REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Pravila delovanja overitelja SIMoD-CA-Restricted, javni del

(Javna pravila SIMoD-CA-Restricted)

Verzija 2.0

Zgodovina sprememb Pravil delovanja overitelja SIMoD-CA-Restricted, javni del:

Izdaja:	Spremembe glede na prejšnjo izdajo:
Pravila delovanja overitelja SIMoD-CA-Restricted, javni del, verzija 2.0	• Pristojnost sprejemanja Pravil delovanja overitelja SIMoD-CA-Restricted je prenesena na Svet za upravljanje z infrastrukturo javnih ključev na MO, • spremenjeno je pravilo za določanje identifikacijskih oznak politik digitalnih potrdil, • dokument nima več identifikacijske oznake, • 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 pridobitve digitalnih potrdil NIZKE stopnje zaupanja.
Spremembe in dopolnitve Pravil delovanja overitelja SIMoD-CA-Restricted, javni del, številka: 382-5/2006-44, datum: 27.12.2007	• Spremenjeno je pravilo za določanje identifikacijske oznake dokumenta, • dopolnjena so določila glede razločevalnega imena imetnika, • dopolnjena so določila glede interpretacije imen, • v postopku izdaje digitalnega potrdila je operativnemu osebju dodana obveza preverjanja pravilnosti naslova elektronske pošte bodočega imetnika.
Pravila delovanja overitelja SIMoD-CA-Restricted, javni del, šifra: 382-5/2006-13, datum: 17.7.2006	V infrastrukturo javnih ključev na MO je umeščen korenski overitelj SIMoD-CA-Root in podrejeni overitelji.
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 7

1.1. Pregled 7
1.2. Identifikacijske oznake politik delovanja 8
1.3. Udeleženci infrastrukture javnih ključev 9
1.3.1. Overitelj SIMoD-CA-Restricted 9
1.3.1.1. Svet za upravljanje z infrastrukturo javnih ključev na MO 9
1.3.1.2. Operativno osebje overitelja SIMoD-CA-Restricted 10
1.3.2. Prijavna služba 10
1.3.3. Imetniki digitalnih potrdil 10
1.3.4. Tretje osebe 11
1.3.5. Posredno odgovorni organi 11
1.4. Namen uporabe digitalnih potrdil 11
1.4.1. Dovoljena uporaba digitalnih potrdil 12
1.4.1.1. Stopnja zaupanja v digitalno potrdilo 12
1.4.1.2. Uporaba digitalnih potrdil VISOKE in SREDNJE stopnje zaupanja 13
1.4.1.3. Uporaba digitalnih potrdil NIZKE stopnje zaupanja 13
1.4.2. Nedovoljena uporaba digitalnih potrdil 13
1.5. Upravljanje s Pravili delovanja overitelja SIMoD-CA-Restricted 13
1.5.1. Organ, ki upravlja s tem dokumentom 13
1.5.2. Kontaktna oseba 13
1.5.3. Odgovorni organ za odobritev skladnosti Pravil delovanja overitelja SIMoD-CA-Restricted s Politiko SIMoD-PKI 14
1.5.4. Postopek odobritve Pravil delovanja overitelja SIMoD-CA-Restricted 14
1.6. Pojmi in kratice 14

2. ODGOVORNOST ZA OBJAVE IN IMENIK 18

2.1. Objave dokumentov in imenik 18
2.2. Objave informacij o digitalnih potrdilih 18
2.3. Čas in pogostost objav 19
2.4. Dostop do podatkov v imeniku in na spletni strani 19

3. PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI 20

3.1. Določanje imen 20
3.1.1. Vrste imen 20
3.1.2. Potreba po smiselnosti imen 20
3.1.3. Anonimnost imetnikov in uporaba psevdonimov 20
3.1.4. Pravila za interpretacijo različnih oblik imen 20
3.1.5. Edinstvenost imen 20
3.1.6. Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk 20
3.2. Preverjanje istovetnosti imetnikov ob prvi registraciji 21
3.2.1. Metode dokazovanja lastništva zasebnega ključa 21
3.2.2. Preverjanje istovetnosti za imetnike, ki niso fizične osebe 21
3.2.2.1. Digitalna potrdila za organizacijske enote MO in institucije, ki opravljajo naloge povezane z obrambo države 21
3.2.2.2. Digitalna potrdila za organizacijske ali funkcijske vloge 21
3.2.2.3. Digitalna potrdila za strežnike, drugo strojno in programsko opremo, izdajatelje varnih časovnih žigov ter druge ponudnike storitev overjanja 21
3.2.3. Preverjanje istovetnosti za fizične osebe 22
3.2.3.1. Zaposleni v MO in institucijah, ki opravljajo naloge povezane z obrambo države 22
3.2.3.2. Digitalna potrdila za vojaške dolžnosti v SV 22
3.2.4. Podatki o naročniku, ki se ne preverjajo 22
3.2.5. Preverjanje pooblastil 22
3.2.6. Merila za medsebojno povezovanje 23
3.3. Preverjanje imetnikov za ponovno izdajo digitalnega potrdila 23
3.3.1. Preverjanje istovetnosti pri rutinski ponovni izdaji digitalnih potrdil 23
3.3.2. Preverjanje istovetnosti za ponovno izdajo digitalnega potrdila po preklicu 23
3.4. Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila 23

4. UPRAVLJANJE Z DIGITALNIMI POTRDILI 24

4.1. Pridobitev digitalnega potrdila 24

4.1.1. Kdo lahko zaprosi za izdajo digitalnega potrdila ... 24
4.1.2. Postopek bodočega imetnika za pridobitev digitalnega potrdila in odgovornosti 24
4.2. Obdelava zahtevka za izdajo digitalnega potrdila ... 24
4.2.1. Preverjanje istovetnosti bodočega imetnika ... 24
4.2.2. Odobritev ali zavrnitev izdaje digitalnega potrdila ... 24
4.2.3. Čas za obdelavo zahtevka za izdajo digitalnega potrdila ... 25
4.3. Izdaja digitalnega potrdila ... 25
4.3.1. Postopki overitelja SIMoD-CA-Restricted ob izdaji potrdil ... 25
4.3.1.1. Dostava zasebnega ključa imetniku ... 25
4.3.1.2. Dostava overiteljevega javnega ključa imetniku ... 25
4.3.2. Obvestilo naročnikom o izdaji digitalnega potrdila ... 26
4.4. Prevzem digitalnega potrdila ... 26
4.4.1. Postopek prevzema digitalnega potrdila ... 26
4.4.2. Objava digitalnega potrdila ... 26
4.4.3. Obveščanje drugih udeležencev o izdaji digitalnega potrdila ... 26
4.5. Uporaba ključev in digitalnih potrdil ... 26
4.5.1. Uporaba ključev in digitalnih potrdil imetnikov ... 27
4.5.1.1. Zasebni ključi in digitalna potrdila overiteljev ... 27
4.5.1.2. Zasebni ključi in digitalna potrdila prijavne službe ... 27
4.5.1.3. Uporabniški zasebni ključi in digitalna potrdila ... 27
4.5.2. Uporaba digitalnih potrdil s strani tretjih oseb ... 27
4.6. Ponovna izdaja digitalnega potrdila brez spremembe javnega ključa ... 27
4.7. Ponovna izdaja digitalnih potrdil ... 28
4.7.1. Razlogi za ponovno izdajo digitalnega potrdila ... 28
4.7.2. Kdo lahko zahteva ponovno izdajo digitalnega potrdila ... 28
4.7.3. Obdelava zahtevkov za ponovno izdajo digitalnega potrdila ... 28
4.7.4. Obvestilo imetniku o izdaji novega digitalnega potrdila ... 28
4.7.5. Postopek potrditve prevzema novega digitalnega potrdila ... 28
4.7.6. Objava novega digitalnega potrdila ... 29
4.7.7. Obveščanje drugih udeležencev o izdaji digitalnega potrdila ... 29
4.8. Sprememba digitalnega potrdila ... 29
4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila ... 29
4.9.1. Okoliščine preklica ... 29
4.9.1.1. Okoliščine preklica imetniških digitalnih potrdil ... 29
4.9.1.2. Okoliščine preklica digitalnega potrdila korenskega overitelja ... 29
4.9.1.3. Okoliščine preklica digitalnega potrdila o priznavanju drugega overitelja ... 29
4.9.1.4. Okoliščine preklica digitalnega potrdila overitelja SIMoD-CA-Restricted ... 29
4.9.2. Kdo lahko zahteva preklic ... 29
4.9.2.1. Kdo lahko zahteva preklic digitalnega potrdila imetnika ... 29
4.9.2.2. Kdo lahko zahteva preklic digitalnega potrdila korenskega overitelja ... 30
4.9.2.3. Kdo lahko zahteva preklic digitalnega potrdila o priznavanju drugega overitelja ... 30
4.9.2.4. Kdo lahko zahteva preklic digitalnega potrdila overitelja SIMoD-CA-Restricted ... 30
4.9.3. Postopki za preklic ... 30
4.9.3.1. Postopki preklica digitalnih potrdil imetnikov ... 30
4.9.3.2. Postopki preklica digitalnega potrdila korenskega overitelja ... 30
4.9.3.3. Postopki preklica digitalnega potrdila o priznavanju drugega overitelja ... 30
4.9.3.4. Postopki preklica digitalnega potrdila overitelja SIMoD-CA-Restricted ... 30
4.9.4. Čas za posredovanje zahtevka za preklic ... 31
4.9.5. Čas od prejema zahtevka za preklic do preklica ... 31
4.9.5.1. Čas za preklic digitalnega potrdila imetnika ... 31
4.9.5.2. Čas za preklic digitalnega potrdila korenskega overitelja ... 31
4.9.5.3. Čas za preklic digitalnega potrdila o priznavanju drugega overitelja ... 31
4.9.5.4. Čas za preklic digitalnega potrdila overitelja SIMoD-CA-Restricted ... 31
4.9.6. Obveza preverjanja registra preklicanih potrdil ... 31
4.9.7. Pogostost objav registrov preklicanih potrdil ... 32
4.9.8. Dovoljene zakasnitve pri objavi registrov preklicanih potrdil ... 32
4.9.9. Storitev sprotnega preverjanje statusa digitalnih potrdil ... 32
4.9.10. Obveza sprotnega preverjanja statusa preklicanih potrdil ... 32
4.9.11. Ostale oblike objavljanja preklicanih digitalnih potrdil ... 32
4.9.12. Posebne zahteve glede zlorabe ključa ... 32
4.9.13. Okoliščine za začasno ukinitev veljavnosti ... 32
4.9.14. Kdo lahko zahteva začasno ukinitev veljavnosti ... 32

