter polno pot digitalnih podpisov do korenskega overitelja. S prvo uporabo oziroma če imetnik osem (8) dni od prevzema digitalnega potrdila overitelja ne obvesti o morebitnih napakah, velja, da je imetnik potrdil točnost podatkov v digitalnem potrdilu in da prevzema tudi vse obveznosti in jamstva iz poglavja 9.6.3 Odgovornost in jamstva imetnikov digitalnih potrdil.

4.4.2. Objava digitalnega potrdila

Digitalno potrdilo z javnim ključem za šifriranje je po izdaji objavljeno v imenikih iz poglavja 2.2. Objave informacij o digitalnih potrdilih. Overitelji lahko v imenikih objavijo tudi digitalna potrdila z javnim ključem za preverjanje digitalnega podpisa.

4.4.3. Obveščanje drugih udeležencev o izdaji digitalnega potrdila

Ni predvideno.

4.5. Uporaba ključev in digitalnih potrdil

Dovoljena je uporaba ključev in digitalnih potrdil kot je definirano v razširitvenem polju v digitalnem potrdilu *KeyUsage* in *extKeyUsage* (glej poglavje 6.1.7 Namen uporabe ključev) in za namene kot je določeno v poglavju 1.4.1 Dovoljena uporaba digitalnih potrdil

4.5.1. Uporaba ključev in digitalnih potrdil imetnikov

4.5.1.1. Zasebni ključi in digitalna potrdila overiteljev

Korenski overitelj lahko uporablja svoj zasebni ključ samo za podpisovanje digitalnih potrdil podrejenih in medsebojno priznanih overiteljev, registrov preklicanih overiteljev in digitalnih potrdil svojega operativnega osebja. Korenski overitelj ne izdaja uporabniških digitalnih potrdil.

Podrejeni overitelji SIMoD-PKI lahko uporabljajo svoje zasebne ključe samo za podpisovanje digitalnih potrdil in registrov preklicanih potrdil. Podrejeni overitelji podpisujejo digitalna potrdila za uporabnike storitev infrastrukture javnih ključev na MO, ki so določeni v poglavju 1.3.3 Imetniki digitalnih potrdil, operativno osebje posameznega overitelja in osebje prijavne službe.

Operativno osebje overiteljev SIMoD-PKI uporablja digitalna potrdila in pripadajoče ključe izključno za izvajanje nalog upravljanja z infrastrukturo posameznega overitelja. V primeru, da overiteljevi zaposleni potrebujejo ključe oziroma digitalna potrdila kot uporabniki oziroma za druge namene, kot je upravljanje z overiteljevo infrastrukturo, morajo zaprositi za izdajo uporabniških digitalnih potrdil.

4.5.1.2. Zasebni ključi in digitalna potrdila prijavne službe

Osebje prijavne službe lahko uporablja digitalna potrdila, izdana za izvajanje nalog prijavne službe, samo za te namene. V primeru, da zaposleni prijavne službe potrebujejo ključe oziroma digitalna potrdila kot uporabniki oziroma za druge namene kot je delo v prijavni službi, morajo zaprositi za izdajo uporabniških digitalnih potrdil.

4.5.1.3. Uporabniški zasebni ključi in digitalna potrdila

Imetnik digitalnega potrdila je dolžan:

- uporabljati ključe in digitalna potrdila samo za namene, ki so definirani v Politiki SIMoD-PKI in pravilih delovanja overitelja,
- po prevzemu digitalnega potrdila preveriti podatke v digitalnem potrdilu in ob morebitnih napakah in problemih takoj obvestiti operativno osebje overitelja oziroma zahtevati preklic digitalnega potrdila,
- vse spremembe, ki so povezane s digitalnimi potrdili, v osmih (8) dneh sporočiti prijavni službi ali operativnemu osebju overitelja,
- uporabljati zasebne ključe in digitalna potrdila samo v obdobju njihove veljavnosti,
- digitalno podpisovati in/ali šifrirati le podatke, katerih veljavnost je krajša od veljavnosti digitalnega potrdila oziroma pred potekom veljavnosti digitalnega potrdila ponovno podpisati in/ali šifrirati podatke, če to ni rešeno na drug način (z aplikacijo),
- varovati svoje zasebne ključe in pametne kartice ali drugačne nosilce zasebnih ključev in upoštevati vse ukrepe, da se prepreči izguba, razkritje, sprememba ali nepooblaščena uporaba in
- ob sumu zlorabe svojega zasebnega ključa ukrepati po postopku, ki je opisan v poglavju 4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila.

4.5.2. Uporaba digitalnih potrdil s strani tretjih oseb

Tretja oseba je dolžna:

- pred uporabo digitalnega potrdila preveriti, ali je ustrezno za predvideno uporabo,
- uporabiti digitalno potrdilo le za namene, določene v Politiki SIMoD PKI, pravilih delovanja overitelja oziroma pogodbi o medsebojnem priznavanju,
- ob domnevni zlorabi zasebnega ključa ali če so spremenjeni podatki iz digitalnega potrdila, na katerega se zanaša, obvestiti operativno osebje overitelja,
- preveriti, če je bil digitalni podpis kreiran v času veljavnosti digitalnega potrdila,
- za vsako uporabljeno digitalno potrdilo izvesti popoln postopek preverjanja poti zaupanja,
- preveriti status digitalnega potrdila v veljavnem registru preklicanih potrdil in
- skrbeti za arhiv dokumentov.

4.6. Ponovna izdaja digitalnega potrdila brez spremembe javnega ključa

Obnova digitalnih potrdil oziroma ponovna izdaja digitalnega potrdila brez spremembe javnega ključa ni dovoljena.

4.7. Ponovna izdaja digitalnih potrdil[6]

4.7.1. Razlogi za ponovno izdajo digitalnega potrdila

Ponovna izdaja digitalnega potrdilo se izvede:

- po preklicu,
- po preteku veljavnosti,
- pred pretekom veljavnosti ali
- če je imetnik v obdobju veljavnosti digitalnega potrdila:
    - pozabil geslo za dostop do zasebnih ključev ali
    - izgubil ali poškodoval pametno kartico ali drugačen nosilec zasebnih ključev.

4.7.2. Kdo lahko zahteva ponovno izdajo digitalnega potrdila

Ponovno izdajo digitalnega potrdila lahko zaprosijo imetniki, oziroma isti subjekti, kot za prvo izdajo, skladno s poglavjem 4.1.1 Kdo lahko zaprosi za izdajo digitalnega potrdila.

4.7.3. Obdelava zahtevkov za ponovno izdajo digitalnega potrdila

Za ponovno izdajo digitalnega potrdila po preklicu in preteku veljavnosti oddajo uporabniki enak zahtevek, kot za prvo pridobitev digitalnega potrdila. Potrebno je ponoviti postopke od 4.1. Pridobitev digitalnega potrdila do 4.4. Prevzem digitalnega potrdila.

S pravili delovanja posameznega overitelja so lahko določeni drugačni postopki obdelave zahtevka za ponovno izdajo digitalnega potrdila v izjemnih primerih.

Ponovna izdaja digitalnih potrdil pred pretekom veljavnosti se za digitalna potrdila po protokolu PKIX-CMP izvede samodejno pred pretekom veljavnosti digitalnega potrdila. Postopek imenujemo tudi rutinska ponovna izdaja digitalnih potrdil.

6 Ponovna izdaja digitalnega potrdila za preverjanje digitalnega podpisa in digitalnega potrdila za preverjanje digitalnega podpisa in šifriranje pomeni generiranje novega para ključev in novega digitalnega potrdila.
Ponovna izdaja digitalnega potrdila za šifriranje pomeni generiranje novega para ključev in novega digitalnega potrdila ter praviloma tudi povrnitev zgodovine ključev v skladu s poglavjem 4.12.1 Povrnitev zgodovine ključev za dešifriranje.

Ponovna izdaja digitalnih potrdil pred pretekom veljavnosti se za digitalna potrdila po protokolu PKCS#10 protokola izvede na osnovi ustreznega elektronskega zahtevka, ki je podpisan z veljavnim digitalnim potrdilom.

Zahtevek za ponovno izdajo digitalnega potrdila se obdeluje smiselno enako kot zahtevek za prvo pridobitev digitalnega potrdila skladu s poglavji 4.1. Pridobitev digitalnega potrdila in 4.2. Obdelava zahtevka za izdajo digitalnega potrdila.

Generiranje novih parov ključev ob rutinski ponovni izdaji digitalnega potrdila po protokolu PKIX-CMP se izvede ob prvi uporabi digitalnega potrdila z neposrednim dostopom do overitelja v obdobju stotih (100) dni pred zadnjim dnem veljavnosti zasebnega ključa. Generiranje novih parov ključev je možno samo v primeru, da je digitalno potrdilo, ki ga trenutno poseduje imetnik, veljavno.

Ponovno izdajo digitalnih potrdil brez preverjanja istovetnosti je možno izvesti dvakrat (2x) zaporedoma.

Ponovna izdaja digitalnih potrdil overiteljev in izdajateljev varnih časovnih žigov mora biti pod kontrolo operativnega osebja SIMoD-PKI.

Za ponovno izdana digitalna potrdila velja politika, veljavna ob datumu generiranja novih parov ključev.

4.7.4. Obvestilo imetniku o izdaji novega digitalnega potrdila

Ob rutinski ponovni izdaji digitalnega potrdila po protokolu PKIX-CMP namenska programska oprema imetnika obvesti o uspešnem prevzemu digitalnega potrdila.

Za digitalna potrdila, ki so ponovno izdana na osnovi zahtevka, prejmejo imetniki obvestilo o izdaji skladno s poglavjem 4.3.2 Obvestilo naročnikom o izdaji digitalnega potrdila.

4.7.5. Postopek potrditve prevzema novega digitalnega potrdila

Enako kot 4.4.1 Postopek prevzema digitalnega potrdila.

4.7.6. Objava novega digitalnega potrdila

Enako kot 4.4.2 Objava digitalnega potrdila.

4.7.7. Obveščanje drugih udeležencev o izdaji digitalnega potrdila

Enako kot 4.4.3 Obveščanje drugih udeležencev o izdaji digitalnega potrdila.

4.8. Sprememba digitalnega potrdila

Sprememba digitalnega potrdila ni možna. Ob spremembah podatkov, vsebovanih v digitalnem potrdilu, je potrebno digitalno potrdilo preklicati.

4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila

4.9.1. Okoliščine preklica

4.9.1.1. Okoliščine preklica imetniških digitalnih potrdil

Razlogi za preklic digitalnih potrdil imetnikov so:

- dejanska ali domnevna zloraba zasebnih ključev,
- neizpolnjevanje obveznosti iz Politike SIMoD-PKI ali pravil delovanja overitelja,

- sprememba podatkov, ki so vsebovani v digitalnem potrdilu in
- razlogi, navedeni v poglavju 4.11. Predčasna prekinitev veljavnosti digitalnih potrdil.

4.9.1.2. Okoliščine preklica digitalnega potrdila korenskega overitelja

Razlogi za preklic digitalnega potrdila korenskega overitelja so:

- domnevna ali dejanska zloraba zasebnega ključa,
- nezmožnost pravočasne ponovne vzpostavitve delovanja po okvari oziroma nesreči,
- odločitev inšpekcije,
- prenehanje delovanja ali
- druge okoliščine, ki lahko ogrozijo zaupanje v digitalno potrdilo korenskega overitelja.

4.9.1.3. Okoliščine preklica digitalnega potrdila o priznavanju drugega overitelja

Korenski overitelj prekliče digitalno potrdilo o priznavanju drugega overitelja iz naslednjih razlogov:

- dejanska ali domnevna zloraba zasebnih ključev drugega overitelja,
- spremembe podatkov o drugem overitelju, tako da je potrebno izdati novo digitalno potrdilo o priznavanju drugega overitelja,
- preklic digitalnega potrdila drugega overitelja,
- drugi primeri, določeni v pogodbi o medsebojnem priznavanju ali
- neizpolnjevanje obvez iz pogodbe o medsebojnem priznavanju.

4.9.1.4. Okoliščine preklica digitalnega potrdila podrejenega overitelja

Razlogi za preklic digitalnega potrdila podrejenega overitelja so:

- domnevna ali dejanska zloraba zasebnega ključa,
- nezmožnost pravočasne ponovne vzpostavitve delovanja po okvari oziroma nesreči,
- odločitev inšpekcije,
- prenehanje delovanja,
- preklic digitalnega potrdila korenskega overitelja ali
- druge okoliščine, ki lahko ogrozijo zaupanje v digitalno potrdilo overitelja.

4.9.2. Kdo lahko zahteva preklic

4.9.2.1. Kdo lahko zahteva preklic digitalnega potrdila imetnika

Zahtevo za preklic digitalnega potrdila imetnika lahko poda:

- imetnik za svoje digitalno potrdilo,
- vodja organizacijske enote MO oziroma predstojnik institucije, ki je povezana z obrambo države,
- nosilec vojaške dolžnosti ali poveljnik enote, v okviru katere je vzpostavljena vojaška dolžnost,
- nosilec, skrbnik oziroma administrator funkcijske ali organizacijske vloge ali njegov nadrejeni oziroma predstojnik ustrezne organizacijske enote MO,
- skrbnik strežnika, druge strojne ali programske opreme, izdajatelja varnih časovnih žigov, ponudnika storitev overjanja,
- operativno osebje overiteljev, ki opravlja naloge prvega ali drugega varnostnega inženirja, če sumi, da imetnik krši pravila varnega ravnanja z digitalnim potrdilom ali
- tretja oseba, če utemeljeno sumi, da je pri določenemu imetniku prišlo do zlorabe zasebnih ključev.

4.9.2.2. Kdo lahko zahteva preklic digitalnega potrdila korenskega overitelja

Preklic digitalnega potrdila korenskega overitelja lahko zahteva:

- Svet za upravljanje z infrastrukturo javnih ključev na MO ali
- pristojni inšpektor v skladu s poglavjem 8 Preverjanje skladnosti in ostale oblike nadzora.

4.9.2.3. Kdo lahko zahteva preklic digitalnega potrdila o priznavanju drugega overitelja

Preklic digitalnega potrdila o priznavanju drugega overitelja zahteva:

- Svet za upravljanje z infrastrukturo javnih ključev na MO ali
- medsebojno priznani overitelj.

4.9.2.4. Kdo lahko zahteva preklic digitalnega potrdila podrejenega overitelja

Preklic digitalnega potrdila overitelja lahko zahteva:

- Svet za upravljanje z infrastrukturo javnih ključev na MO ali
- pristojni inšpektor v skladu s poglavjem 8 Preverjanje skladnosti in ostale oblike nadzora.

4.9.3. Postopki za preklic

4.9.3.1. Postopki preklica digitalnih potrdil imetnikov

Načini posredovanja zahtevkov za preklic:

- poslati digitalno podpisano elektronsko sporočilo operativni osebi overitelja ali na skupinski elektronski naslov overitelja,
- kot zahtevek v elektronskem dokumentacijskem sistemu, podpisan z veljavnim digitalnim potrdilom, posredovan operativnemu osebju overitelja,
- kot lastnoročno podpisani zahtevek za preklic posredovan operativnemu osebju overitelja ali
- po telefonu na dežurno številko za preklic.

V primeru telefonsko posredovanega zahtevka dežurna oseba posreduje zahtevek za preklic operativnemu osebju overitelja.

Preklic izvrši operativno osebje overitelja.

Preklic lahko po lastni presoji izvede prvi ali drugi varnostni inženir na podlagi ocene o domnevni ali dejanski zlorabi zasebnega ključa. Odločitev mora biti utemeljena in zabeležena.

Po preklicu mora overitelj objaviti preklicano digitalno potrdilo v registru preklicanih potrdil.

Operativno osebje overitelja o preklicu digitalnega potrdila po elektronski pošti ali pismeno obvesti imetnika ali odgovorno osebo.

Za izdajo novega digitalnega potrdila po preklicu je potrebno ponoviti postopek kot za prvo pridobitev digitalnega potrdila v skladu s poglavji 4.1. Pridobitev digitalnega potrdila do 4.4. Prevzem digitalnega potrdila.

4.9.3.2. Postopki preklica digitalnega potrdila korenskega overitelja

Preklic digitalnega potrdila korenskega overitelja izvedeta prvi in drugi varnostni inženir korenskega overitelja na zahtevo Sveta za upravljanje z infrastrukturo javnih ključev na MO.

Korenski overitelj mora ob preklicu svojega digitalnega potrdila izvesti naslednje postopke:

- preklicati vsa digitalna potrdila,
- zagotavljati razpoložljivost registrov preklicanih overiteljev vsaj še devetdeset (90) dni od preklica svojega digitalnega potrdila,

- objaviti preklic digitalnega potrdila v registru preklicanih overiteljev,
- javno objaviti obvestilo o preklicu svojega potrdila na spletni strani http://www.simod-pki.mors.si
- ustvariti nove ključe in generirati novo samopodpisano potrdilo in
- izdati podrejenim overiteljem nova digitalna potrdila.

4.9.3.3. Postopki preklica digitalnega potrdila o priznavanju drugega overitelja

Preklic potrdila o priznavanju drugega overitelja izvedeta prvi in drugi varnostni inženir korenskega overitelja na zahtevo Sveta za upravljanje z infrastrukturo javnih ključev na MO.

Postopek preklica digitalnega potrdila o priznavanju drugega overitelja je opredeljen v pogodbi o medsebojnem priznavanju.

Preklicano digitalno potrdilo mora bit objavljeno v registru preklicanih overiteljev.

4.9.3.4. Postopki preklica digitalnega potrdila podrejenega overitelja

Preklic potrdila podrejenega overitelja izvedeta prvi ali drugi varnostni inženir korenskega overitelja na zahtevo Sveta za upravljanje z infrastrukturo javnih ključev na MO.

Podrejeni overitelj mora ob preklicu svojega digitalnega potrdila izvesti naslednje postopke:

- preklicati vsa digitalna potrdila,
- zagotavljati razpoložljivost registrov preklicanih potrdil vsaj še devetdeset (90) dni od preklica svojega digitalnega potrdila,
- ustvariti nove ključe in
- izdati imetnikom nova digitalna potrdila.

Korenski overitelj mora ob preklicu digitalnega potrdila podrejenega overitelja izvesti naslednje postopke:

- preklicano digitalno potrdilo objaviti v registru preklicanih overiteljev,
- javno objaviti obvestilo o preklicu potrdila podrejenega overitelja na spletni strani http://www.simod-pki.mors.si.

4.9.4. Čas za posredovanje zahtevka za preklic

Osebe, ki lahko zahtevajo preklic (glej poglavje 4.9.2 Kdo lahko zahteva preklic), morajo posredovati zahtevek za preklic takoj, ko zvejo za okoliščino preklica.

4.9.5. Čas od prejema zahtevka za preklic do preklica

4.9.5.1. Čas za preklic digitalnega potrdila imetnika

Operativno osebje izvede preklic v osmih (8) urah po prejemu zahtevka za preklic v primeru:

- dejanske ali domnevne zlorabe zasebnih ključev ali
- neizpolnjevanja obveznosti po Politiki SIMoD-PKI ali pravilih delovanja overitelja.

Operativno osebje izvede preklic v štiriindvajsetih (24) urah po prejemu zahtevka za preklic v primeru:

- spremembe podatkov v digitalnem potrdilu,
- prenehanja delovnega razmerja imetnika,
- prenehanja delovanja organizacijske enote MO ali institucije, ki je povezana z obrambo države, ukinitve vojaške dolžnosti, organizacijske ali funkcijske vloge,
- spremembe statusa imetnika, zaposlenega v instituciji, ki je povezana z obrambo države, ki ima za posledico dejstvo, da imetnik ne opravlja več nalog povezanih z obrambo države ali
- spremembe statusa institucije, ki je povezana z obrambo države, ki ima za posledico dejstvo, da institucija ne opravlja več nalog povezanih z obrambo države.

24-urni rok velja za primere, ko je bila sprememba v času oddaje zahtevka že v veljavi. V primerih, ko je bil zahtevek oddan pred uveljavitvijo spremembe, se preklic opravi na dan uveljavitve spremembe.

4.9.5.2. Čas za preklic digitalnega potrdila korenskega overitelja

Korenski overitelj prekliče svoje samopodpisano digitalno potrdilo takoj, ko prejme zahtevek, ali v roku, ki ga določi Svet za upravljanje z infrastrukturo javnih ključev na MO.

4.9.5.3. Čas za preklic digitalnega potrdila o priznavanju drugega overitelja

V primeru medsebojnega priznavanja korenski overitelj prekliče digitalno potrdilo o priznavanju drugega overitelja najkasneje v osmih (8) urah, če so okoliščine preklica:

- dejanska ali domnevna zloraba zasebnih ključev drugega overitelja,
- preklic digitalnega potrdila drugega overitelja ali
- neizpolnjevanje obveznosti iz pogodbe o medsebojnem priznavanju.

V primeru medsebojnega priznavanja korenski overitelj prekliče digitalno potrdilo o priznavanju drugega overitelja v roku štiriindvajset (24) ur, če je okoliščina preklica sprememba podatkov o drugem overitelju, tako da je potrebno izdati novo digitalno potrdilo o priznavanju drugega overitelja.

24-urni rok velja za primere, ko je bila sprememba v času oddaje zahtevka že v veljavi. V primerih, ko je bil zahtevek oddan pred uveljavitvijo spremembe, se preklic opravi na dan uveljavitve spremembe.

4.9.5.4. Čas za preklic digitalnega potrdila podrejenega overitelja

Korenski overitelj prekliče digitalna potrdila podrejenih overiteljev takoj, ko prejme zahtevek, ali v roku, ki ga določi Svet za upravljanje z infrastrukturo javnih ključev na MO.

4.9.6. Obveza preverjanja registra preklicanih potrdil

Tretje osebe, ki se zanašajo na digitalno potrdilo, so pred uporabo dolžne preveriti najnovejši register preklicanih potrdil. Kot del postopka preverjanja je potrebno preveriti tudi veljavnost in verodostojnost registra preklicanih potrdil. Tretja oseba mora za vsako uporabljeno digitalno potrdilo izvesti popoln postopek preverjanja poti zaupanja v skladu z RFC 3280.

Uporaba digitalnih potrdil v aplikacijah, ki ne preverjajo statusa digitalnih potrdil, praviloma ni dovoljena, razen v nujnih primerih, ko je potrebno takojšnje ukrepanje.

Če tretja oseba ne more preveriti veljavnosti digitalnega potrdila v registru preklicanih potrdil, ima dve možnosti:

- zavrne uporabo digitalnega potrdila in ne izvrši akcije ali
- digitalno potrdilo uporabi in zavestno sprejme tveganje, odgovornost in posledice uporabe preklicanega digitalnega potrdila.

Infrastruktura javnih ključev na MO zagotavlja varnostne mehanizme ob predpostavki rednega preverjanja veljavnosti digitalnih potrdil. Aplikacija oziroma informacijska rešitev, ki uporablja varnostne mehanizme infrastrukture javnih ključev na MO, mora odstopanje od dolžnosti uporabe preverjenih digitalnih potrdil jasno navesti v svojih pravilih delovanja.

4.9.7. Pogostost objav registrov preklicanih potrdil

Overitelji so dolžni objaviti nov register preklicanih potrdil vsaj na petindvajset (25) ur.

Ob preklicu digitalnega potrdila morajo overitelji takoj objaviti nov register preklicanih potrdil.

4.9.8. Dovoljene zakasnitve pri objavi registrov preklicanih potrdil

Dovoljena zakasnitev od izdaje novega registra preklicanih do njegove objave je največ sto dvajset (120) minut.

Overitelji morajo izdati nov register preklicanih potrdil toliko časa pred iztekom veljavnosti starega, da je zagotovljen prenos novega registra do vseh lokacij, kjer se le ta objavlja, še pred iztekom veljavnosti starega registra.