4.9.15. Postopki za začasno ukinitev veljavnosti ... 32
4.9.16. Omejitve obdobja začasne ukinitve veljavnosti ... 32
4.10. Storitve objavljanja statusa digitalnih potrdil ... 32
4.10.1. Tehnične lastnosti storitve ... 32
4.10.2. Razpoložljivost storitve ... 33
4.10.3. Dodatne možnosti ... 33
4.11. Predčasna prekinitev veljavnosti digitalnih potrdil ... 33
4.12. Varnostno kopiranje in odkrivanje zasebnega ključa ... 33
4.12.1. Povrnitev zgodovine ključev za dešifriranje ... 33
4.12.2. Odkrivanje kopije ključev za dešifriranje ... 34
4.12.3. Zaščita odkritega zasebnega ključa in postopek prenosa ... 34

5. FIZIČNO VAROVANJE, ORGANIZACIJSKI VARNOSTNI UKREPI IN ZAHTEVE ZA OSEBJE ... 35

5.1. Fizično varovanje ... 35
5.1.1. Lokacija in konstrukcija prostorov ter fizični dostop ... 35
5.1.2. Fizični dostop ... 35
5.1.3. Napajanje in klimatske naprave ... 35
5.1.4. Zaščita pred poplavo ... 35
5.1.5. Zaščita pred ognjem ... 35
5.1.6. Shranjevanje medijev ... 35
5.1.7. Odstranjevanje odpadkov ... 35
5.1.8. Hranjenje na oddaljeni lokaciji ... 36
5.2. Organizacijski varnostni ukrepi ... 36
5.2.1. Organizacija overitelja SIMoD-CA-Restricted ... 36
5.2.1.1. Operativno osebje overitelja SIMoD-CA-Restricted ... 36
5.2.1.2. Prijavna služba ... 36
5.2.1.3. Druge funkcije ... 37
5.2.2. Število oseb, potrebnih za izvedbo postopkov ... 37
5.2.3. Preverjanje istovetnosti operativnega osebja ... 37
5.3. Zahteve za osebje overitelja ... 37
5.3.1. Kvalifikacije, izkušnje in varnostno preverjanje ... 37
5.3.2. Dovoljenja za dostop do tajnih podatkov ... 38
5.3.3. Usposabljanje osebja overitelja ... 38
5.3.4. Pogostost dodatnih usposabljanj ... 38
5.3.5. Kroženje med delovnimi mesti ... 38
5.3.6. Ukrepi ob kršitvah pooblastil ... 38
5.3.7. Zunanji izvajalci ... 38
5.3.8. Dokumentacija za osebje overitelja ... 38
5.4. Postopki varnostnih pregledov sistema ... 38
5.4.1. Vrste beleženih dogodkov ... 38
5.4.2. Pogostost pregleda dnevnikov beleženih dogodkov ... 39
5.4.3. Obdobje hranjenja dnevnikov beleženih dogodkov ... 39
5.4.4. Zaščita dnevnikov beleženih dogodkov ... 39
5.4.5. Varnostne kopije dnevnikov beleženih dogodkov ... 40
5.4.6. Način zbiranja beleženih dogodkov ... 40
5.4.7. Obveščanje povzročitelja dogodka ... 40
5.4.8. Ocena in odprava ranljivosti ... 40
5.5. Arhiviranje podatkov ... 40
5.5.1. Vrste arhiviranih podatkov ... 40
5.5.2. Obdobje hranjenja arhiva ... 40
5.5.3. Zaščita arhiva ... 40
5.5.4. Varnostna kopija arhiva ... 41
5.5.5. Časovno žigosanje zapisov ... 41
5.5.6. Način arhiviranja ... 41
5.5.7. Postopek vpogleda v in verifikacije arhiva ... 41
5.6. Zamenjava ključev overitelja SIMoD-CA-Restricted ... 41
5.7. Okrevalni načrt ... 41
5.7.1. Postopki v primeru okvar in zlorab ... 41
5.7.2. Uničenje programske, strojne opreme ali podatkov overitelja ... 41
5.7.3. Zloraba zasebnega ključa overitelja SIMoD-CA-Restricted ... 42

5.7.4. Zagotavljanje kontinuitete delovanja po nesrečah ... 42
5.8. Prenehanje delovanja overitelja SIMoD-CA-Restricted ... 42
6. TEHNIČNE VARNOSTNE ZAHTEVE ... 43
6.1. Generiranje in namestitev para ključev ... 43
6.1.1. Generiranje para ključev ... 43
6.1.2. Dostava zasebnega ključa imetniku ... 44
6.1.3. Dostava imetnikovega javnega ključa overitelju ... 44
6.1.4. Dostava overiteljevega javnega ključa uporabnikom ... 45
6.1.5. Dolžina ključev ... 45
6.1.6. Parametri za generiranje javnih ključev in preverjanje parametrov ... 45
6.1.7. Namen uporabe ključev ... 45
6.2. Zaščita zasebnih ključev in zahteve za kriptografske module ... 45
6.2.1. Standardi za kriptografski modul ... 45
6.2.2. Nadzor zasebnega ključa z več pooblaščenimi osebami ... 46
6.2.3. Odkrivanje zasebnega ključa ... 46
6.2.4. Varnostno kopiranje zasebnih ključev ... 46
6.2.5. Arhiviranje zasebnega ključa ... 46
6.2.6. Zapis zasebnega ključa v kriptografski modul in iz njega ... 46
6.2.7. Hranjenje zasebnega ključev v kriptografskem modulu ... 46
6.2.8. Postopek za aktiviranje zasebnega ključa ... 47
6.2.9. Postopek za deaktiviranje zasebnega ključa ... 47
6.2.10. Postopek za uničenje zasebnega ključa ... 47
6.2.11. Stopnja varnosti kriptografskih modulov ... 47
6.3. Ostali vidiki upravljanja s pari ključev ... 47
6.3.1. Arhiviranje javnega ključa ... 47
6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil ... 48
6.4. Gesla za dostop do zasebnih ključev ... 48
6.4.1. Določanje gesel za dostop do zasebnih ključev v kriptografskih modulih ... 48
6.4.2. Zaščita gesel ... 48
6.4.3. Druge zahteve za gesla ... 48
6.5. Varnostne zahteve za računalnike ... 48
6.5.1. Specifične tehnične varnostne zahteve za računalnike ... 48
6.5.2. Raven varnostne zaščite računalnikov ... 49
6.6. Tehnični nadzor življenjskega cikla overitelja ... 49
6.6.1. Nadzor razvoja sistema ... 49
6.6.2. Upravljanje varnosti ... 49
6.6.3. Upravljanje varnosti čez življenjski cikel ... 49
6.7. Varnostne kontrole na ravni računalniškega omrežja ... 49
6.8. Časovno žigosanje ... 49
7. PROFIL DIGITALNIH POTRDIL IN REGISTROV PREKLICANIH POTRDIL ... 50
7.1. Profil digitalnih potrdil ... 50
7.1.1. Verzija digitalnih potrdil ... 50
7.1.2. Razširitvena polja ... 51
7.1.3. Identifikacijske oznake algoritmov ... 53
7.1.4. Oblike imen ... 53
7.1.5. Omejitve imen ... 53
7.1.6. Identifikacijska oznaka politik ... 53
7.1.7. Način uporabe razširitvenega polja za omejitev uporabe politik ... 53
7.1.8. Specifični podatki o politiki ... 53
7.1.9. Procesiranje oznake kritičnosti razširitvenih polj ... 53
7.2. Profil registrov preklicanih potrdil ... 54
7.2.1. Verzija registrov preklicanih potrdil ... 54
7.2.2. Razširitvena polja registrov preklicanih potrdil ... 54
7.3. Profil OSCP ... 54
7.3.1. Verzija OSCP ... 54
7.3.2. Razširitve OSCP ... 54
8. PREVERJANJE SKLADNOSTI IN OSTALE OBLIKE NADZORA ... 55
8.1. Pogostost inšpekcije ... 55

8.2. Pogoji za inšpektorja 55
8.3. Relacija med inšpektorjem in overitelji SIMoD-PKI 55
8.4. Področja inšpekcije 55
8.5. Postopki po opravljeni inšpekciji 55
8.6. Prejemniki ugotovitev o inšpekciji 56
9. OSTALE POSLOVNE IN PRAVNE ZADEVE 57
9.1. Cenik 57
9.1.1. Cena prve in ponovne izdaje digitalnega potrdila 57
9.1.2. Cena dostopa do digitalnega potrdila 57
9.1.3. Cena dostopa do podatka o statusu in preklicu potrdila 57
9.1.4. Cene drugih storitev 57
9.1.5. Povračilo stroškov 57
9.2. Finančna odgovornost 57
9.2.1. Višina zavarovanja 57
9.2.2. Druge oblike zavarovanja 57
9.2.3. Zavarovanje ali jamstva za končne uporabnike 57
9.3. Zaupnost poslovnih informacij 57
9.3.1. Obseg zaupnih poslovnih informacij 57
9.3.2. Informacije izven obsega zaupnih poslovnih informacij 57
9.3.3. Odgovornost za zagotavljanje zaupnosti poslovnih informacij 57
9.4. Zaupnost osebnih podatkov 57
9.4.1. Načrt zagotavljanja zaupnosti osebnih podatkov 57
9.4.2. Obseg osebnih podatkov, ki se obravnavajo kot zaupni 58
9.4.3. Osebni podatki, ki se ne obravnavajo kot zaupni 58
9.4.4. Odgovornost glede varovanja osebnih podatkov 58
9.4.5. Dovoljenje za uporabo osebnih podatkov 58
9.4.6. Posredovanje osebnih podatkov v sodnih in upravnih postopkih 58
9.4.7. Druge okoliščine posredovanja osebnih podatkov 58
9.5. Zaščita intelektualne lastnine 58
9.6. Odgovornosti in jamstva 58
9.6.1. Odgovornosti in jamstva overitelja SIMoD-CA-Restricted 58
9.6.2. Odgovornost in jamstva prijavne službe 58
9.6.3. Odgovornost in jamstva imetnikov digitalnih potrdil 58
9.6.4. Odgovornost in jamstva tretje osebe 59
9.6.5. Odgovornost in jamstva drugih udeležencev 59
9.7. Zanikanje odgovornosti overitelja SIMoD-CA-Restricted 59
9.8. Omejitve odgovornosti overitelja SIMoD-CA-Restricted 59
9.9. Zavarovanje pred škodo zaradi neizpolnjevanja obveznosti 59
9.10. Začetek in prenehanje veljavnosti 60
9.10.1. Začetek veljavnosti 60
9.10.2. Prenehanje veljavnosti 60
9.10.3. Posledice prenehanja veljavnosti 60
9.11. Obvestila in komuniciranje z udeleženci 60
9.12. Spreminjanje dokumenta 60
9.12.1. Postopke uveljavitve spremembe 60
9.12.2. Postopek obveščanja in rok za pripombe 60
9.12.3. Spremembe, ki zahtevajo novo identifikacijsko oznako politike 60
9.13. Reševanje sporov 60
9.14. Veljavna zakonodaja 60
9.15. Ostala relevantna zakonodaja 61
9.16. Razne določbe 61
9.17. Končne določbe 62