4.9.9. Storitev sprotnega preverjanje statusa digitalnih potrdil

Storitev sprotnega preverjanja statusa digitalnih potrdil (ang. On-line Certificate Status Protocol, OCSP) ni na voljo.

4.9.10.Obveza sprotnega preverjanja statusa preklicanih potrdil

Ni relevantno.

4.9.11.Ostale oblike objavljanja preklicanih digitalnih potrdil

Ni relevantno.

4.9.12.Posebne zahteve glede zlorabe ključa

Ni predpisano.

4.9.13.Okoliščine za začasno ukinitev veljavnosti

Ni podprto.

4.9.14.Kdo lahko zahteva začasno ukinitev veljavnosti

Ni podprto.

4.9.15.Postopki za začasno ukinitev veljavnosti

Ni podprto.

4.9.16.Omejitve obdobja začasne ukinitve veljavnosti

Ni podprto.

4.10. Storitve preverjanja statusa digitalnih potrdil

4.10.1.Tehnične lastnosti storitve

Storitve preverjanja statusa digitalnih potrdil niso implementirane. Možno je samo preverjanje veljavnosti digitalnih potrdil v registrih preklicanih potrdil.

4.10.2.Razpoložljivost storitve

Ni relevantno.

4.10.3.Dodatne možnosti

Niso na voljo.

4.11. Predčasna prekinitev veljavnosti digitalnih potrdil

Predčasno se prekine veljavnost digitalnega potrdila iz naslednjih razlogov:

- prenehanje delovnega razmerja imetnika,
- prenehanje delovanja organizacijske enote MO oziroma institucije, ki je opravlja naloge povezane z obrambo države,
- ukinitev vojaške dolžnosti, organizacijske ali funkcijske vloge,
- sprememba statusa imetnika, zaposlenega v instituciji, ki je opravlja naloge povezane z obrambo države, ki ima za posledico dejstvo, da imetnik ne opravlja več nalog povezanih z obrambo države,
- sprememba statusa institucije, ki je opravlja naloge povezane z obrambo države, ki ima za posledico dejstvo, da institucija ne opravlja več nalog, povezanih z obrambo države,
- prenehanje potrebe po varnostni storitvi strežnika, druge strojne ali programske opreme in
- prenehanje potrebe po storitvi izdajanja časovnih žigov ali podobni storitvi overjanja.

Razlog za predčasno prekinitev veljavnosti digitalnega potrdila podrejenega overitelja je prenehanje potrebe po izdajanju digitalnih potrdil imetnikom.

Prekinitev veljavnosti digitalnega potrdila pred iztekom obdobja veljavnosti se izvede kot preklic potrdila v skladu s poglavjem 4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila.

4.12. Varnostno kopiranje in odkrivanje zasebnega ključa

Hranjenje kopij zasebnih ključev pri zunanjih subjektih (ang. Key Escrow) ni dovoljeno.

Dovoljeno je varnostno kopiranje (ang. Key Backup) in posledično povrnitev zgodovine ključev (ang. Key Recovery) ter odkrivanje ključev samo za zasebne ključe za dešifriranje v povezavi z digitalnimi potrdili za šifriranje po protokolu PKIX-CMP.

Varnostno kopiranje zasebnih ključev za digitalna potrdila izdana po protokolu PKCS#10 ni možno.

Varnostno kopiranje zasebnih ključev overiteljev in izdajateljev varnih časovnih žigov se zagotavlja v skladu s poglavji 6.2.4 Varnostno kopiranje zasebnih ključev.

4.12.1.Povrnitev zgodovine ključev za dešifriranje

Overitelji morajo v svojih pravilih delovanja navesti, za katera digitalna potrdila je omogočena storitev varnostnega kopiranja in povrnitve zgodovine ključev za dešifriranje.

Povrnitev zgodovine ključev za dešifriranje se izvede ob ponovni izdaji digitalnega potrdila (glej poglavje 4.7. Ponovna izdaja digitalnih potrdil).

Ob prošnji za pridobitev digitalnega potrdila po preklicu ali preteku veljavnosti digitalnih potrdil se imetniku ob izdaji novih digitalnih potrdil praviloma tudi povrne zgodovina zasebnih ključev za dešifriranje.

4.12.2.Odkrivanje kopije ključev za dešifriranje

Overitelji morajo v svojih pravilih delovanja navesti, za katera digitalna potrdila je omogočena storitev odkrivanja kopije ključev za dešifriranje.

Odkrivanje kopije ključev za dešifriranje je dovoljeno le v izjemnih primerih za dostop do podatkov, ki so šifrirani in dostopni z imetnikovim ključem za dešifriranje, ko le-ti niso dostopni:

- imetnikovemu predstojniku na podlagi zahtevka za odkrivanje kopije ključev za dešifriranje ali

- če to odredi pristojno sodišče, sodnik za prekrške ali upravni organ.

O odobritvi zahtevka za odkrivanje kopije zasebnega ključa za dešifriranje odloči Svet za upravljanje z infrastrukturo javnih ključev na MO.

Overitelj pred odkrivanjem kopije ključev za dešifriranje:

- po elektronski pošti obvesti imetnika digitalnega potrdila o datumu ter vlagatelju zahtevka za odkrivanje kopije njegovih ključev za dešifriranje in
- prekliče digitalno potrdilo za šifriranje in o preklicu obvesti imetnika v skladu s poglavjem 4.9.3 Postopki za preklic.

Če je v zahtevku zahtevano takojšnje odkritje kopije, mora overitelj v roku štiriindvajset (24) ur od prejetja zahtevka odkriti kopijo zasebnega ključa za dešifriranje in jo posredovati predstojniku ali subjektu, ki je naveden v odločbi sodišča ali upravnega organa.

4.12.3.Zaščita odkritega zasebnega ključa in postopek prenosa

Postopek prenosa odkritega zasebnega ključa je enak kot postopek prenosa dešifrirnega zasebnega ključa ob ponovnem generiranju digitalnega potrdila v skladu s protokolom PKIX-CMP.

5. FIZIČNO VAROVANJE, ORGANIZACIJSKI VARNOSTNI UKREPI IN ZAHTEVE ZA OSEBJE

5.1. Fizično varovanje

5.1.1. Lokacija in konstrukcija prostorov ter fizični dostop

Dejavnosti overiteljev SIMoD-PKI se izvajajo v varovanih prostorih in na varnih lokacijah.

Prostori izpolnjujejo pogoje za namestitev komunikacijske in informacijske opreme ter arhivskih medijev skladno s predpisi, ki urejajo področje tajnih podatkov. Komunikacijska in informacijska oprema overiteljev SIMoD-PKI mora biti nameščena v prostorih varnostnega območja I. ali II. stopnje.

5.1.2. Fizični dostop

Nadzor fizičnega dostopa izvaja pristojna služba MO.

Nadzor nad vstopom se izvaja z uporabo tehničnih sredstev, ki preprečujejo nepooblaščen vstop. Vstop je dovoljen samo operativnemu osebju overiteljev SIMoD-PKI. Druge osebe, ki izkažejo upravičeni interes, smejo vstopiti v prostore samo v spremstvu operativnega osebja overiteljev SIMoD-PKI. Vstop v prostore je video nadzorovan. O vstopih in izstopih v prostore se vodi evidenca, ki zagotavlja natančen pregled prisotnosti v prostorih.

Preden operativno osebje overitelja zapusti prostore overitelja, mora preveriti:

- da programska in strojna oprema pravilno in varno deluje (overitelj opravlja svoje storitve, gesla za upravljanje z overiteljem pa morajo biti deaktivirana),
- da so varnostne omare pravilno zaklenjene,
- da so morebitni zapisi podatkov (npr. izpisi iz tiskalnika) primerno hranjeni, odvečno gradivo pa uničeno in
- da so varnostni mehanizmi vklopljeni in delujejo.

5.1.3. Napajanje in klimatske naprave

Prostor s komunikacijsko in informacijsko opremo overiteljev je opremljen s:

- sistemom za brezprekinitveno napajanje naprav in
- klimatsko napravo za kontrolo temperature in vlage.

5.1.4. Zaščita pred poplavo

Prostori s komunikacijsko in informacijsko opremo overiteljev SIMoD-PKI so na lokaciji, kjer je verjetnost poplave zelo majhna.

5.1.5. Zaščita pred ognjem

Prostori s komunikacijsko in informacijsko opremo overiteljev SIMoD-PKI so opremljeni z detektorji temperature in dima.

5.1.6. Shranjevanje medijev

Mediji z varnostnimi kopijami in arhiv podatkov stopnje tajnosti ZAUPNO in TAJNO so hranjeni v ustreznih protivlomnih omarah.

Mediji, hranjeni na oddaljeni lokaciji, so v prostorih, ki zagotavljajo enake pogoje, kot so v prostorih overiteljev.

5.1.7. Odstranjevanje odpadkov

Dokumenti v papirni obliki se uničujejo z rezalnikom v varovanih prostorih overiteljev. Vsebina medijev, na katerih se hranijo tajni podatki, se pred odstranitvijo iz prostorov overiteljev varno izbriše ali pa se medije fizično uniči.

V primeru, da medijev ni mogoče varno izbrisati ali uničiti v prostorih overiteljev, je potrebno medij dostaviti v uničevalno mesto po postopku, predpisanem za stopnjo tajnosti podatkov, ki jih medij hrani.

5.1.8. Hranjenje na oddaljeni lokaciji

Overitelji SIMoD-PKI uporabljajo oddaljeno lokacijo za varno hranjenje varnostnih kopij in arhivskih podatkov. Podatki, mediji ali naprave so na oddaljeni lokaciji shranjene v varovanih prostorih, ki zagotavljajo enako raven varnosti, kot je v prostorih overiteljev.

Kriptografski material, s katerim je zaščiten overiteljev zasebni ključ, se hrani porazdeljen na več delov na več lokacijah.

5.2. Organizacijski varnostni ukrepi

5.2.1. Organizacija upravljanja overitelja

5.2.1.1. Operativno osebje overiteljev SIMoD-PKI

Naloge upravljanja z infrastrukturo javnih ključev na MO na nivoju posameznega overitelja so porazdeljene med operativno osebje tako, da je zagotovljena ločitev med zaključenimi vsebinskimi področji upravljanja. Operativno osebje overiteljev SIMoD-PKI je glede na vsebinska področja upravljanja razdeljeno na zaključene organizacijske skupine:

- upravljanje z digitalnimi potrdili,
- upravljanje s programsko in strojno opremo overiteljev ter
- varovanje in nadzor komunikacijskega sistema za infrastrukturo javnih ključev na MO.

Posamezni operativni osebi na nivoju posameznega overitelja je dovoljeno opravljanje nalog samo znotraj ene zaključene organizacijske skupine. Posamezna oseba lahko opravlja naloge za več SIMoD-PKI overiteljev, pri čemer mora biti pri vsakem overitelju član natanko ene organizacijske skupine.

V organizacijski skupini za upravljanje z digitalnimi potrdili so:

- prvi varnostni inženir,
- drugi varnostni inženirji in
- administratorji potrdil.

V organizacijski skupini za upravljanje s programsko in strojno opremo overiteljev so:

- prvi administrator overitelja in
- administratorji overitelja.

V organizacijski skupini za varovanje in nadzor komunikacijskega sistema so:

- prvi administrator komunikacijskega sistema in
- administratorji komunikacijskega sistema.

V organizacijski skupini za upravljane z digitalnimi potrdili so najmanj tri (3) osebe, v organizacijski skupini za upravljane s programsko in strojno opremo overiteljev sta najmanj dve osebi (2), v organizacijski skupini za zavarovanje in nadzor sta najmanj dve (2) osebi.

Podrobnejša razdelitev nalog je podana v pravilih delovanja posameznega overitelja.

5.2.1.2. Prijavna služba

Naloge prijavne službe opravlja pooblaščeno osebje organizacijske enote MO, pristojne za kadrovske zadeve. Naloge prijavne služba so:

- sprejemanje zahtevkov za izdajo digitalnega potrdila,
- preverjanje istovetnosti naročnikov oziroma imetnikov in točnosti podatkov v zahtevku za izdajo digitalnega potrdila,
- hranjenje dokazila o postopkih preverjanja istovetnosti,
- posredovanje zahtevkov operativnemu osebju, ki upravlja z digitalnimi potrdili in
- obveščanje operativnega osebja, ki upravlja z digitalnimi potrdili, o spremembah podatkov o imetnikih digitalnih potrdil (npr. prekinitev delovnega razmerja, premestitev v drugo organizacijsko enoto).