Na podlagi 102. člena Zakona o obrambi (Uradni list RS, št. 103/04 - uradno prečiščeno besedilo) v zvezi z 28. in 29. členom Uredbe o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06) ter v skladu z 9. odstavkom poglavja 1.1. Pregled Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, Verzija 2.0, št. 382-5/2006-109 z dne 25.08.2010 izdajam

PRAVILA DELOVANJA OVERITELJA SIMoD-CA-Restricted, JAVNI DEL

(JAVNA PRAVILA SIMoD-CA-Restricted)

Verzija 2.0

1. UVOD

1.1. Pregled

Ministrstvo za obrambo Republike Slovenije (v nadaljnjem besedilu: MO) upravlja z infrastrukturo javnih ključev na MO (ang. **S**lovenian **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 SIMoD-CA-Root (ang. **S**lovenian **M**inistry **o**f **D**efence **Root C**ertification **A**uthority) in podrejeni overitelji digitalnih potrdil, v nadaljevanju overitelji SIMoD-PKI.

Overitelj SIMoD-CA-Restricted (ang. **S**lovenian **M**inistry **o**f **D**efence **Restricted C**ertification **A**uthority) je podrejeni overitelj korenskega overitelja SIMoD-CA-Root.

Overitelj SIMoD-CA-Restricted deluje v skladu s [3] Politika SIMoD-PKI, ki 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 ter tretje osebe, ki se zanašajo na digitalna potrdila ter drugi overitelji, ki se želijo povezovati z overitelji SIMoD-PKI.

Pravila delovanja overitelja SIMoD-CA-Restricted, javni del, predstavljajo javni del notranjih pravil overitelja v skladu z [2] Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje.

Polni naziv pričujočega dokumenta je Pravila delovanja overitelja SIMoD-CA-Restricted, javni del. Skrajšani naziv dokumenta je Javna pravila SIMoD-CA-Restricted.

Javna pravila SIMoD-CA-Restricted, podajajo opis overiteljeve infrastrukture, postopkov overitelja in izpolnjevanje zahtev Politike SIMoD-PKI. Za oceno zaupanja v SIMoD-PKI kot celoto je potrebno poleg tega dokumenta upoštevati še dokumenta [3] Politika SIMoD-PKI in [4] Pravila SIMoD-CA-Root.

Overitelj SIMoD-CA-Restricted izdaja digitalna potrdila za potrebe uporabnikov in aplikacij v omrežju MO in SV klasificiranem za obdelavo podatkov stopnje tajnosti INTERNO za zagotavljanje varnostnih storitev pri hranjenju in prenosu podatkov z ali brez stopnje tajnosti, za digitalno podpisovanje datotek, sporočil in elektronskih obrazcev ter preverjanje istovetnosti oseb in gradnikov informacijske infrastrukture kot so strežniki, usmerjevalniki, požarne pregrade in imeniki.

Overitelj SIMoD-CA-Restricted izdaja digitalna potrdila z naslednjimi nameni uporabe:

- za preverjanje digitalnega podpisa za storitve prepoznavanja in preverjanja istovetnosti, celovitosti in nezanikanja,
- za šifriranje za storitve zagotavljanja tajnosti oziroma zaupnosti,
- za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe in
- za izdajatelje varnih časovnih žigov.

Overitelj SIMoD-CA-Restricted izdaja naslednje tipe digitalnih potrdil:

- upravljana digitalna potrdila - tip A, imenovana tudi *Entrust ID*[1],
- neupravljana digitalna potrdila - tip B, imenovana tudi spletna[2] ali WEB[3] digitalna potrdila in
- digitalna potrdila za izdajatelje varnih časovnih žigov.

Dokument je skladen z [8] RFC 3647 in predstavlja pravila delovanja overitelja (ang. Certification Practices Statement, CPS) v odnosu na Politiko SIMoD-PKI, ki predstavlja politiko delovanja (ang. Certificate Policy, CP).

1.2. Identifikacijske oznake politik delovanja

V okviru upravljanih digitalnih potrdil oziroma *Entrust ID* overitelj SIMoD-CA-Restricted izdaja naslednje skupke potrdil tipa A, ki vključujejo 2 digitalna potrdila:

Upravljana digitalna potrdila, tip A oziroma *Entrust ID*				
Imetniki	Namen uporabe	Stopnja zaupanja	Identifikacijske oznake politik	Identifikacija ETSI TS 101 456
Fizične osebe	Digitalno potrdilo za preverjanje digitalnega podpisa	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.1.1, 0.4.0.1456.1.1	QCP public + SSCD
	Digitalno potrdilo za šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.2.1, 0.4.0.1456.1.1	QCP public + SSCD
Funkcijske ali organizacijske vloge	Digitalno potrdilo za preverjanje digitalnega podpisa	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.2.1.1, 0.4.0.1456.1.1	QCP public + SSCD
	Digitalno potrdilo za šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.2.2.1, 0.4.0.1456.1.1	QCP public + SSCD
	Digitalno potrdilo za preverjanje digitalnega podpisa	SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.2.1.1, 0.4.0.1456.1.2	QCP public
	Digitalno potrdilo za šifriranje	SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.2.2.1, 0.4.0.1456.1.2	QCP public
	Digitalno potrdilo za preverjanje digitalnega podpisa	NIZKA	1.3.6.1.4.1.22295.10.1.2.2.2.1.1	
	Digitalno potrdilo za šifriranje	NIZKA	1.3.6.1.4.1.22295.10.1.2.2.2.2.1	
Organizacijske enote MO, institucije, ki opravljajo naloge povezane z obrambo, vojaške dolžnosti	Digitalno potrdilo za preverjanje digitalnega podpisa	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.3.1.1, 0.4.0.1456.1.1	QCP public + SSCD
	Digitalno potrdilo za šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.3.2.1, 0.4.0.1456.1.1	QCP public + SSCD

[1] Poimenovanje upravljanih digitalnih potrdil v okviru uporabljene tehnološke rešitve.

[2] Ime spletno digitalno potrdilo izhaja iz zgodovine oziroma prvotnega namena uporabe neuprvljanih potrdil; tovrstna digitalna potrdila se pretežno uporabljajo v spletnem okolju.

[3] Namesto spletna digitalna potrdila se pogosto uporablja angleški izraz WEB digitalna potrdila.

Overitelj SIMoD-CA-Restricted izdaja naslednja neupravljana, spletna (WEB) oziroma digitalna potrdila tipa B:

Neupravljana, tip B, spletna, WEB digitalna potrdila				
Imetniki	Namen uporabe	Stopnja zaupanja v potrdilo	Identifikacijska oznaka politike	Identifikacija po ETSI TS 101 456
Fizične osebe	Digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.3.1, 0.4.0.1456.1.1	QCP public + SSCD
		SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.1.3.1, 0.4.0.1456.1.2	QCP public
		NIZKA	1.3.6.1.4.1.22295.10.1.2.2.1.3.1	
Funkcijske ali organizacijske vloge	Digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.2.3.1, 0.4.0.1456.1.1	QCP public + SSCD
		NIZKA	1.3.6.1.4.1.22295.10.1.2.2.2.3.1	
Organizacijske enote MO, institucije, ki opravljajo naloge povezane z obrambo in vojaške dolžnosti	Digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.3.3.1, 0.4.0.1456.1.1	QCP public + SSCD
		NIZKA	1.3.6.1.4.1.22295.10.1.2.2.3.3.1	
Strežniki, druga strojna in programska oprema.	Digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.4.3.1, 0.4.0.1456.1.1	QCP public + SSCD
		SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.4.3.1, 0.4.0.1456.1.2	QCP public
		NIZKA	1.3.6.1.4.1.22295.10.1.2.2.4.3.1	

Overitelj SIMoD-CA-Restricted izdaja digitalna potrdila za izdajatelje varnih časovnih žigov:

Namen uporabe	Stopnja zaupanja	Identifikacijska oznaka politike
Digitalno potrdilo izdajatelja varnih časovnih žigov	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.5.4.1

1.3. Udeleženci infrastrukture javnih ključev

1.3.1. Overitelj SIMoD-CA-Restricted

Overitelj SIMoD-CA-Restricted je podrejeni overitelj korenskega overitelja SIMoD-CA-Root in izdaja digitalna potrdila za potrebe uporabnikov in aplikacij v omrežju KIS MO in SV, klasificiranem za prenos podatkov stopnje tajnosti INTERNO.

Overitelj SIMoD-CA-Restricted sestavlja strojna in programska oprema ter operativno osebje, ki izvaja predpisane postopke in ukrepe za varno in zanesljivo delovanje overitelja SIMoD-CA-Restricted.