5.2.1.3. Druge funkcije

Pristojne organizacijske enote v MO skrbijo za:

- fizično varovanje in nadzor prostorov overiteljev ter
- pravne zadeve.

Pomoč uporabnikom opravlja skupina zaposlenih v organizacijski enoti MO, pristojni za informatiko in telekomunikacije, ki skrbi za pomoč uporabnikom pri delu z informacijskimi sistemi ter pooblaščene osebe za informatiko v organizacijskih enotah MO. Zaposleni iz tega odstavka niso del operativnega osebja overiteljev SIMoD-PKI.

Nastavitev uporabniškega okolja uporabnikom digitalnih potrdil je naloga skupine zaposlenih v organizacijski enoti MO, pristojni za informatiko in telekomunikacije, ki skrbi za uporabniško okolje ter pooblaščenih oseb za informatiko v organizacijskih enotah MO. Zaposleni iz tega odstavka niso del operativnega osebja overiteljev SIMoD-PKI.

5.2.2. Število oseb, potrebnih za izvedbo postopkov

Za izvedbo naslednjih operacij je zahtevana prisotnost vsaj dveh oseb iz skupine za upravljanje s programsko in strojno opremo overitelja:

- generiranje kriptografskih ključev overitelja,
- preklic overiteljevega potrdila,
- spreminjanje gesel aplikacije za delo z overiteljem,
- ponovno šifriranje overiteljeve baze podatkov,
- nastavitev števila potrebnih prisotnih varnostnih inženirjev za izvedbo kritičnih operacij pri upravljanju s potrdili,
- restavriranje prijavnih imen varnostnih inženirjev,
- spreminjanje nastavitve zgoščevalnih algoritmov,
- spreminjanje nastavitev kriptografskih algoritmov,
- aktiviranje avtomatskega zagona overiteljevih servisov in
- ukinitev obvezne prisotnosti vsaj dveh oseb za izvedbo zgoraj navedenih operacij.

Za izvedbo naslednjih operacij je zahtevana prisotnost dveh zaposlenih s funkcijo prvega ali drugega varnostnega inženirja:

- nastavitev življenjske dobe digitalnih potrdil,
- medsebojno priznavanje z drugimi overitelji,
- nastavitev ali spreminjanje administrativnih pravil,
- nastavitev ali spreminjanje uporabniških pravil,
- dodajanje, brisanje ali preslikava identifikacijskih oznak politik digitalnih potrdil,
- dodajanje, spreminjanje ali brisanje varnostnih inženirjev,
- povrnitev zgodovine ključev za dešifriranje in
- odkrivanje kopije ključev za dešifriranje.

5.2.3. Preverjanje istovetnosti operativnega osebja

Operativno osebje overiteljev izkaže svojo istovetnost:

- pri vstopu v varovane prostore s komunikacijsko in informacijsko opremo overitelja z identifikacijsko kartico in vstopno kodo,
- za delo na overiteljevemu informacijskemu sistemu s prijavnim imenom in geslom.

Vsako prijavno ime ali digitalno potrdilo za opravljanje nalog operativne osebe mora:

- pripadati eni sami fizični osebi in
- omogočati avtorizacijo za izvedbo nalog samo v obsegu predpisanih nalog.

5.3. Zahteve za osebje overiteljev

5.3.1. Kvalifikacije, izkušnje in varnostno preverjanje

Operativno osebje overiteljev:

- mora biti ustrezno usposobljeno in o tem imeti dokazila,
- mora imeti za opravljanje nalog pri overitelju imenovanje Sveta za upravljanje z infrastrukturo javnih ključev na MO,
- ne sme opravljati drugih nalog, ki bi bile v nasprotju z opravljanjem nalog v okviru infrastrukture javnih ključev na MO,
- ne sme biti na prejšnjih podobnih dolžnostih (npr. skrbnik kriptografskih naprav, varnostni inženir v informacijskem sistemu) razrešeno nalog zaradi malomarnosti ali neizpolnjevanja obveznosti in
- mora imeti dovoljenje za dostop do tajnih podatkov najmanj TAJNO.

5.3.2. Dovoljenja za dostop do tajnih podatkov

V skladu z [10] ZTP.

5.3.3. Usposabljanje osebja

5.3.3.1. Usposabljanje osebja overiteljev

Operativno osebje overiteljev SIMoD-PKI se redno usposablja na naslednjih področjih:

- varnostni principi in mehanizmi infrastrukture javnih ključev,
- delo s strojno in programsko opremo overitelja,
- opravljanje nalog, za katere so zadolženi in
- ukrepanje ob izrednih dogodkih in zagotavljanje neprekinjenega delovanja.

Osebje prijavne službe mora biti usposobljeno za:

- identifikacijo naročnikov in preverjanje pravilnosti podatkov v zahtevkih ter
- delo s programsko opremo prijavne službe.

5.3.3.2. Usposabljanje osebja za pomoč uporabnikom

Osebje za pomoč uporabnikom in nastavitev uporabniškega okolja mora biti usposobljeno na področjih:

- osnove infrastrukture javnih ključev,
- administracija potrdil in
- delo z uporabniško strojno in programsko opremo.

5.3.4. Pogostost dodatnih usposabljanj

Osebje mora pridobiti potrebna znanja pred vsako nadgradnjo.

5.3.5. Kroženje med delovnimi mesti

Ni predpisano.

5.3.6. Ukrepi ob kršitvah pooblastil

Proti operativni osebi overiteljev, ki neopravičeno ne izvaja svojih nalog ali zlorabi svoja pooblastila, se ukrepa v skladu s predpisi. V primeru nepravilnosti ali suma nepravilnosti Svet za upravljanje z infrastrukturo javnih ključev na MO zahteva odvzem pooblastila osebi ter preklic prijavnega imena in digitalnega potrdila, izdanega osebi za opravljanje zaupanih nalog.

5.3.7. Zunanji izvajalci

Zunanji izvajalci morajo za izvajanje posegov izpolnjevati vse pogoje, določene v [10] ZTP oziroma implementacijo pravil na lokacijah overiteljev.

5.3.8. Dokumentacija za osebje overiteljev

Operativnemu osebju overiteljev, skupini za pomoč uporabnikom in skupini za nastavitev uporabniškega okolja so na voljo interni priročniki, originalna dokumentacija programske in strojne opreme ter priročniki šolanj, glede na njihovo funkcijo in načrt izobraževanja.

5.4. Postopki varnostnih pregledov sistema

5.4.1. Vrste beleženih dogodkov

Overitelji so dolžni beležiti dogodke:

- na operacijskem sistemu, programski in strojni opremi overitelja,
- na operacijskih sistemih, programski in strojni opremi elementov komunikacijskega sistema,
- v zvezi s ključi overitelja,
- v zvezi z imetniškimi ključi in digitalnimi potrdili - izdaja, prevzem, obnova, preklic, povrnitev zgodovine ključev za dešifriranje in odkrivanje kopije ključev za dešifriranje,
- v zvezi z varnostno politiko in upravljanjem informacijskega sistema overitelja in
- v zvezi z varnostno politiko in upravljanjem komunikacijskega sistema.

Zapis dogodka, pa naj bo to v elektronski ali pisni obliki, vsebuje datum in čas dogodka, osebo, ki je dogodek povzročila ter če je možno in smiselno tudi IP naslov, od katerega dogodek izvira.

Overitelji so dolžni zbirati in beležiti v elektronski ali pisni obliki tudi podatke, ki vplivajo na varnost, niso pa del komunikacijsko informacijskega sistema overitelja:

- dogodke v zvezi s fizičnim dostopom do sistemov overitelja ter fizično lokacijo,
- kadrovske spremembe operativnega osebja overiteljev SIMoD-PKI in
- dogodke povezane z uničevanjem občutljivega materiala, na primer kriptografskega materiala oziroma ključev in nosilcev ključev.

Originali dnevnikov beleženih dogodkov v pisni obliki in kopija dnevnikov beleženih v elektronski obliki se hranijo v varovanih prostorih overitelja.

5.4.2. Pogostost pregleda dnevnikov beleženih dogodkov

Operativno osebje overiteljev pregleduje dnevnike beleženih dogodkov ob vsakem prejetem opozorilu iz nadzornih sistemov. Pregled vključuje:

- preverjanje integritete dnevnikov,

- pregled zapisov v dnevniku in
- analizo in poročanje o relevantnih dogodkih - razreševanje problemov.

Operativno osebje overiteljev SIMoD-PKI izvaja redne preglede beleženih dogodkov in sicer najmanj enkrat letno. Redni pregled vključuje:

- zbiranje in združevanje dnevnikov od zadnjega rednega pregleda,
- preverjanje integritete dnevnikov,
- pregled zapisov v dnevniku in izdelava poročila o relevantnih dogodkih in
- izdelava arhivskih kopij dnevnikov.

5.4.3. Obdobje hranjenja dnevnikov beleženih dogodkov

Najmanj do naslednjega rednega pregleda na sistemih in najmanj pet (5) let v arhivu.

5.4.4. Zaščita dnevnikov beleženih dogodkov

Dnevniki se hranijo v ustreznem varnostnem območju. Lokacija varnostne kopije je vsaj 25 km oddaljena od prostora overitelja.

Dostop do dnevnikov beleženih dogodkov je dovoljen samo pooblaščenim osebam:

- Svetu za upravljanje z infrastrukturo javnih ključev na MO,
- operativnemu osebju overitelja SIMoD-PKI v okviru svojih delovnih nalog in
- inšpektorju.

Za dnevnike beleženih dogodkov v elektronski obliki morajo biti implementirani mehanizmi za zagotavljanje celovitosti. Za dnevnike beleženih dogodkov na operacijskem sistemu so uporabljene zaščite, kot jih le-ta dopušča.

5.4.5. Varnostne kopije dnevnikov beleženih dogodkov

Varnostne kopije dnevnikov beleženih dogodkov, ki se zbirajo v elektronski obliki, se izdeluje dnevno v okviru rednega varnostnega kopiranja sistemov. Enkrat mesečno se en izvod varnostne kopije dnevnikov v elektronski obliki prenese na oddaljeno lokacijo.

5.4.6. Način zbiranja beleženih dogodkov

Zapisi o dogodkih se zbirajo avtomatsko, kjer to ni mogoče, pa ročno.

5.4.7. Obveščanje povzročitelja dogodka

Povzročitelja dogodka o dogodku ni treba obvestiti.

5.4.8. Ocena in odprava ranljivosti

Dnevnike beleženih dogodkov pregleduje operativno osebje overitelja SIMoD-PKI z namenom odkrivanja in odprave ranljivosti. Ugotovljeno ranljivost se oceni s stališča verjetnosti povzročitve škode in predvidi ukrepe za zmanjšanje grožnje.

5.5. Arhiviranje podatkov

5.5.1. Vrste arhiviranih podatkov

Overitelji morajo hraniti naslednje podatke:

- dnevnike beleženih dogodkov iz poglavja 5.4.1 Vrste beleženih dogodkov,
- zahtevke imetnikov digitalnih potrdil,
- dokumentacijo o izvedbi preverjanja istovetnosti uporabnikov,

- korespondenco in pogodbe imetnikov digitalnih potrdil z overitelji SIMoD-PKI,
- digitalna potrdila in liste preklicanih potrdil,
- verzije Politik SIMoD-PKI in svojih pravil delovanja ter
- zasebne dešifrirne ključe v skladu s poglavjem 6.2.4 Varnostno kopiranje zasebnih ključev.

5.5.2. Obdobje hranjenja arhiva

Overitelji SIMoD-PKI hranijo dnevnike beleženih dogodkov najmanj pet (5) let od posameznega dogodka ali dejanja.

Overitelji SIMoD-PKI hranijo zahtevke imetnikov, korespondenco in pogodbe imetnikov z overiteljem najmanj pet (5) let od zaključka zadeve, ki je vezana na zahtevek, korespondenco ali pogodbo oziroma od zadnjega dne veljavnosti digitalnega potrdila, ki je povezano s hranjenim zahtevkom, korespondenco ali pogodbo.

Digitalna potrdila in zasebni ključi se hranijo vsaj pet (5) let po preteku veljavnosti zadnjega digitalnega potrdila imetnika.

5.5.3. Zaščita arhiva

Podatki, ki sodijo v dokumentarno gradivo (zahtevki imetnikov, dokumentacija o izvedbi identifikacije, korespondenca in pogodbe imetnikov digitalnih potrdil z overitelji SIMoD-PKI, verzije Politik SIMoD-PKI, verzije pravil delovanja overiteljev in dnevniki beleženih dogodkov v pisni obliki), se hranijo in arhivirajo v skladu s postopki dela z dokumentarnim gradivom v MO.

Arhivirani podatki, ki se beležijo v okviru informacijskega sistema (avtomatsko generirani dnevniki beleženih dogodkov, digitalna potrdila in liste preklicanih potrdil ter zasebni dešifrirni ključi), se nahajajo na vsaj dveh kopijah na ločenih lokacijah. Arhiv, ki se hrani na drugi lokaciji, je zaščiten z ekvivalentnimi varnostnimi mehanizmi, kot so implementirani v prostorih overitelja.

5.5.4. Varnostna kopija arhiva

Podatkom, ki sodijo v dokumentarno gradivo (zahtevki imetnikov, dokumentacija o izvedbi identifikacije, korespondenca in pogodbe imetnikov digitalnih potrdil z overitelji SIMoD-PKI, verzije Politik SIMoD-PKI, verzije pravil delovanja overiteljev in dnevniki beleženih dogodkov v pisni obliki), se zagotavlja razpoložljivost arhiva v skladu s postopki dela z dokumentarnim gradivom v MO.

Ob izdelavi arhiva podatkov, ki se beležijo v okviru informacijskega sistema (avtomatsko generirani dnevniki beleženih dogodkov, digitalna potrdila in liste preklicanih potrdil ter zasebni dešifrirni ključi), se izdela varnostna kopija.

5.5.5. Časovno žigosanje zapisov

Ni predpisano.

5.5.6. Način arhiviranja

Ni predpisano.

5.5.7. Postopek vpogleda v in verifikacije arhiva

Ob kreiranju arhiva se preveri integriteta medija. Enkrat letno se preverja integriteta medijev z arhiviranimi podatki in možnost branja podatkov iz arhiva. Dostop do arhiva je dovoljen samo:

- Svetu za upravljanje z infrastrukturo javnih ključev na MO,
- operativnemu osebju overitelja SIMoD-PKI v okviru njegovih delovnih nalog in
- inšpektorju.

5.6. Zamenjava ključev overiteljev

5.6.1. Obnova potrdila korenskega overitelja

Veljavnost samopodpisanega potrdila korenskega overitelja je vedno daljša, kot je veljavnost kateregakoli digitalnega potrdila podrejenega overitelja, podpisanega s pripadajočim zasebnim ključem.

Za podpisovanje digitalnih potrdil podrejenih overiteljev se vedno uporablja najnovejši zasebni ključ korenskega overitelja. Za preverjanje veljavnosti digitalnih potrdil podrejenih overiteljev pa se uporablja predhodno potrdilo korenskega overitelja vse dokler ne poteče veljavnost zadnjega digitalnega potrdila, podpisanega s starim zasebnim ključem korenskega overitelja. Zasebni ključ se vedno uporablja krajše obdobje kot je veljavnost pripadajočega digitalnega potrdila.

Za podpisovanje registra preklicanih overiteljev se stari zasebni ključ korenskega overitelja še vedno lahko uporablja do konca veljavnosti pripadajočega digitalnega potrdila.

Obnova digitalnega potrdila korenskega overitelja se izvede po predpisanem in nadzorovanem postopku. Posamezne korake postopka izvaja operativno osebje korenskega overitelja. Prisotne so tudi priče, ki nadzorujejo izvajanje postopka. Izvedba postopka je dokumentirana v zapisniku, ki ga podpišejo vsi prisotni.

5.6.2. Obnova potrdil podrejenih overiteljev

Veljavnost overiteljevega potrdila je vedno daljša, kot je veljavnost kateregakoli digitalnega potrdila imetnika, podpisanega s pripadajočim zasebnim ključem.

Za podpisovanje digitalnih potrdil se vedno uporablja najnovejši overiteljev zasebni ključ. Za preverjanje veljavnosti digitalnih potrdil pa se uporablja predhodno overiteljevo potrdilo vse dokler ne poteče veljavnost zadnjega digitalnega potrdila, podpisanega s starim zasebnim overiteljevim ključem. Zasebni ključ overitelja se vedno uporablja krajše obdobje kot je veljavnost pripadajočega overiteljevega potrdila.

Za podpisovanje registra preklicanih potrdil se stari zasebni ključ podrejenega overitelja še vedno lahko uporablja do konca veljavnosti pripadajočega digitalnega potrdila.

Obnova digitalnih potrdil podrejenih overiteljev se izvede po predpisanem in nadzorovanem postopku. Posamezne korake postopka izvaja operativno osebje korenskega overitelja in podrejenega overitelja. Prisotne so tudi zaupanja vredne priče, ki nadzorujejo izvajanje postopka. Izvedba postopka je dokumentirana v zapisniku, ki ga podpišejo vsi prisotni.

5.7. Okrevalni načrt

5.7.1. Postopki v primeru okvar in zlorab

Načrt ponovne vzpostavitve delovanja je predpisan v zaupnem delu pravil posameznega overitelja.

5.7.2. Uničenje programske, strojne opreme ali podatkov overitelja

V primeru okvare strojne ali programske opreme oziroma podatkov, pri kateri zasebni ključ overitelja ni bil uničen, bodo storitve overitelja ponovno vzpostavljene v najkrajšem možnem času. Overitelj mora najkrajšem možnem času vzpostaviti vsaj funkcionalnost preklica digitalnih potrdil in objavljanja registra preklicanih potrdil. Skrajni rok za vzpostavitev storitve preklica digitalnih potrdil in objavljanja registra preklicanih potrdil je sedem (7) dni. Po tem roku mora overitelj objaviti preklic svojega potrdila in ukrepati v skladu s poglavjem 4.9.3.2

Postopki preklica digitalnega potrdila korenskega overitelja oziroma 4.9.3.4 Postopki preklica digitalnega potrdila podrejenega overitelja.

V primeru okvare, kjer pride do uničenja overiteljevega zasebnega ključa in vseh njegovih kopij, se postopa, kot da je prišlo do zlorabe ključa v skladu s poglavjem 4.9.3.2 Postopki preklica digitalnega potrdila korenskega overitelja oziroma 4.9.3.4 Postopki preklica digitalnega potrdila podrejenega overitelja.

V posebnih primerih lahko aplikacije še naprej določen čas uporabljajo digitalna potrdila, podpisana z uničenim zasebnim overiteljevim ključem. Ta možnost mora biti predvidena v pravilih uporabe konkretne aplikacije.

5.7.3. Zloraba zasebnega ključa overitelja

Postopki ob zlorabi zasebnega ključa overitelja so predpisani v poglavju 4.9.3.2 Postopki preklica digitalnega potrdila korenskega overitelja oziroma 4.9.3.4 Postopki preklica digitalnega potrdila podrejenega overitelja.

5.7.4. Zagotavljanje kontinuitete delovanja po nesrečah

Postopki v primeru naravnih in drugih nesreč, ki imajo za posledico fizično uničenje ali varnostno vprašljivo delovanje programske opreme, strojne opreme ali ogroženo celovitost podatkov overitelja oziroma uničenje in poškodovanje varovanih prostorov overitelja, so predpisani v zaupnem delu pravil delovanja posameznega overitelja.

5.8. Prenehanje delovanja overitelja

Vzroki za prenehanje delovanja overitelja so podani v poglavju 4.9.1.2 Okoliščine preklica digitalnega potrdila korenskega overitelja oziroma 4.9.1.4 Okoliščine preklica digitalnega potrdila podrejenega overitelj. Odločitev o prenehanju delovanja izda Svet za upravljanje z infrastrukturo javnih ključev na MO.

V skladu z veljavnimi predpisi v Republiki Sloveniji lahko odločitev za prenehanje delovanja overitelja izda tudi pristojna inšpekcijska služba oziroma pristojno sodišče.

Takoj po sprejetju odločitve o prenehanju delovanja, nikoli pa kasneje kot tri (3) dni pred predvidenim prenehanjem delovanja bo overitelj obvestil:

- celotno operativno osebje,
- vse imetnike digitalnih potrdil oziroma odgovorne osebe,
- morebitne medsebojno priznane ali podrejene overitelje in
- ministrstvo, pristojno za registracijo overiteljev v Republiki Sloveniji.

Overitelj bo po prenehanju delovanja izvedel postopke predpisane v poglavju 4.9.3.2 Postopki preklica digitalnega potrdila korenskega overitelja oziroma 4.9.3.4 Postopki preklica digitalnega potrdila podrejenega overitelj.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev para ključev

6.1.1. Generiranje para ključev

Postopek generiranja ključev overitelja izvede operativno osebje overitelja, prisotne so zaupanja vredne priče. Izvedba postopka je dokumentirana v zapisniku. Generiranje para ključev je vedno izvedeno znotraj varnostnega kriptografskega modula.

Imetniški par ključev za podpisovanje oziroma par ključev za oba namena uporabe (podpisovanje in šifriranje) se razen v primerih iz naslednjega odstavka generira pri bodočem imetniku in pod njegovo izključno kontrolo. Če ima bodoči imetnik sredstvo za varno elektronsko podpisovanje, to je varnostni kriptografski modul ali pametno kartico, je generiranje para ključev izvedeno znotraj tega sredstva.

Za digitalna potrdila z obvezno uporabo pametne kartice, kjer overitelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, se zasebni ključ za podpisovanje oziroma za oba namena uporabe (podpisovanje in šifriranje) generira na pametni kartici pri overitelju.

Imetniški par ključev za šifriranje, za katerega overitelj zagotavlja storitev povrnitve zgodovine ključev, se generira pri overitelju in varno prenese bodočemu imetniku.

6.1.2. Dostava zasebnega ključa imetniku

Za digitalna potrdila, za katere se par ključev za šifriranje generira pri overitelju, se zasebni ključ do imetnika prenese po protokolu PKIX-CMP kot integralni del postopka za generiranje ključev in prevzem digitalnega potrdila.

Par ključev za podpisovanje se vedno ustvari na strani bodočega imetnika oziroma v primeru uporabe pametnih kartic znotraj le te. Zasebni ključ za podpisovanje se nikdar ne generira, ne prenaša in ne hrani na strojni ali programski opremi overitelja.

V primeru digitalnih potrdil z obvezno uporabo pametne kartice, kjer overitelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, se zasebni ključ za podpisovanje oziroma za oba namena uporabe (podpisovanje in šifriranje) generira na pametni kartici pri overitelju. Pametna kartica se nato varno posreduje imetniku.

6.1.3. Dostava imetnikovega javnega ključa overitelju

Javni ključ para ključev, ki se generira na strani imetnika, se dostavi overitelju po protokolih PKIX-CMP ali PKCS#10.

6.1.4. Dostava overiteljevega javnega ključa uporabnikom

Javni ključ overitelja oziroma overiteljevo potrdilo, ki vsebuje overiteljev javni ključ, se pošlje bodočemu imetniku digitalnega potrdila kot integralni del postopka za prevzem potrdila.

Tretje osebe lahko overiteljevo potrdilo kadarkoli pridobijo tudi iz imenika ali na spletnih straneh overitelja (poglavje 2.2. Objave informacij o digitalnih potrdilih) vendar je njihova obveznost, da preverijo istovetnost overitelja in celovitost overiteljevega potrdila.

6.1.5. Dolžina ključev

Dolžine zasebnih ključev so določene v pravilih delovanja posameznega overitelja.