1.3.1.1. Svet za upravljanje z infrastrukturo javnih ključev na MO

Svet za upravljanje z infrastrukturo javnih ključev na MO zastopa overitelja SIMoD-CA-Restricted in ima v zvezi s tem naslednje obveznosti:

- nadzira izdelavo, vodi postopek potrditve, ocenjuje predlagane spremembe, predlaga uveljavitve sprememb in načrtuje postopek uveljavitve sprememb Pravil delovanja overitelja SIMoD-CA-Restricted, javnega in zaupnega dela,

- ocenjuje in potrjuje skladnost Pravil delovanja overitelja SIMoD-CA-Restricted, javnega in zaupnega dela s Politiko SIMoD-PKI,
- sprejema Pravila delovanja overitelja SIMoD-CA-Restricted, javni in zaupni del,
- imenuje operativno osebje overitelja SIMoD-CA-Restricted,
- operativnemu osebju daje usmeritve za odpravljanje pomanjkljivosti, ugotovljene ob inšpekcijskem in drugih oblikah nadzora ter uveljavlja druge ukrepe, kot je npr. preklic overiteljevega potrdila in
- ocenjuje ustreznost politik 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 je za svoje delo odgovoren ministru.

1.3.1.2. Operativno osebje overitelja SIMoD-CA-Restricted

Operativno osebje overitelja SIMoD-CA-Restricted 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 overitelja SIMoD-CA-Restricted.

1.3.2. Prijavna služba

Prijavna služba sprejema zahtevke in preverja točnost podatkov naročnikov digitalnih potrdil. Naloge prijavne službe opravlja organizacijska enota MO, ki je 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 overitelja SIMoD-CA-Restricted 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.

Odgovorna oseba za digitalno potrdilo za institucije, ki opravljajo naloge povezane z obrambo, je predstojnik institucije.

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.

Odgovorna oseba za digitalno potrdilo za strežnike in drugo strojno ter programsko opremo je skrbnik strežnika, druge strojne ali programske opreme.

Odgovorna oseba za digitalno potrdilo za izdajatelje varnih časovnih žigov in druge ponudnike storitev overjanja je vodja notranje organizacijske enote MO, ki upravlja z izdajateljem varnega časovnega žiga ali drugim ponudnikom storitev overjanja.

Odgovorne osebe imajo glede digitalnega potrdila enake obveznosti kot fizične osebe.

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 digitalno potrdilo overitelja SIMoD-CA-Restricted in korenskega overitelja SIMoD-CA-Root.

Tretje osebe so:

- imetniki digitalnih potrdil overiteljev SIMoD-PKI,
- imetniki digitalnih potrdil overiteljev, ki so medsebojno priznani z SIMoD-PKI,
- podrejeni overitelji in
- subjekti, ki nimajo digitalnega potrdila overitelja SIMoD-PKI, a se zanašajo na digitalna potrdila, ki so jih izdali overitelji SIMoD-PKI.

1.3.5. Posredno odgovorni organi

Overitelj SIMoD-CA-Restricted deluje v skladu s predpisi MO za področje KIS MO in SV. Posredno odgovorni organi so tudi notranje organizacijske enote MO, pristojne za področje varovanja ter nadzora KIS MO in SV.

1.4. Namen uporabe digitalnih potrdil

Namen uporabe digitalnih potrdil overitelja SIMoD-CA-Restricted je določen z namenom uporabe pripadajočih ključev (poglavje 6.1.7 Namen uporabe ključev). Namen uporabe javnih in zasebnih ključev za določeno digitalno potrdilo overitelja SIMoD-CA-Restricted je povzet v spodnji tabeli:

Vrsta digitalnega potrdila	Namen uporabe zasebnega ključa	Namen uporabe javnega ključa oziroma digitalnega potrdila
digitalno potrdilo za preverjanje digitalnega podpisa	digitalno podpisovanje	preverjanje digitalnega podpisa
digitalno potrdilo za šifriranje	dešifriranje[4]	šifriranje[5]
digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje	digitalno podpisovanje in dešifriranje	preverjanje digitalnega podpisa in šifriranje
digitalno potrdilo izdajatelja varnih časovnih žigov	digitalno podpisovanje varnih časovnih žigov	preverjanje varnih časovnih žigov

Digitalna potrdila overitelja SIMoD-CA-Restricted se morajo uporabljati v skladu s Politiko SIMoD-PKI in Pravili delovanja overitelja SIMoD-CA-Restricted. Namenjena so izključno službeni uporabi v MO, v drugih institucijah pa je namen omejen na opravljanje nalog povezanih z obrambo države.

Digitalna potrdila overitelja SIMoD-CA-Restricted omogočajo implementacijo naslednjih 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 elektronskih podatkov,
- **preverjanje istovetnosti**, kot mehanizem za preverjanje identitete v elektronski obliki in
- **selektivno omejevanje dostopa**, v smislu, da so šifrirani podatki nerazumljivi ali nerazpoložljivi neavtoriziranim osebam.

Prepoznavanje oziroma preverjanje istovetnosti, celovitosti in nezanikanja se realizira z varnostnim mehanizmom digitalnega podpisa, zaupnost in selektivno omejevanje dostopa pa z mehanizmi izmenjave ključev kot podporo simetričnim šifrirnim algoritmom. Te osnovne

[4] Zasebni ključ se uporablja za dešifriranje dejanskih simetričnih šifrirnih ključev.

[5] Javni ključ se uporablja za šifriranje dejanskih simetričnih šifrirnih ključev.

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 digitalnega potrdila za preverjanje digitalnega 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.

Overitelj SIMoD-CA-Restricted izdaja digitalna potrdila naslednjih stopenj zaupanja:

		Stopnja zaupanja:		
		VISOKA	SREDNJA	NIZKA
		Identifikacija digitalnega potrdila po ETSI TS 101 456:		
		QCP public + SSCD[6]	QCP public[7]	
Pogoj, ki določa stopnjo zaupanja (izpolnjen DA/NE):	Ob prvi registraciji obvezno preverjanje identitete v prijavni službi	DA	DA	NE
	Obvezna uporaba sredstva za varno elektronsko podpisovanje	DA	NE	NE
	Zasebni ključ se hrani in je pod izključno kontrolo imetnika[8]	DA	DA	DA

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 overitelja SIMoD-CA-Restricted 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.

[6] Kvalificirano potrdilo z obvezno uporabo sredstva za varno elektronsko podpisovanje

[7] Kvalificirano potrdilo

[8] Za digitalna potrdila za šifriranje se šteje, da je pogoj »zasebni ključ je pod izključno kontrolo imetnika« izpolnjen tudi, če je zagotovljeno varnostno kopiranje zasebnega ključa za dešifriranje pri overitelju SIMoD-CA-Restricted ob pogojih iz Pravil delovanja SIMoD-CA-Restricted. Za digitalna potrdila za preverjanje digitalnega podpisa se za izpolnitev pogoja »zasebni ključ je pod izključno kontrolo imetnika« zasebni ključ ne sme varnostno kopirati pri nobenem subjektu, razen pri imetniku digitalnega potrdila.

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

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 [15] ZTP, npr. osebni podatki,
- upravljanje z varnostnimi parametri v KIS, npr. 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 digitalnih potrdil majhna.

1.4.2. Nedovoljena uporaba digitalnih potrdil

Ni relevantno.

1.5. Upravljanje s Pravili delovanja overitelja SIMoD-CA-Restricted

1.5.1. Organ, ki upravlja s tem dokumentom

Svet za upravljanje z infrastrukturo javnih ključev na MO nadzira izdelavo, vodi postopek potrditve in sprejema Pravila delovanja SIMoD-CA-Restricted, javni in zaupni del ter ocenjuje in potrjuje predlagane spremembe.

Operativno osebje overitelja SIMoD-CA-Restricted predlaga Svetu za upravljanje z infrastrukturo javnih ključev na MO spremembe Pravil delovanja SIMoD-CA-Restricted, javnega in zaupnega dela.

1.5.2. Kontaktna oseba

Naslov:	Republika Slovenija Ministrstvo za obrambo Sekretariat generalnega sekretarja Urad za informatiko in komunikacije Svet za upravljanje z infrastrukturo javnih ključev na MO Vojkova cesta 55, 1000 Ljubljana
Telefon:	01 230 5314
Fax:	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 skladnosti Pravil delovanja overitelja SIMoD-CA-Restricted s Politiko SIMoD-PKI

Skladnost Pravil delovanja overitelja SIMoD-CA-Restricted, javnega in zaupnega dela s Politiko SIMoD-PKI potrjuje Svet za upravljanje z infrastrukturo javnih ključev na MO.

1.5.4. Postopek odobritve Pravil delovanja overitelja SIMoD-CA-Restricted

V postopku odobritve Pravil delovanja overitelja SIMoD-CA-Restricted, javnega in zaupnega dela, se preveri:

- skladnost Pravil delovanja overitelja SIMoD-CA-Restricted, javnega in zaupnega dela, z zahtevami Politike SIMoD-PKI in
- skladnost infrastrukture in postopkov overitelja SIMoD-CA-Restricted z določili Politike SIMoD-PKI in Pravili delovanja overitelja SIMoD-CA-Restricted, javnega in zaupnega dela.

Izdaja digitalnega potrdila overitelju SIMoD-CA-Restricted s strani overitelja SIMoD-CA-Root 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).
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 4043	Priporočilo, ki definira posebno polje *Permanent Identifier* v razširitvi *subjectAltName* v digitalnih potrdilih.
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)
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

Overitelj SIMoD-CA-Restricted v imenikih objavlja naslednje podatke:

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

Imeniki so dostopni po protokolu LDAP.

V primarnem imeniku so objavljeni naslednji podatki:

- digitalna potrdila imetnikov in
- registri preklicanih potrdil (ang. Certificate Revocation List, CRL).

Zrcalni imenik vsebuje kopijo podatkov iz primarnega imenika. Zrcalni imenik ima dodatni naslov (ang. alias) imenik.simod-pki.mors.si.

Digitalna potrdila in združeni register preklicanih potrdil se kopirajo tudi v druge imenike.