6.1.6. Parametri za generiranje javnih ključev in preverjanje parametrov

Vsi postopki v zvezi z RSA ključi so po protokolu PKCS#1.

6.1.7. Namen uporabe ključev

Namen uporabe ključev je določen v razširitvenem polju *keyUsage* in *extKeyUsage*. Uporaba polja *keyUsage* in *extKeyUsage* je predpisana v priporočilu X.509v3 oziroma RFC 3280.

Dovoljene vrednosti razširitvenega polja *keyUsage* glede na vrsto digitalnega potrdila so:

Vrsta digitalnega potrdila	Vrednost polja *keyUsage*
overiteljevo potrdilo	*keyCertSign, cRLSign*
digitalno potrdilo za preverjanje digitalnega podpisa	*digitalSignature*
digitalno potrdilo za šifriranje	*keyEncipherment*
digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje	*digitalSignature, keyEncipherment*
digitalno potrdilo za izdajatelje varnih časovnih žigov	*digitalSignature*

Za podpisovanje digitalnih potrdil in registrov preklicanih potrdil se uporabljajo samo zasebni ključi overiteljev.

Izdajatelji varnih časovnih žigov para ključev v povezavi s šifrirnim potrdilom ne uporabljajo, par ključev v povezavi s potrdilom za preverjanje podpisa pa uporabljajo za digitalno podpisovanje. Razširjena uporaba ključa za preverjanje podpisa je časovno žigosanje, zato ima potrdilo dodatno standardno razširitveno polje *extKeyUsage* z vrednostjo *id-kp-timeStamping*.

Uporaba razširitvenega polja *NonRepudiation* ni predpisana s Politiko SIMoD-PKI. Vrednost razširitvenega polja *NonRepudiation* predpišejo overitelji v svojih pravilih delovanja.

Overitelji SIMoD-PKI predpišejo vrednosti razširitvenih polj *keyUsage* in *extKeyUsage* za digitalna potrdila za strežnike, drugo strojno in programsko opremo ter ponudnike storitev overjanja.

6.2. Zaščita zasebnih ključev in zahteve za kriptografske module

6.2.1. Standardi za kriptografske module

Overitelji digitalnih potrdil in izdajatelji varnih časovnih žigov morajo uporabljati strojne varnostne kriptografske module, ki ustrezajo enemu od standardov:

- FIPS 140-2 Level 3 ali višji,
- CEN CWA 14167-2, 14167-3 ali 14167-4,
- CEN CWA 14169 ali ISO/IEC 15408 level EAL4+ ali višji.

Operativno osebje overiteljev in prijavne službe ter imetniki digitalnih potrdil VISOKE stopnje zaupanja morajo uporabljati pametne kartice ali podobne nosilce ključev stopnje varnosti FIPS 140-2 level 2 ali CEN CWA 14169. Pametna kartica se mora uporabljati na način, da zasebni ključ pametne kartice nikoli ne zapusti.

Imetniki digitalnih potrdil SREDNJE stopnje zaupanja uporabljajo programske kriptografske module vsaj stopnje varnosti FIPS 140-2 level 1 ali pametne kartice vsaj stopnje varnosti FIPS 140-2 level 1.

6.2.2. Nadzor zasebnega ključa z več pooblaščenimi osebami

Za upravljanje z zasebnim ključem overitelja oziroma z varnostnim kriptografskim modulom je potrebna prisotnost vsaj dveh oseb z ustreznimi pooblastili, ki izkažeta svojo istovetnost s pametno kartico s porazdeljenim ključem kriptografskega modula in geslom kartice.

6.2.3. Odkrivanje zasebnega ključa

Odkrivanje zasebnega ključa overiteljev ni dovoljeno. Tehnična izvedba varnostnega kriptografskega modula ne omogoča prikaza zasebnega ključa overitelja v nešifrirani obliki.

Povrnitev zgodovine in odkrivanje kopije imetniških zasebnih ključev za dešifriranje je možno ob pogojih iz poglavja 4.12.1 Povrnitev zgodovine ključev za dešifriranje oziroma 4.12.2 Odkrivanje kopije ključev za dešifriranje.

6.2.4. Varnostno kopiranje zasebnih ključev

Varnostna kopija zasebnega ključa overitelja se zagotavlja z mehanizmi varnostnega kriptografskega modula. Varnostna kopija se pred izvozom iz varnostnega kriptografskega modula šifrira. Dešifrirni ključ je porazdeljen na N[7] od M[8] administratorskih pametnih karticah.

Kopije zasebnih ključev za dešifriranje digitalnih potrdil, za katera overitelj zagotavlja storitev povrnitve zgodovine ključev, se morajo hraniti pri overitelju v šifrirani obliki.

6.2.5. Arhiviranje zasebnega ključa

Overiteljev zasebni ključ se ne arhivira.

Arhivira se samo zasebne dešifrirne ključe imetniških digitalnih potrdil, za katera overitelj zagotavlja povrnitev zgodovine in odkrivanje kopije ključev za dešifriranje.

6.2.6. Zapis zasebnega ključa v kriptografski modul in iz njega

Zasebni ključ overitelja digitalnih potrdil ali izdajatelja varnih časovnih žigov se generira v varnostnem kriptografskem modulu.

Zasebni ključi za podpisovanje se v primeru digitalnih potrdil VISOKE stopnje varnosti generirajo na pametni kartici.

Zasebni ključi se v primeru digitalnih potrdil SREDNJE in NIZKE stopnje varnosti generirajo v programskem modulu ali na pametni kartici pri bodočem imetniku.

Zasebni ključi za dešifriranje se v primeru digitalnih potrdil, za katera overitelj zagotavlja storitev povrnitve zgodovine in odkrivanja kopije ključev, generirajo v overiteljevem kriptografskem modulu in se prenesejo k bodočemu imetniku z uporabo protokola PKIX-CMP.

Izvoz zasebnega ključa iz varnega kriptografskega modula ali pametne kartice mora biti onemogočen.

6.2.7. Hranjenje zasebnega ključev v kriptografskem modulu

Zasebni ključi overitelja digitalnih potrdil oziroma izdajatelja varnih časovnih žigov so shranjeni v varnostnem kriptografskem modulu v šifrirani obliki in se nikdar ne pojavijo izven modula v nešifrirani obliki.

[7] N mora biti večji ali enak 2
[8] M mora biti večji ali enak 3

6.2.8. Postopek za aktiviranje zasebnega ključa

Zasebni ključ overitelja digitalnih potrdil oziroma izdajatelja varnih časovnih žigov se aktivira ob zagonu aplikativne programske opreme. Za aktiviranje je potrebno predložiti operatersko pametno kartico varnostnega kriptografskega modula ter geslo administratorja overitelja.

Uporabniška programska oprema imetnikov digitalnih potrdil mora preveriti istovetnost uporabnika z geslom in šele po uspešnem preverjanju istovetnosti aktivirati zasebni ključ.

6.2.9. Postopek za deaktiviranje zasebnega ključa

Zasebni ključ overitelja digitalnih potrdil oziroma izdajatelja varnih časovnih žigov se deaktivira z zaustavitvijo aplikativne programske opreme.

Imetniki digitalnih potrdil morajo uporabljati uporabniško programsko opremo, ki deaktivira zasebni ključ, ko se imetniki odjavijo oziroma ko poteče določen čas neaktivnosti.

Ob zaustavitvi aplikativne programske opreme overitelja digitalnih potrdil oziroma izdajatelja varnih časovnih žigov se uničijo vsi ključi, ki se nahajajo v delovnem pomnilniku varnostnega kriptografskega modula. Zasebni ključi se nikoli ne nahajajo v sistemskem pomnilniku, temveč samo v strojni opremi varnostnega kriptografskega modula.

Zasebni ključi pri digitalnih potrdilih VISOKE stopnje zaupanja se nikoli ne nahajajo v sistemskem pomnilniku, vedno samo v strojni opremi pametne kartice.

Imetniki digitalnih potrdil SREDNJE in NIZKE stopnje zaupanja morajo uporabljati uporabniško programsko opremo, ki z operacijo brisanja uniči ključe, ki se nahajajo v nešifrirani obliki v sistemskem pomnilniku in na disku.

6.2.10.Postopek za uničenje zasebnega ključa

Zasebne ključe overiteljev digitalnih potrdil oziroma izdajateljev varnih časovnih žigov je obvezno uničiti, ko jim poteče obdobje uporabe, oziroma se ne uporabljajo več iz drugih razlogov. Ob uničenju ključev je potrebno uničiti aktivno kopijo na varnostnem kriptografskem modulu in vse varnostne kopije

6.2.11.Stopnja varnosti kriptografskih modulov

Opisano v poglavju 6.2.1 Standardi za kriptografske modul.

6.3. Ostali vidiki upravljanja s pari ključev

6.3.1. Arhiviranje javnega ključa

Overitelj arhivira svoj javni ključ za preverjanje podpisa in imetniške javne ključe v povezavi z digitalnimi potrdili za preverjanje podpisa kot del arhiviranja digitalnih potrdil (glej poglavje 5.5. Arhiviranje podatkov). Javni ključi v povezavi s šifrirnimi digitalnimi potrdili se ne arhivirajo.

6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil

Veljavnost digitalnih potrdil oziroma javnih in zasebnih ključev je določena v pravilih delovanja posameznega overitelja

6.4. Gesla za dostop do zasebnih ključev

6.4.1. Določanje gesel za dostop do zasebnih ključev v kriptografskih modulih

Gesla za varnostni kriptografski modul se določijo v postopku inicializacije varnostnega kriptografskega modula.

Razen v primerih iz naslednjega odstavka določijo geslo za pametne kartice imetniki v postopku inicializacije pametne kartice pred prvim prevzemom digitalnega potrdila.

Za digitalna potrdila z obvezno uporabo pametne kartice, kjer overitelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, se geslo generira ob prevzemu digitalnega potrdila. To geslo mora imetnik spremeniti pred prvo uporabo digitalnega potrdila.

Za dostop do zasebnih ključev, ki se hranijo v programski obliki (npr. Microsoft Cryptographic Store) morajo uporabniki uporabljati visoko stopnjo zaščite, ki jo nudi programska oprema. Geslo za dostop do zasebnih ključev, ki se hranijo v programski obliki, določijo imetniki ob prevzemu digitalnega potrdila.

6.4.2. Zaščita gesel

Gesla se morajo hraniti na način, ki zagotavlja njihovo zaupnost. Če je bilo geslo za dostop do pametne kartice že določeno pri overitelju, ga overitelj dostavi imetniku na varen način.

6.4.3. Druge zahteve za gesla

Geslo za dostop do pametne kartice oziroma za aktivacijo pametne kartice mora biti dolgo najmanj 9 znakov in mora vsebovati velike in male črke, številke ter posebne znake in ne sme biti beseda iz slovarja.

6.5. Varnostne zahteve za računalnike

6.5.1. Specifične tehnične varnostne zahteve za računalnike

Overitelj ima v sistemski in aplikativni programski opremi implementirane tehnične varnostne kontrole, ki vključujejo:

- kontrolo dostopa do overiteljevih storitev,
- delitev nalog med operativnim osebjem overitelja,
- preverjanje istovetnosti operativnega osebja overitelja,
- šifrirane komunikacijske poti oziroma seje ali fizični nadzor komunikacijske poti,
- šifriranje zaupnih podatkov v bazi overitelja,
- varen arhiv overitelja in kopij ključev imetnikov ter varnostnih beležk,
- varnostne beležke vseh varnostno relevantnih dogodkov in
- mehanizme restavriranja sistema, ključev overitelja ter baze podatkov overitelja.

6.5.2. Raven varnostne zaščite računalnikov

Ni predpisano.

6.6. Tehnični nadzor življenjskega cikla overitelja

6.6.1. Nadzor razvoja sistema

Strojna oprema, operacijski sistem in programska oprema overiteljev so komercialni proizvodi.

6.6.2. Upravljanje varnosti

Overitelj mora evidentirati postopke inštalacije, sprememb konfiguracije in nadgradnje za vse svoje informacijske in komunikacijske komponente.