Na primarnem spletnem strežniku v internem KIS MO in SV na spletni strani http://www.simod-pki.mors.si so objavljeni naslednji podatki o overitelju SIMoD-CA-Restricted:

- digitalno potrdilo overitelja SIMoD-CA-Restricted,
- združeni register preklicanih potrdil overitelja SIMoD-CA-Restricted,
- Javna pravila SIMoD-CA-Restricted in
- druge javne objave.

Zrcalni spletni strežnik http://www.simod-pki.mors.si v javnem internet omrežju vsebuje kopijo podatkov iz primarnega spletnega strežnika.

2.2. Objave informacij o digitalnih potrdilih

Digitalna potrdila so objavljena v primarnem in zrcalnem imeniku v spodaj navedenih poddrevesih, glede na tip imetnika digitalnega potrdila:

Poddrevo v imeniku:	Digitalno potrdilo glede na tip imetnika:
ou=ljudje,o=mors,c=si	fizične osebe – zaposleni v MO in zaposleni v institucijah, ki opravljajo naloge povezane z obrambo
ou=organizacije,o=mors,c=si	• organizacijske enote MO, • institucije, ki opravljajo naloge povezane z obrambo in • vojaške dolžnosti v SV
ou=vloge,o=mors,c=si	funkcijske in organizacijske vloge, povezane z opravljanjem vojaških nalog ali drugih nalog s področja obrambe,
ou=naprave,o=mors,c=si	• strežniki in druga strojna ter programska oprema • izdajatelji varnih časovnih žigov in drugi ponudniki storitev overjanja
ou=simod-pki,o=mors,c=si	overitelji digitalnih potrdil

Registri preklicanih potrdil so v imeniku objavljeni v naslednjih vozliščih v atributu certificateRevocationList:

- deljeni registri so v cn=CRL*n*, cn=simod-ca-restricted,ou=simod-pki,o=mors,c=si, kjer je *n* 1, 2,...,
- združeni register je v cn=simod-ca-restricted,ou=simod-pki,o=mors,c=si.

Združeni register preklicanih potrdil je na primarnem in zrcalnem spletnem strežniku dostopen tudi po protokolu HTTP na naslovu http://www.simod-pki/mors.si/crl/simod-ca-restricted.crl.

2.3. Čas in pogostost objav

Pogostost objav registrov preklicanih potrdil je opisana v poglavju 4.9.7 Pogostost objav registrov preklicanih potrdil.

2.4. Dostop do podatkov v imeniku in na spletni strani

Dostop do primarnega imenika je dovoljen samo ustreznemu overitelju in upravljavcem imenika.

Dostop do digitalnih potrdil in registrov preklicanih potrdil v zrcalnem imeniku je omogočen vsem uporabnikom in tretjim osebam v internem KIS MO in SV.

Dostop do podatkov na primarnem spletnem strežniku je omogočen vsem uporabnikom in tretjim osebam v internem KIS MO in SV.

Dostop do podatkov na zrcalnem spletnem strežniku je omogočen vsem uporabnikom in tretjim osebam v zunanjih omrežjih.

Dokument Pravila delovanja overitelja SIMoD-CA-Restricted, zaupni del, je stopnje tajnosti INTERNO in ni javno objavljen.

Overitelj SIMoD-CA-Restricted zagotovi dokument Pravila delovanja overitelja SIMoD-CA-Restricted, zaupni del, in dopolnjujoča navodila in postopkovnike, če je to potrebno zaradi nadzora, akreditacije ali medsebojnega povezovanja, ob pogojih, ki jih določa [15] ZTP.

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 (ang. Distinguished Name, DN) v skladu z [9] 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 digitalnega potrdila *subjectAltName* v skladu z [9] RFC 3280 ali [10] RFC 4043. Tip alternativnega imena je običajno:

- *rfc822Name*; vrednost polja je naslov elektronske pošte v skladu z [9] RFC 3280 ali
- *otherName*; vrednost polja je enolična oznaka *Permanent Identifier* v skladu z [10] RFC 4043. Enolično oznako *Permanent Identifier* sestavljata dva dela:
    - vrsta enolične oznake (*assigner*) - OID vrste oznake in
    - vrednost oznake (*identifierValue*) - enolično število v okviru vrste oznake ali
- *DNS Name*; vrednost je domensko ime strežnika ali naprave.

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 SIMoD-CA-Restricted 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 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 (številko) dodano splošnemu imenu.

3.1.6. Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk

Uporaba zaščitenih znamk v imenih je dovoljena samo nosilcem zaščitenih znamk. Overitelj SIMoD-CA-Restricted ne sme 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 overitelj SIMoD-CA-Restricted 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

Overitelj SIMoD-CA-Restricted preverja lastništvo zasebnega ključa, ki odgovarja javnemu ključu, vsebovanem v zahtevku. V ta namen morajo prosilci za izdajo digitalnega potrdila posredovati overitelju javni ključ:

- kot [12] PKCS#10 zahtevek ali
- po PKIX-CMP protokolu v skladu z [11] RFC 4210.

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 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 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 SIMoD-CA-Root.

3.3. Preverjanje imetnikov za ponovno izdajo digitalnega potrdila

3.3.1. Preverjanje istovetnosti pri rutinski ponovni izdaji digitalnih potrdil

Ob rutinski ponovni izdaji upravljanih digitalnih potrdil[9], ki so bila izdana po protokolu PKIX-CMP, imetnik izkaže svojo istovetnost s posedovanjem še veljavnega zasebnega ključa.

Rutinska ponovna izdaja neupravljanih digitalnih potrdil[10] (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.

3.4. Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila

Oseba, ki želi preklicati digitalno potrdilo, se lahko identificira:

- z digitalno podpisanim zahtevkom za preklic digitalnega potrdila,
- z oddajo pisnega zahtevka za preklic digitalnega potrdila, pri čemer je postopek preverjanja istovetnosti enak kot pri prvi registraciji v skladu s poglavjem 3.2. Preverjanje istovetnosti imetnikov ob prvi registraciji ali
- s skrivnim geslom, ki ga je imetnik izbral ob oddaji zahtevka za izdajo digitalnega potrdila.

[9] Imenovana tudi digitalna potrdila tipa A ali *Entrust ID.*

[10] Imenovana tudi digitalna potrdila tipa B, spletna ali WEB potrdila.

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 overitelja SIMoD-CA-Restricted.

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 SIMoD-CA-Restricted 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 SIMoD-CA-Restricted. Obvestilo o zavrnitvi pošlje operativno osebje overitelja SIMoD-CA-Restricted 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 overitelja SIMoD-CA-Restricted 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

Izdaja digitalnega potrdila je neločljivo povezana s prevzemom digitalnega potrdila. Bodoči imetnik praviloma prevzame digitalno potrdilo z aktivacijskimi podatki: referenčno številko in avtorizacijsko kodo.

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

Tehnični postopek prevzema je odvisen od tipa potrdila in uporabniške programske opreme.

Prevzem upravljanih digitalnih potrdil[11] se izvaja s programsko opremo Entrust Entelligence Security Provider. Navodila za namestitev in uporabo programske opreme se nahajajo na spletni strani http://www.simod-pki.mors.si.

Prevzem neupravljanih digitalnih potrdil[12] se izvaja preko spletnega vmesnika. Spletni naslov vmesnika in navodila za prevzem so dostopna na spletnem naslovu http://www.simod-pki.mors.si.

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 in polno pot digitalnih podpisov do korenskega overitelja SIMoD-CA-Root. 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 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 2.1. Objave dokumentov in imenik. Overitelj SIMoD-CA-Restricted praviloma ne objavlja digitalnih potrdil z javnimi ključi za preverjanje 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.

---

[11] Imenovana tudi digitalna potrdila tipa A ali *Entrust ID*.

[12] Imenovana tudi digitalna potrdila tipa B, spletna ali WEB potrdila.

4.5.1. Uporaba ključev in digitalnih potrdil imetnikov

4.5.1.1. Zasebni ključi in digitalna potrdila overiteljev

Overitelj SIMoD-CA-Restricted uporablja svoje zasebne ključe samo za podpisovanje digitalnih potrdil imetnikom, ki so določeni v poglavju 1.3.3 Imetniki digitalnih potrdil in svojemu operativnemu osebju ter za podpisovanje registrov preklicanih potrdil.

Operativno osebje overitelja SIMoD-CA-Restricted uporablja digitalna potrdila in pripadajoče ključe izključno za izvajanje nalog upravljanja z infrastrukturo overitelja SIMoD-CA-Restricted. 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 za izvajanje nalog prijavne službe ne potrebuje namenskih digitalnih potrdil.

4.5.1.3. Uporabniški zasebni ključi in digitalna potrdila

Imetnik digitalnega potrdila overitelja SIMoD-CA-Restricted je dolžan:

- uporabljati ključe in digitalna potrdila samo za namene, ki so definirani v Politiki SIMoD-PKI in Pravilih delovanja overitelja SIMoD-CA-Restricted,
- 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 SIMoD-CA-Restricted 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 oziroma ponovna izdaja digitalnega potrdila brez spremembe javnega ključa ni dovoljena.

4.7. Ponovna izdaja digitalnih potrdil[13]

4.7.1. Razlogi za ponovno izdajo digitalnega potrdila

Ponovna izdaja digitalnega potrdila 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 ali preteku veljavnosti oddajo uporabniki enak zahtevek, kot za prvo pridobitev digitalnega potrdila. Zahtevek 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.

Ponovna izdaja digitalnih potrdil pred pretekom veljavnosti se za upravljana digitalna potrdila[14], izdana po protokolu PKIX-CMP, izvede samodejno ob prvi uporabi digitalnega potrdila ob dostopu 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. Postopek imenujemo tudi rutinska ponovna izdaja digitalnih potrdil.

Ponovna izdaja digitalnih potrdil pred pretekom veljavnosti se za neupravljana digitalna potrdila[15] po protokolu PKCS#10 izvede na osnovi ustreznega elektronskega zahtevka, ki je podpisan z veljavnim digitalnim potrdilom.

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

Ponovna izdaja digitalnega potrdila overitelja SIMoD-CA-Restricted in izdajateljev varnih časovnih žigov mora biti pod kontrolo operativnega osebja.

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 upravljanega 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.

---

[13] 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.

[14] Imenovana tudi digitalna potrdila tipa A ali *Entrust ID*.

[15] Imenovana tudi digitalna potrdila tipa B, spletna ali WEB 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 SIMoD-CA-Restricted,
- sprememba podatkov, ki so vsebovani v digitalnem potrdilu ali
- razlogi, navedeni v poglavju 4.11. Predčasna prekinitev veljavnosti digitalnih potrdil.

4.9.1.2. Okoliščine preklica digitalnega potrdila korenskega overitelja

Ni relevantno.

4.9.1.3. Okoliščine preklica digitalnega potrdila o priznavanju drugega overitelja

Ni relevantno.

4.9.1.4. Okoliščine preklica digitalnega potrdila overitelja SIMoD-CA-Restricted

Razlogi za preklic digitalnega potrdila overitelja SIMoD-CA-Restricted 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 SIMoD-CA-Root ali
- druge okoliščine, ki lahko ogrozijo zaupanje v digitalno potrdilo overitelja SIMoD-CA-Restricted.

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 overitelja SIMoD-CA-Restricted, 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

Ni relevantno.

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

Ni relevantno.

4.9.2.4. Kdo lahko zahteva preklic digitalnega potrdila overitelja SIMoD-CA-Restricted

Preklic digitalnega potrdila overitelja SIMoD-CA-Restricted 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 z veljavnim digitalnim potrdilom elektronsko podpisan zahtevek po elektronski pošti na kontaktni naslov overitelja (poglavje 1.5.2 Kontaktna oseba),
- osebno, z oddajo zahtevka za preklic v prijavni službi ali
- po telefonu na dežurno številko za preklic, pri tem se mora imetnik identificirati s skrivnim geslom, ki ga je izbral ob oddaji zahtevka za pridobitev digitalnega potrdila.

V primeru, ko je prejemnik zahtevka za preklic prijavna služba, ta po uspešnem postopku preverjanja istovetnosti vlagatelja pošlje zahtevek operativnemu osebju overitelja SIMoD-CA-Restricted.

V primeru telefonsko posredovanega zahtevka dežurna oseba posreduje zahtevek za preklic operativnemu osebju overitelja SIMoD-CA-Restricted.

Preklic izvrši operativno osebje overitelja SIMoD-CA-Restricted.

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 SIMoD-CA-Restricted objaviti preklicano digitalno potrdilo v registru preklicanih potrdil.

Operativno osebje overitelja SIMoD-CA-Restricted 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.

4.9.3.2. Postopki preklica digitalnega potrdila korenskega overitelja

Ni relevantno.

4.9.3.3. Postopki preklica digitalnega potrdila o priznavanju drugega overitelja

Ni relevantno.

4.9.3.4. Postopki preklica digitalnega potrdila overitelja SIMoD-CA-Restricted

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

Overitelj SIMoD-CA-Restricted ob preklicu svojega digitalnega potrdila izvede naslednje postopke:

- prekliče vsa digitalna potrdila,
- zagotavlja razpoložljivost registrov preklicanih potrdil vsaj še devetdeset (90) dni od preklica svojega digitalnega potrdila,
- ustvari nove ključe,
- izda imetnikom nova digitalna potrdila in
- objavi obvestilo o preklicu svojega potrdila 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 SIMoD-CA-Restricted 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 SIMoD-CA-Restricted.

Operativno osebje SIMoD-CA-Restricted 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

Ni relevantno.

4.9.5.3. Čas za preklic digitalnega potrdila o priznavanju drugega overitelja

Ni relevantno.

4.9.5.4. Čas za preklic digitalnega potrdila overitelja SIMoD-CA-Restricted

Korenski overitelj SIMoD-CA-Root prekliče digitalna potrdila overitelja SIMoD-CA-Restricted 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 morajo 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

Veljavnost registrov preklicanih potrdil, ki jih izdaja overitelj SIMoD-CA-Restricted, je 25 ur.

Overitelj SIMoD-CA-Restricted objavi nov register preklicanih potrdil pred potekom veljavnosti starega oziroma takoj po preklicu digitalnega potrdila.

4.9.8. Dovoljene zakasnitve pri objavi registrov preklicanih potrdil

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

Overitelj SIMoD-CA-Restricted izda nov register preklicanih potrdil vsaj 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 objavljanja 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, strojne ali programske opreme in
- prenehanje potrebe po storitvi izdajanja varnih časovnih žigov ali drugi storitvi overjanja.

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 poglavjem 6.2.4 Varnostno kopiranje zasebnih ključev .

4.12.1.Povrnitev zgodovine ključev za dešifriranje

Overitelj SIMoD-CA-Restricted omogoča povrnitev zgodovine ključev za dešifriranje za naslednja upravljana digitalna potrdila, izdana po protokolu PKIX-CMP protokolu:

Imetniki	Namen uporabe	Stopnja zaupanja	Identifikacijske oznake politik
Fizične osebe	Digitalno potrdilo za šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.2.1, 0.4.0.1456.1.1
Funkcijske ali organizacijske vloge	Digitalno potrdilo za šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.2.2.1, 0.4.0.1456.1.1
	Digitalno potrdilo za šifriranje	SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.2.2.1, 0.4.0.1456.1.2
	Digitalno potrdilo za šifriranje	NIZKA	1.3.6.1.4.1.22295.10.1.2.2.2.2.1
Organizacijske enote MO, institucije, ki opravljajo naloge povezane z obrambo, vojaške dolžnosti	Digitalno potrdilo za šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.3.2.1, 0.4.0.1456.1.1

Povrnitev zgodovine ključev za dešifriranje se izvede:

- na osnovi zahtevka za povrnitev zgodovine ključev – imetnik vloži zahtevek, če je pred pretekom veljavnosti digitalnega potrdila izgubil geslo za dostop do zasebnih ključev, izgubil ali poškodoval pametno kartico ali drug nosilec zasebnih ključev in
- praviloma ob ponovni izdaji digitalnega potrdila.

4.12.2.Odkrivanje kopije ključev za dešifriranje

Overitelj SIMoD-CA-Restricted omogoča odkrivanje kopije ključev za dešifriranje za digitalna potrdila, ki so navedena v poglavju 4.12.1 Povrnitev zgodovine 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 SIMoD-CA-Restricted 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

Prostori, kjer se izvajajo dejavnosti overitelja SIMoD-CA-Restricted, izpolnjujejo pogoje za namestitev komunikacijske in informacijske opreme ter arhivskih medijev skladno s predpisi, ki urejajo področje tajnih podatkov.

Strežnik overitelja SIMoD-CA-Restricted je v prostorih, ki so varnostno območje I. 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 v prostore je video nadzorovan. O vstopih in izstopih v prostore se vodi evidenca.

Preden operativno osebje zapusti prostore overitelja SIMoD-CA-Restricted, mora preveriti:

- da programska in strojna oprema pravilno in varno deluje (overitelj SIMoD-CA-Restricted 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 overitelja SIMoD-CA-Restricted 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 overitelja SIMoD-CA-Restricted so na lokaciji, kjer je verjetnost poplave zelo majhna.

5.1.5. Zaščita pred ognjem

Prostori s komunikacijsko in informacijsko opremo overitelja SIMoD-CA-Restricted so opremljeni z detektorji temperature in dima.

5.1.6. Shranjevanje medijev

Mediji z varnostnimi kopijami in arhiv podatkov so hranjeni v protivlomni omari.

Mediji, hranjeni na oddaljeni lokaciji, so v prostorih, ki zagotavljajo enake pogoje, kot so v prostorih overitelja SIMoD-CA-Restricted.

5.1.7. Odstranjevanje odpadkov

Dokumenti v papirni obliki se uničujejo z rezalnikom v varovanih prostorih overitelja SIMoD-CA-Restricted. Mediji, na katerih se hranijo tajni podatki, se pred odstranitvijo iz prostorov overitelja SIMoD-CA-Restricted varno izbrišejo ali pa se medije fizično uniči.

V primeru, da medija ni mogoče varno izbrisati ali uničiti v prostorih overitelja SIMoD-CA-Restricted, se medij dostavi v uničevalno mesto po postopku, predpisanem za stopnjo tajnosti podatkov, ki jih medij hrani.

5.1.8. Hranjenje na oddaljeni lokaciji

Overitelj SIMoD-CA-Restricted uporablja 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 overitelja SIMoD-CA-Restricted.

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 overitelja SIMoD-CA-Restricted

5.2.1.1. Operativno osebje overitelja SIMoD-CA-Restricted

Naloge upravljanja z infrastrukturo overitelja SIMoD-CA-Restricted so porazdeljene med operativno osebje tako, da je zagotovljena ločitev med zaključenimi vsebinskimi področji upravljanja. Operativno osebje overitelja SIMoD-CA-Restricted je glede na vsebinska področja upravljanja razdeljeno na zaključene organizacijske skupine:

- upravljanje z digitalnimi potrdili,
- upravljanje s programsko in strojno opremo overitelja SIMoD-CA-Restricted ter
- varovanje in nadzor komunikacijskega sistema.

Operativni osebi overitelja SIMoD-CA-Restricted je dovoljeno opravljanje nalog samo znotraj ene zaključene organizacijske skupine.

V organizacijski skupini za upravljanje z digitalnimi potrdili overitelja SIMoD-CA-Restricted so:

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

V organizacijski skupini za upravljanje s programsko in strojno opremo overitelja SIMoD-CA-Restricted so:

- prvi administrator overitelja SIMoD-CA-Restricted in
- administratorji overitelja SIMoD-CA-Restricted.

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 del zaupnega dela Pravil delovanja overitelja SIMoD-CA-Restricted.

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 in preklic digitalnega potrdila,
- preverjanje istovetnosti naročnikov oziroma imetnikov in točnosti podatkov v zahtevkih za izdajo in preklic digitalnega potrdila,
- hranjenje dokazil o postopkih preverjanja istovetnosti,
- posredovanje zahtevkov operativnemu osebju overitelja SIMoD-CA-Restricted, ki upravlja z digitalnimi potrdili in
- obveščanje operativnega osebje overitelja SIMoD-CA-Restricted, ki upravlja z digitalnimi potrdili, o spremembi podatkov imetnika digitalnega potrdila (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 overitelja SIMoD-CA-Restricted 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 overitelja SIMoD-CA-Restricted.

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 overitelja SIMoD-CA-Restricted.