Operativno osebje overiteljev periodično in ob vsaki namestitvi nove verzije ali popravka preverja celovitost operacijskega sistema in aplikativne programske opreme overiteljev.

Zunanji izvajalec, ki je dobavil informacijsko in komunikacijsko opremo in izvedel začetno inštalacijo, jamči:

- da oprema res izvira od proizvajalca,
- v obdobju med proizvodnjo in inštalacijo ni prišlo do spreminjanja in posegov v opremo,
- je inštaliral opremo prave verzije in s predvidenim namenom uporabe.

Programska oprema overitelja je zaščitena na način, da se da preveriti njen izvor in celovitost.

6.6.3. Upravljanje varnosti čez življenjski cikel

Nadgradnje, nove verzije in popravki delov informacijskih in komunikacijskih sistemov overiteljev, oziroma upravljanje varnosti skozi celoten življenjski cikel, morajo biti v skladu z 6.6.2 Upravljanje varnosti.

6.7. Varnostne kontrole na ravni računalniškega omrežja

Korenski overitelj ni povezan v nobeno računalniško omrežje.

Komunikacijsko informacijski sistemi posameznega overitelja delujejo v izoliranih omrežjih, ki so z drugimi omrežji KIS MO in SV povezani preko varnostnih pregrad. Varnostna pravila na varnostnih pregradah dovoljujejo prehod samo protokolom, potrebnim za dostop do storitev overiteljev.

6.8. Časovno žigosanje

Ni predpisano.

7. PROFIL DIGITALNIH POTRDIL IN REGISTROV PREKLICANIH POTRDIL

7.1. Profil digitalnih potrdil

7.1.1. Verzija digitalnih potrdil

Overitelji v okviru infrastrukture javnih ključev na MO izdajajo digitalna potrdila X.509 verzije 3 v skladu s priporočilom [7] RFC 3280, ki vsebujejo naslednja osnovna polja:

Naziv osnovnega polja	Slovenski naziv in opis	Vrednost
version	verzija potrdila X.509	*v3*
serialNumber	enolična serijska številka	enolična serijska številka
signature	algoritem za podpis potrdila	*sha1WithRSAEncryption*
issuer	izdajatelj	razločevalno ime overitelja
validity	veljavnost potrdila	*Not Before*: začetek veljavnosti *Not After*: konec veljavnosti
subject	imetnik	razločevalno ime imetnika
subjectPublicKeyInfo	podatki o imetnikovem javnem ključu	*rsaEncryption*, modul, eksponent, vrednost javnega ključa

7.1.2. Razširitvena polja

Standardna razširitvena polja po priporočilu [7] RFC 3280, uporabljena v digitalnih potrdilih overiteljev SIMoD-PKI:

Naziv standardnega razširitvenega polja		Slovenski naziv in opis	Vrednost
AuthorityKeyIdentifier		identifikator javnega ključa overitelja	*KeyID* = SHA-1 odtis javnega ključa overitelja
SubjectKeyIdentifier		identifikator imetnikovega javnega ključa	SHA-1 odtis javnega ključa imetnika
KeyUsage		namen uporabe ključa	določeno v 6.1.7 Namen uporabe ključev
extendedKeyUsage		razširjen namen uporabe ključa	določeno v 6.1.7 Namen uporabe ključev
PrivateKeyUsagePeriod		veljavnost zasebnega ključa	*Not Before*: začetek veljavnosti *Not After*: konec veljavnosti
certificatePolicies:		oznaka politike potrdila	
	policyIdentifier	enolična oznaka politike	Skladno s 1.2. Identifikacijske oznake politik delovanja in 7.1.6 Identifikacijske oznake politik
	policyQualifier	identifikator politike	*[1,1]Policy Qualifier Info:* *Policy Qualifier Id=CPS* *Qualifier:* *http:/www.simod-pki.mors.si/*
CRLDistributionPoints		objave registra preklicanih potrdil	določeno v pravilih delovanja overitelja
SubjectAltName		alternativno ime imetnika	določeno v pravilih delovanja overitelja

basicConstraints	osnovne omejitve	določeno v pravilih delovanja overitelja

Kvailficirana potrdila, skladna z [3] ETSI TS 101 456, morajo vsebovati izjavo, da ustrezajo profilu kvalificiranih potrdil po priporočilu [4] ETSI TS 101 862. V ta namen vsebujejo dodatno razširitveno polje:

qcStatement 1.3.6.1.5.5.7.1.3	izjava, da je potrdilo kvalificirano	*QcComplianceStatment,* ob obvezni uporabi sredstva za varno podpisovanje še: *QcSSCD Statement*

Polja *certificatePolicies*, *keyUsage* in *extKeyUsage* so označena kot kritična.

Uporaba razširitvenih polj, ki se uporabljajo v potrdilih o priznavanju drugega overitelja (*policyMappings, nameConstraints, basicConstraint* in *policyConstraints*), se določi ob medsebojnem priznavanju.

Overitelji lahko uporabljajo dodatna standardna in lastna razširitvena polja.

7.1.3. Identifikacijske oznake algoritmov

Identifikacijski oznaki kriptografskih algoritmov, uporabljena v digitalnih potrdilih, sta:

Algoritem	Identifikacijska oznaka
rsaEncryption	1.2.840.113549.1.1.1
sha1WithRSAEncryption	1.2.840.113549.1.1.5

7.1.4. Oblike imen

Kot v poglavju 3.1.1 Vrste imen.

7.1.5. Omejitve imen

Omejitve za razločevalna imena so opisana v poglavju 3.1.2 Potreba po smiselnosti imen.

Upravitelj imenika lahko določi dodatne omejitve glede imen.

Uporaba polja *nameConstraints* se določi ob medsebojnem priznavanju.

7.1.6. Identifikacijske oznake politik

Digitalno potrdilo vsebuje v polju *certificatePolicies* identifikacijsko oznako politike, ki je določena v pravilih delovanja overitelja.

Kvalificirana potrdila imajo skladno s priporočilom [3] ETSI TS 101 456 v polju *certificatePolicies*, *policyIdentifier* poleg oznake politike, določene s pravili delovanja overitelja, še vrednost *0.4.0.1456.1.2;* kvalificirana potrdila z obvezno uporabo sredstva za varno podpisovanje pa še vrednost *0.4.0.1456.1.1*.

7.1.7. Način uporabe razširitvenega polja za omejitev uporabe politik

Da se prepreči nenadzorovano prenašanje zaupanja v verigi medsebojno priznanih overiteljev, je polje *PolicyConstrains* označeno kot kritično.

7.1.8. Specifični podatki o politiki

V razširitvenem polju za specifične podatke o politiki *certificatePolicies, policyQualifier* se objavi spletni naslov, kjer so objavljena pravila delovanja overitelja (ang. CPS Pointer).

Razširitveno polje za specifične podatke o politiki *certificatePolicies, policyQualifier* se ne uporablja za objavo obvestila uporabnikom (ang. User Notice).

7.1.9. Procesiranje oznake kritičnosti razširitvenih polj

Uporabniške aplikacije morajo procesirati razširitvena polja digitalnega potrdila, označena kot kritična, v skladu s priporočili [7] RFC 3280.

7.2. Profil registrov preklicanih potrdil

7.2.1. Verzija registrov preklicanih potrdil

Overitelji SIMoD-PKI izdajajo registre preklicanih potrdil verzije 2 v skladu s priporočilom [7] RFC 3280, ki vsebujejo naslednja osnovna polja:

Osnovno polje - angleški naziv	Osnovno polje - slovenski opis	Vrednost
version	verzija	v2
signature	algoritem za podpis registra	sha1WithRSAEncryption
Issuer	izdajatelj	razločevalno ime overitelja
thisUpdate	čas izdaje registra	čas izdaje po GMT
nextUpdate	čas izdaje naslednjega registra	čas naslednje izdaje po GMT
revokedCertificates:	preklicana potrdila	
userCertificate	preklicano potrdilo	serijska številka preklicanega potrdila
revocationDate	datum preklica	čas preklica
reasonCode	vzrok za preklic	Možne vrednosti: *Unspecified (0), keyCompromise (1), cACompromise (2), affiliationChanged(3), superseded (4), cessationOfOperation (5), certificateHold (6), removeFromCRL (8), privilegeWithdrawn (9), aACompromise (10)*

7.2.2. Razširitvena polja registrov preklicanih potrdil

Overitelji SIMoD-PKI izdajajo registre preklicanih potrdil verzije 2 v skladu s priporočilom [7] RFC 3280, ki vsebujejo naslednja standardna razširitvena polja:

Razširitveno polje - angleški naziv	Razširitveno polje - slovenski opis	Vrednost
CRLNumber	zaporedna številka registra	zaporedna številka registra
AuthorityKeyIdentifier	identifikator javnega ključa overitelja, ki podpisuje register preklicanih potrdil	*KeyID* = SHA-1 odtis javnega ključa overitelja

Overitelji lahko v registrih preklicanih potrdil uporabljajo dodatna standardna in lastna razširitvena polja.

7.3. Profil OSCP

7.3.1. Verzija OSCP

Ni podprto.

7.3.2. Razširitve OSCP

Ni podprto.

8. PREVERJANJE SKLADNOSTI IN OSTALE OBLIKE NADZORA

8.1. Pogostost inšpekcije

Pogostost inšpekcijskega nadzora je v pristojnosti inšpekcijske službe, ki je določena z [1] ZEPEP.

Svet za upravljanje z infrastrukturo javnih ključev na MO lahko kadarkoli zahteva preverjanje skladnosti delovanja overitelja s Politiko SIMoD-PKI in pravili delovanja overitelja, za kar pooblasti zunanjo inšpekcijsko službo ali organizacijo.

8.2. Pogoji za inšpektorja

Izvajalec inšpekcijskega nadzora mora imeti ustrezno dovoljenje za dostop do tajnih podatkov.

Zunanja inšpekcijska služba ali organizacija, ki jo Svet za upravljanje z infrastrukturo javnih ključev na MO pooblasti za preverjanje skladnosti delovanja overitelja s Politiko SIMoD-PKI in pravili delovanja overitelja, mora imeti ustrezna znanja in izkušnje s področja infrastrukture javnih ključev.

8.3. Relacija med inšpektorjem in overitelji SIMoD-PKI

Inšpektor mora biti neodvisen od infrastrukture javnih ključev na MO.

8.4. Področja inšpekcije

Inšpekcijski nadzor preverja skladnost delovanja overiteljev z [1] ZEPEP, Politiko SIMoD-PKI in pravili delovanja overitelja.

Zunanja inšpekcijska služba preverja samo skladnost delovanja overitelja s Politiko SIMoD-PKI in pravili delovanja overitelja.

Svet za upravljanje z infrastrukturo javnih ključev na MO ob nameri medsebojnega priznavanja z drugimi overitelji zagotovi drugim overiteljem jamstva, da overitelj izpolnjuje zahteve iz Politike SIMoD-PKI ter zahteva od drugih overiteljev enaka jamstva, da le ti delujejo v skladu s svojimi politikami. Način in podrobnosti izmenjave ugotovitev o inšpekciji med medsebojno priznanimi overitelji so določeni v pogodbi o medsebojnem priznavanju.

8.5. Postopki po opravljeni inšpekciji

V primeru ugotovljenih nepravilnosti mora overitelj pripraviti načrt za odpravo pomanjkljivosti in poročilo o odpravi pomanjkljivosti, ki ju posreduje inšpektorju in Svetu za upravljanje z infrastrukturo javnih ključev na MO.

Če overitelj pomanjkljivosti ne odpravi, je Svet za upravljanje z infrastrukturo javnih ključev na MO dolžan ukrepati v okviru naslednjih možnosti:

- opozori na pomanjkljivosti, vendar kljub temu dovoli obratovanje overitelja do naslednje predvidene inšpekcije ali
- pred preklicem overiteljevega potrdila dodeli overitelju 30 dni za odpravo pomanjkljivosti, v tem času dovoli overitelju delovanje ali
- odredi preklic overiteljevega potrdila.