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 SIMoD-CA-Restricted:

- generiranje kriptografskih ključev overitelja SIMoD-CA-Restricted,
- preklic overiteljevega potrdila,
- spreminjanje gesel aplikacije za delo z overiteljem SIMoD-CA-Restricted,
- 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 oseb iz skupine za upravljanje z digitalnimi potrdili s funkcijo prvega ali drugega varnostnega inženirja:

- nastavitev življenjske dobe digitalnih potrdil,
- 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 overitelja SIMoD-CA-Restricted izkaže svojo istovetnost:

- pri vstopu v varovane prostore s komunikacijsko in informacijsko opremo overitelja SIMoD-CA-Restricted z identifikacijsko kartico in vstopno kodo,
- za delo na overiteljevem informacijskem 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 overitelja

5.3.1. Kvalifikacije, izkušnje in varnostno preverjanje

Operativno osebje overitelja SIMoD-CA-Restricted:

- je ustrezno usposobljeno in o tem imeti dokazila,

- ima za opravljanje nalog pri overitelju SIMoD-CA-Restricted imenovanje Sveta za upravljanje z infrastrukturo javnih ključev na MO,
- ne sme opravljati drugih nalog, ki bi bile v nasprotju z opravljanjem nalog pri overitelju SIMoD-CA-Restricted,
- ni bilo 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 [15] ZTP.

5.3.3. Usposabljanje osebja overitelja

Operativno osebje overitelja SIMoD-CA-Restricted se redno usposablja na 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 se usposablja za identifikacijo naročnikov in preverjanje pravilnosti podatkov v zahtevkih.

Osebje za pomoč uporabnikom in nastavitev uporabniškega okolja se usposablja na področjih:

- osnove infrastrukture javnih ključev in
- namestitev in delo z namensko 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 overitelja SIMoD-CA-Restricted, 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 osebi odvzeme pooblastila ter zahteva 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 [15] ZTP oziroma implementacijo pravil na lokaciji overitelja SIMoD-CA-Restricted.

5.3.8. Dokumentacija za osebje overitelja

Operativnemu osebju overitelja SIMoD-CA-Restricted, skupini za pomoč uporabnikom in skupini za nastavitev uporabniškega okolja so na voljo interni priročniki, originalna dokumentacija programske in strojne opreme ter priročniki šolanj.

5.4. Postopki varnostnih pregledov sistema

5.4.1. Vrste beleženih dogodkov

Overitelj SIMoD-CA-Restricted beleži dogodke:

- na operacijskem sistemu, programski in strojni opremi overitelja SIMoD-CA-Restricted,

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

Overitelj SIMoD-CA-Restricted zbira in beleži v elektronski ali pisni obliki tudi podatke, ki vplivajo na varnost, niso pa del komunikacijsko informacijskega sistema overitelja SIMoD-CA-Restricted:

- dogodke v zvezi s fizičnim dostopom do overitelja SIMoD-CA-Restricted ter fizično lokacijo,
- kadrovske spremembe operativnega osebja overitelja SIMoD-CA-Restricted,
- 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 SIMoD-CA-Restricted.

5.4.2. Pogostost pregleda dnevnikov beleženih dogodkov

Operativno osebje overitelja SIMoD-CA-Restricted pregleduje dnevnike beleženih dogodkov ob vsakem opozorilu iz nadzornih sistemov. Pregled vključuje:

- preverjanje integritete dnevnikov,
- pregled zapisov v dnevniku in
- analizo in poročanje o relevantnih dogodkih - razreševanje problemov.

Operativno osebje overitelja SIMoD-CA-Restricted izvaja redne preglede beleženih dogodkov 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 več kot 25 km oddaljena od prostora overitelja SIMoD-CA-Restricted.

Dostop do dnevnikov beleženih dogodkov je dovoljen samo pooblaščenim osebam:

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

Za dnevnike na operacijskem sistemu so uporabljene zaščite operacijskega sistema. Dnevniki programske opreme za upravljanje s ključi in digitalnimi potrdili so zaščiteni s tehnologijo kriptografije javnih ključev.

5.4.5. Varnostne kopije dnevnikov beleženih dogodkov

Varnostne kopije dnevnikov beleženih dogodkov v elektronski obliki se izdeluje v okviru 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-CA-Restricted 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

Overitelj SIMoD-CA-Restricted hrani naslednje podatke:

- dnevnike beleženih dogodkov iz poglavja 5.4.1 Vrste beleženih dogodkov,
- zahtevke imetnikov digitalnih potrdil,
- dokumentacijo o izvedbi postopka izdaje digitalnih potrdil,
- korespondenco in pogodbe imetnikov digitalnih potrdil z overiteljem SIMoD-CA-Restricted,
- digitalna potrdila in liste preklicanih potrdil,
- verzije pravil delovanja overitelja SIMoD-CA-Restricted, tako javnih kot zaupnih delov in
- zasebne dešifrirne ključe v skladu s poglavjem 6.2.4 Varnostno kopiranje zasebnih ključev.

5.5.2. Obdobje hranjenja arhiva

Overitelj SIMoD-CA-Restricted hrani dnevnike beleženih dogodkov najmanj pet (5) let od posameznega dogodka ali dejanja.

Overitelj SIMoD-CA-Restricted hrani zahtevke imetnikov, korespondenco in pogodbe imetnikov z overiteljem SIMoD-CA-Restricted 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 hranjeno zahtevek, 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 za izdajo digitalnih potrdil in spremljajoči dokumenti, dokumentacija o izvedbi postopka izdaje digitalnih potrdil, korespondenca in pogodbe z imetniki digitalnih potrdil, verzije pravil delovanja overitelja SIMoD-CA-Restricted in dnevniki beleženih dogodkov v pisni obliki) se hranijo in arhivirajo v skladu s predpisi za delo z dokumentarnim gradivom.

Arhivirani podatki, ki se beležijo v okviru informacijskega sistema (avtomatsko generirani dnevniki beleženih dogodkov, digitalna potrdila in liste preklicanih potrdil) se nahajajo v vsaj dveh izvodih na ločenih lokacijah. Enkrat letno se preverja integriteta medijev z arhiviranimi podatki. Arhiv, ki se hrani na drugi lokaciji, je zaščiten z ekvivalentnimi varnostnimi mehanizmi, kot so implementirani v prostorih overitelja SIMoD-CA-Restricted.

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 overiteljem SIMoD-CA-Restricted, pravila delovanja overitelja SIMoD-CA-Restricted 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 overitelja SIMoD-CA-Restricted (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 možen samo

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

5.6. Zamenjava ključev overitelja SIMoD-CA-Restricted

Veljavnost digitalnega potrdila overitelja SIMoD-CA-Restricted 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 SIMoD-CA-Restricted se vedno uporablja krajše obdobje kot je veljavnost pripadajočega overiteljevega potrdila.

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

Obnova digitalnega potrdila overitelja SIMoD-CA-Restricted se izvede po predpisanem in nadzorovanem postopku. Posamezne korake postopka izvaja operativno osebje korenskega overitelja in overitelja SIMoD-CA-Restricted. 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

Postopki v primeru okvar in zlorab so del okrevalnega načrta, ki je predpisan v zaupnem delu Pravil delovanja overitelja SIMoD-CA-Restricted.

5.7.2. Uničenje programske, strojne opreme ali podatkov overitelja

V primeru okvare strojne ali programske opreme oziroma podatkov, pri kateri zasebni ključ overitelja SIMoD-CA-Restricted ni bil uničen, bodo storitve overitelja SIMoD-CA-Restricted vzpostavljene nazaj v najkrajšem možnem času. Overitelj SIMoD-CA-Restricted bo v najkrajšem možnem času vzpostavil 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 bo overitelj SIMoD-CA-Restricted objavil preklic svojega potrdila in ukrepal v skladu s poglavjem 4.9.3.4 Postopki preklica digitalnega potrdila overitelja SIMoD-CA-Restricted.

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 4.9.3.4 Postopki preklica digitalnega potrdila overitelja SIMoD-CA-Restricted.

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 SIMoD-CA-Restricted

Postopki ob zlorabi zasebnega ključa overitelja SIMoD-CA-Restricted so predpisani v poglavju 4.9.3.4 Postopki preklica digitalnega potrdila overitelja SIMoD-CA-Restricted.

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 ali strojne opreme ali ogroženo celovitost podatkov overitelja SIMoD-CA-Restricted oziroma uničenje in poškodovanje varovanih prostorov overitelja SIMoD-CA-Restricted, so del okrevalnega načrta, ki je predpisan v zaupnem delu Pravil delovanja overitelja SIMoD-CA-Restricted.

5.8. Prenehanje delovanja overitelja SIMoD-CA-Restricted

Vzroki za prenehanje delovanja overitelja SIMoD-CA-Restricted so podani v poglavju 4.9.1.4 Okoliščine preklica digitalnega potrdila overitelja SIMoD-CA-Restricted. 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 SIMoD-CA-Restricted 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 SIMoD-CA-Restricted obvestil:

- operativno osebje,
- vse imetnike digitalnih potrdil oziroma odgovorne osebe in
- ministrstvo, pristojno za registracijo overiteljev v Republiki Sloveniji.

Overitelj SIMoD-CA-Restricted bo po prenehanju delovanja izvedel postopke predpisane v poglavju 4.9.3.4 Postopki preklica digitalnega potrdila overitelja SIMoD-CA-Restricted.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev para ključev

6.1.1. Generiranje para ključev

Generiranje ključev overitelja SIMoD-CA-Restricted izvede operativno osebje, prisotne so zaupanja vredne priče. Izvedba postopka je dokumentirana v zapisniku. Generiranje para ključev je izvedeno znotraj varnostnega kriptografskega modula.

Par ključev izdajateljev časovnih žigov se vedno generira pri izdajatelju časovnih žigov v varnostnem kriptografskem modulu in pod njegovo kontrolo.