8.6. Prejemniki ugotovitev o inšpekciji

Ugotovitve inšpekcijskega nadzora mora inšpektor poslati Svetu za upravljanje z infrastrukturo javnih ključev na MO.

Overitelj se na osnovi ugotovitev inšpektorja odloči ali je potrebno obvestiti imetnike in ostale udeležence. Obvestilo imetnikom in ostalim udeležencem objavi v skladu s poglavjem 9.11. Obvestila in komuniciranje z udeleženci.

Način in podrobnosti izmenjave ugotovitev o inšpekciji med medsebojno priznanimi overitelji so določeni v pogodbi o medsebojnem priznavanju.

9. OSTALE POSLOVNE IN PRAVNE ZADEVE

9.1. Cenik

9.1.1. Cena prve in ponovne izdaje digitalnega potrdila

Ni predpisano.

9.1.2. Cena dostopa do digitalnega potrdila

Ni predpisano.

9.1.3. Cena dostopa do podatka o statusu in preklicu potrdila

Ni predpisano.

9.1.4. Cene drugih storitev

Ni predpisano.

9.1.5. Povračilo stroškov

Ni predpisano.

9.2. Finančna odgovornost

9.2.1. Višina zavarovanja

Ministrstvo za obrambo ima glede delovanja overiteljev infrastrukture javnih ključev na MO ustrezno zavarovano svojo odgovornost skladno z [1] ZEPEP oziroma [2] Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje.

9.2.2. Druge oblike zavarovanja

Ni predpisano.

9.2.3. Zavarovanje ali jamstva za končne uporabnike

Ni predpisano.

9.3. Zaupnost poslovnih informacij

9.3.1. Obseg zaupnih poslovnih informacij

Ni predpisano.

9.3.2. Informacije izven obsega zaupnih poslovnih informacij

Ni predpisano.

9.3.3. Odgovornost za zagotavljanje zaupnosti poslovnih informacij

Ni predpisano.

9.4. Zaupnost osebnih podatkov

9.4.1. Načrt zagotavljanja zaupnosti osebnih podatkov

Overitelji pridobijo osebne podatke od bodočih imetnikov z zahtevkom za izdajo digitalnega potrdila. Pridobljeni podatki se uporabljajo izključno za potrebe izdaje in upravljanja digitalnih potrdil. Osebni podatki imetnikov se obdelujejo kot določa [11] Zakon o varstvu osebnih podatkov.

9.4.2. Obseg osebnih podatkov, ki se obravnavajo kot zaupni

Osebne podatke določa [11] Zakon o varstvu osebnih podatkov.

9.4.3. Osebni podatki, ki se ne obravnavajo kot zaupni

Podatki, objavljeni v digitalnih potrdilih, imenikih in registrih preklicanih potrdil, se ne obravnavajo kot zaupni.

9.4.4. Odgovornost glede varovanja osebnih podatkov

Za varovanje osebnih podatkov je odgovorna prijavna služba.

9.4.5. Dovoljenje za uporabo osebnih podatkov

Prijavna služba mora od bodočih imetnikov pridobiti dovoljenje za uporabo osebnih podatkov v postopku preverjanja istovetnosti in v postopkih upravljanja digitalnih potrdil ter za objavo podatkov, vsebovanih v digitalnih potrdilih, imenikih in registrih preklicanih potrdil.

9.4.6. Posredovanje osebnih podatkov v sodnih in upravnih postopkih

Osebne podatke se v sodnih in upravnih postopkih posreduje v skladu z [11] Zakon o varstvu osebnih podatkov in ostalimi predpisi.

9.4.7. Druge okoliščine posredovanja osebnih podatkov

Ni predpisano.

9.5. Zaščita intelektualne lastnine

Ministrstvo za obrambo Republike Slovenije je lastnik vseh podatkov v digitalnih potrdilih, imenikih in registrih preklicanih potrdil.

Na zasebnem ključu za podpisovanje pripadajo vse pravice imetniku digitalnega potrdila za podpisovanje.

Ob pogojih iz poglavja 4.12.2 Odkrivanje kopije ključev za dešifriranje se lahko prenese lastništvo zasebnega ključa za dešifriranje drugemu subjektu kot je imetnik digitalnega potrdila.

9.6. Odgovornosti in jamstva

9.6.1. Odgovornosti in jamstva overitelja

Overitelj jamči, da upravlja z digitalnimi potrdili v skladu s Politiko SIMoD-PKI in svojimi pravili delovanja. Svet za upravljanje z infrastrukturo javnih ključev na MO predstavlja overitelje SIMoD-PKI in jamči za izpolnjevanje njihovih obveznosti.

9.6.2. Odgovornost in jamstva prijavne službe

Prijavna služba je odgovorna za skladnost identifikacijskih postopkov s Politiko SIMoD-PKI in točnost podatkov v zahtevkih. Za pravilnost delovanja prijavne službe jamči overitelj, oziroma Svet za upravljanje z infrastrukturo javnih ključev na MO.

9.6.3. Odgovornost in jamstva imetnikov digitalnih potrdil

Imetnik digitalnega potrdila jamči, da:

- je bil seznanjen s Politiko SIMoD PKI pred podpisom zahtevka za izdajo digitalnega potrdila,
- ravna v skladu s Politiko SIMoD-PKI in ostalimi pravnimi akti,
- spremlja obvestila overiteljev SIMoD-PKI in ravna v skladu z njimi,
- je prijavni službi in operativnemu osebju overitelja, ki upravlja z digitalnimi potrdili, posredoval popolne in točne podatke in
- se strinja z javno objavo svojega digitalnega potrdila.

Obveznosti imetnikov digitalnih potrdil glede uporabe zasebnih ključev in digitalnih potrdil so opisane v poglavju 4.5.1.3 Uporabniški zasebni ključi in digitalna potrdila

9.6.4. Odgovornost in jamstva tretjih oseb

Tretja oseba, ki se zanaša na digitalna potrdila overitelja SIMoD-PKI, jamči, da uporablja digitalna potrdila le za namene, določene v Politiki SIMoD-PKI in pravilih delovanja overitelja, ki je izdal digitalno potrdilo ter v pogodbi o medsebojnem priznavanju.

Obveznosti tretjih oseb glede uporabe zasebnih ključev in digitalnih potrdil so opisane v poglavju 4.5.2 Uporaba digitalnih potrdil s strani tretjih oseb.

9.6.5. Odgovornost in jamstva drugih udeležencev

Ni relevantno.

9.7. Zanikanje odgovornosti overitelja

Overitelj SIMoD-PKI ni odgovoren za škodo (direktno ali posredno), izgube, stroške ter terjatve, ki izhajajo iz ali so nastale zaradi uporabe digitalnih potrdil in z njimi povezanih ključev, če:

- je bilo digitalno potrdilo izdano kot rezultat napake ali neverodostojnosti podatkov v zahtevku,
- je bilo digitalno potrdilo spremenjeno ali kakor koli drugače modificirano,
- je bilo digitalno potrdilo uporabljeno po preteku veljavnosti,
- je bilo digitalno potrdilo uporabljeno po preklicu in objavi v registru preklicanih potrdil,
- je bil zasebni ključ zlorabljen ali obstaja sum, da je bil zlorabljen,
- je bilo digitalno potrdilo uporabljeno v drugačne namene, kot je dovoljeno s Politiko SIMoD-PKI, pravili delovanja overitelja ali morebitni drugi pogodbi,

- imetnik ali tretja oseba ni postopala v skladu s predpisanimi postopki v Politiki SIMoD-PKI, pravili delovanja overitelja ali morebitni drugi pogodbi in obvestili overitelja ali
- je nastala škoda zaradi napake v delovanju strojne ali programske opreme imetnika ali tretje osebe,
- je do ravnanja v nasprotju s Politiko SIMoD-PKI ali ostalimi dokumenti prišlo zaradi višje sile, to je izredne nepredvidljive okoliščine na katere udeleženci infrastrukture javnih ključev na MO ne morejo vplivati (na primer naravne nesreče, terorizem, …).

9.8. Omejitve odgovornosti overiteljev SIMoD-PKI

Overitelj SIMoD-PKI jamči za vrednost posameznega pravnega posla do vrednosti glede na vrsto digitalnega potrdila:

- za digitalna potrdila VISOKE stopnje zaupanja do 5.000 EUR in
- za digitalna potrdila SREDNJE stopnje zaupanja do 1.000 EUR.

Za digitalna potrdila NIZKE stopnje zaupanja overitelji SIMoD-PKI ne prevzemajo jamstva.

9.9. Zavarovanje pred škodo zaradi neizpolnjevanja obveznosti

Za škodo odgovarja stranka, ki je škodo povzročila zaradi neizpolnjevanja ali neupoštevanja relevantnih pravil in predpisov.

9.10. Začetek in prenehanje veljavnosti

9.10.1.Začetek veljavnosti

Politika SIMoD-PKI začne veljati naslednji dan po podpisu, uporabljati pa se začne trideset (30) dni po podpisu.

9.10.2.Prenehanje veljavnosti

Veljavnost Politike SIMoD-PKI ni časovno omejena in velja do uveljavitve nove verzije.

9.10.3.Posledice prenehanja veljavnosti

Po prenehanju veljavnosti Politike SIMoD-PKI zaradi objave nove verzije imetniki praviloma uporabljajo obstoječa digitalna potrdila v skladu z določili Politike SIMoD-PKI in pravili delovanja overitelja, po kateri so bila izdana. V primeru, da zaradi spremenjenih okoliščin to ne bo več mogoče, bo overitelj ob izdaji nove verzije Politike SIMoD-PKI in posledično novih pravilih delovanja obvestil imetnike.

9.11. Obvestila in komuniciranje z udeleženci

Obvestila udeležencem infrastrukture javnih ključev na MO so objavljena na spletni strani: http://www.simod-pki.mors.si.

9.12. Spreminjanje dokumenta

9.12.1.Postopek uveljavitve spremembe

Svet za upravljanje z infrastrukturo javnih ključev na MO pripravi spremembe Politike SIMoD-PKI in jih predlaga ministru v sprejem.

9.12.2.Postopek in roki obveščanja

Spremembe Politike SIMoD-PKI je potrebno objaviti v skladu s poglavjem 9.11. Obvestila in komuniciranje z udeleženci. Izjema je vnos uredniških in tipografskih popravkov, ki smiselno ne vplivajo na vsebino Politike SIMoD-PKI.

Svet za upravljanje z infrastrukturo javnih ključev na MO o spremembah Politike SIMoD-PKI pisno obvesti medsebojno priznane overitelje najmanj osem (8) dni pred uveljavitvijo sprememb.

9.12.3.Spremembe, ki zahtevajo novo identifikacijsko oznako politike

Overitelj po lastni presoji odloči, ali so spremembe Politike SIMoD-PKI takšne, da zahtevajo objavo novih pravil delovanja in spremembe identifikacijskih oznak politik delovanja.

9.13. Reševanje sporov

Stranke si bodo prizadevale za sporazumno reševanje sporov, če pa to ne bo mogoče, je za reševanje sporov pristojno sodišče v Ljubljani. Stranke za reševanje sporov dogovorijo izključno uporabo predpisov Republike Slovenije.

9.14. Veljavna zakonodaja

Overitelji SIMoD-PKI delujejo v skladu z predpisi in priporočili:

[1]	ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 – UPB1, 61/06)
[2]	Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje	(Uradni list RS, št. 77/00, 2/01 in 86/06)
[3]	ETSI TS 101 456	Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates
[4]	ETSI TS 101 862	Qualified Certificate profile
[5]	EU Direktiva o elektronskem podpisu	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE CONCIL of 13 December 1999 on a Community framework for electronic signatures
[6]	RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[7]	RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

9.15. Ostala relevantna zakonodaja

Overitelji SIMoD-PKI delujejo morajo pri svojem delovanju upoštevati tudi:

[8] ETSI TS 102 023 Policy requirements for time-stamping authorities

[9] ZObr Zakon o obrambi (Uradni list RS, št. 103/04 – UPB1)

[10] ZTP Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – UPB2, 9/10)

[11] Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – UPB1)

9.16. Razne določbe

Ni raznih določb.

9.17. Ostale določbe

Ni ostalih določb.