Ključi imetnikov upravljanih digitalnih potrdil[16] se generirajo:

Ključ:	Stopnja zaupanja:	Kje se ključ generira:	Kje se ključ hrani:	Kje se hrani kopija ključa:
zasebni ključ za dešifriranje	VISOKA	pri overitelju	na uporabnikovi pametni kartici	šifrirana v bazi overitelja
javni ključ za šifriranje	VISOKA	pri overitelju	na uporabnikovi pametni kartici	v vsaki kopiji digitalnega potrdila za šifriranje
zasebni ključ za digitalni podpis	VISOKA	na uporabnikovi pametni kartici	na uporabnikovi pametni kartici	ne obstaja
javni ključ za preverjanje digitalnega podpisa	VISOKA	na uporabnikovi pametni kartici	na uporabnikovi pametni kartici	v vsaki kopiji digitalnega potrdila za preverjanje digitalnega podpisa
zasebni ključ za dešifriranje	SREDNJA	pri overitelju	na uporabnikovi pametni kartici ali v programski opremi pri uporabniku	šifrirana v bazi overitelja
javni ključ za šifriranje	SREDNJA	pri overitelju	na uporabnikovi pametni kartici ali v programski opremi pri uporabniku	v vsaki kopiji digitalnega potrdila za šifriranje
zasebni ključ za digitalni podpis	SREDNJA	na uporabnikovi pametni kartici ali v programski opremi pri uporabniku	na uporabnikovi pametni kartici ali v programski opremi pri uporabniku	ne obstaja
javni ključ za preverjanje digitalnega podpisa	SREDNJA	na uporabnikovi pametni kartici ali v programski opremi pri uporabniku	na uporabnikovi pametni kartici ali v programski opremi pri uporabniku	v vsaki kopiji digitalnega potrdila za preverjanje digitalnega podpisa
zasebni ključ za dešifriranje	NIZKA	pri overitelju	v programski opremi pri uporabniku	šifrirana v bazi overitelja
javni ključ za šifriranje	NIZKA	pri overitelju	v programski opremi pri uporabniku	v vsaki kopiji digitalnega potrdila za šifriranje
zasebni ključ za digitalni podpis	NIZKA	v programski opremi pri uporabniku	v programski opremi pri uporabniku	ne obstaja
javni ključ za preverjanje digitalnega podpisa	NIZKA	v programski opremi pri uporabniku	v programski opremi pri uporabniku	v vsaki kopiji digitalnega potrdila za preverjanje digitalnega podpisa

[16] Digitalna potrdila tipa A oziroma *Entrust ID*

Ključi imetnikov neupravljanih[17] digitalnih potrdil se generirajo:

Ključ:	Stopnja zaupanja:	Kje se ključ generira:	Kje se ključ hrani:	Kje se hrani kopija ključa:
zasebni ključ za digitalni podpis in dešifriranje	VISOKA[18]	na uporabnikovi pametni kartici, generiranje izvede operativno osebje overitelja	na uporabnikovi pametni kartici	ne obstaja
javni ključ za preverjanje digitalnega podpisa in šifriranje	VISOKA[18]	na uporabnikovi pametni kartici, generiranje izvede operativno osebje overitelja	na uporabnikovi pametni kartici	v vsaki kopiji digitalnega potrdila za preverjanje digitalnega podpisa in šifriranje
zasebni ključ za digitalni podpis in dešifriranje	SREDNJA	na uporabnikovi pametni kartici ali v programski opremi pri uporabniku	na uporabnikovi pametni kartici ali v programski opremi pri uporabniku	ne obstaja
javni ključ za preverjanje digitalnega podpisa in šifriranje	SREDNJA	na uporabnikovi pametni kartici ali v programski opremi pri uporabniku	na uporabnikovi pametni kartici ali v programski opremi pri uporabniku	v vsaki kopiji digitalnega potrdila za preverjanje digitalnega podpisa in šifriranje
zasebni ključ za digitalni podpis in dešifriranje	NIZKA	v programski opremi pri uporabniku	v programski opremi pri uporabniku	ne obstaja
javni ključ za preverjanje digitalnega podpisa in šifriranje	NIZKA	v programski opremi pri uporabniku	v programski opremi pri uporabniku	v vsaki kopiji digitalnega potrdila za preverjanje digitalnega podpisa in šifriranje

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 pri bodočem imetniku. 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 (to so neupravljana digitalna potrdila VISOKE stopnje zaupanja), izvede generiranje zasebnega ključa za digitalni podpis in dešifriranje na uporabnikovi pametni kartici operativno osebje overitelja SIMoD-CA-Restricted. Pametna kartica se nato varno posreduje imetniku.

6.1.3. Dostava imetnikovega javnega ključa overitelju

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

[17] Digitalna potrdila tipa B, spletna ali WEB digitalna potrdila.

[18] Neupravljana digitalna potrdila VISOKE stopnje zaupanja so digitalna potrdila z obvezno uporabo pametne kartice. Ker zaradi uporabljene tehnologije 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.

6.1.4. Dostava overiteljevega javnega ključa uporabnikom

Javni ključ overitelja SIMoD-CA-Restricted oziroma overiteljevo digitalno 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

Dolžina RSA zasebnega ključa korenskega overitelja SIMoD-CA-Root je 4096 bitov.

Dolžina RSA zasebnega ključa overitelja SIMoD-CA-Restricted je 2048 bitov.

Dolžina RSA zasebnega ključa v imetniških digitalnih potrdilih je 2048 bitov.

6.1.6. Parametri za generiranje javnih ključev in preverjanje parametrov

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

6.1.7. Namen uporabe ključev

Namen uporabe ključev je določen v razširitvenem polju *keyUsage* in *extKeyUsage* po priporočilu [9] RFC 3280.

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

Vrsta digitalnega potrdila	Vrednost polja *keyUsage*
digitalno potrdilo overitelja SIMoD-CA-Restricted	*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*

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

Razširitveno polje *NonRepudiation* se ne uporablja.

6.2. Zaščita zasebnih ključev in zahteve za kriptografske module

6.2.1. Standardi za kriptografski modul

Overitelj SIMoD-CA-Restricted uporablja strojni varnostni kriptografski modul, ki ima potrdilo o skladnosti z FIPS 140-2 Level 3.

Izdajatelj varnih časovnih žigov mora uporabljati strojni varnostni kriptografski modul, ki ustreza 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 overitelja SIMoD-CA-Restricted in imetniki digitalnih potrdil VISOKE stopnje zaupanja uporabljajo pametne kartice stopnje varnosti FIPS 140-2 level 2. Pametna kartica se uporablja na način, da zasebni ključ pametne kartice nikoli ne zapusti.

Imetniki digitalnih potrdil SREDNJE stopnje zaupanja uporabljajo programske kriptografske module 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 SIMoD-CA-Restricted 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 overitelja SIMoD-CA-Restricted ni možno. Tehnična izvedba varnostnega kriptografskega modula ne omogoča prikaza zasebnega ključa overitelja v nešifrirani obliki.

Odkrivanje zasebnega ključa izdajateljev časovnih žigov ni dovoljeno.

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 SIMoD-CA-Restricted se zagotavlja z mehanizmi varnostnega kriptografskega modula. Varnostna kopija se pred izvozom iz varnostnega kriptografskega modula šifrira. Dešifrirni ključ je porazdeljen na N[19] od M[20] administratorskih pametnih karticah.

Kopije zasebnih ključev za dešifriranje digitalnih potrdil za katera overitelj zagotavlja storitev povrnitve zgodovine ključev, se hranijo na overiteljevih sistemih 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 ključev za dešifriranje.

6.2.6. Zapis zasebnega ključa v kriptografski modul in iz njega

Zasebni ključ overitelja SIMoD-CA-Restricted in izdajateljev 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 bodočemu imetniku z uporabo protokola PKIX-CMP.

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

6.2.7. Hranjenje zasebnega ključev v kriptografskem modulu

Zasebni ključi overitelja SIMoD-CA-Restricted in izdajateljev časovnih žigov se hranijo v varnostnem kriptografskem modulu in v varnostni kopiji na disku v šifrirani obliki in se nikdar ne pojavijo izven modula v nešifrirani obliki.

---

[19] N mora biti enako ali večje od 2.

[20] M mora biti eneko ali večje od 5.

6.2.8. Postopek za aktiviranje zasebnega ključa

Zasebni ključi overitelja SIMoD-CA-Restricted in izdajateljev varnih časovnih žigov se aktivirajo ob zagonu aplikativne programske opreme. Za aktiviranje je potrebno predložiti operatersko pametno kartico varnostnega kriptografskega modula ter administratorsko geslo.

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 ključi overitelja SIMoD-CA-Restricted in izdajateljev varnih časovnih žigov se deaktivirajo 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 SIMoD-CA-Restricted 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

Operativno osebje uniči zasebne ključe overitelja SIMoD-CA-Restricted, ko jim poteče obdobje uporabe, oziroma se ne uporabljajo več iz drugih razlogov. Ob uničenju ključev se uničitjo aktivne kopije v varnostnem kriptografskem modulu in vse varnostne kopije.

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

6.2.11. Stopnja varnosti kriptografskih modulov

Opisano v poglavju 6.2.1 Standardi za kriptografski modul.

6.3. Ostali vidiki upravljanja s pari ključev

6.3.1. Arhiviranje javnega ključa

Overitelj SIMoD-CA-Restricted 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:

Vrsta digitalnega potrdila	Ključ	Veljavnost
digitalno potrdilo korenskega overitelja SIMoD-CA-Root	zasebni	šest (6) let
	javni	dvanajst (12) let
digitalno potrdilo overitelja SIMoD-CA-Restricted	zasebni	tri (3) leta
	javni	šest (6) let
digitalno potrdilo za preverjanje digitalnega podpisa	zasebni	dve (2) leti
	javni	tri (3) leta
digitalno potrdilo za šifriranje	zasebni	neomejeno
	javni	tri (3) leta
digitalna potrdilo za preverjanje digitalnega podpisa in šifriranje	zasebni	tri (3) leta
	javni	tri (3) leta
digitalno potrdilo izdajateljev varnih časovnih žigov	zasebni	eno (1) leto
	javni	tri (3) leta

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 (to so neupravljana digitalna potrdila VISOKE stopnje zaupanja), 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 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 SIMoD-CA-Restricted 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

Elementi informacijskega sistem overitelja SIMoD-CA-Restricted za upravljanje z digitalnimi potrdili dosegajo raven varnostne zaščite računalnikov vsaj EAL 3.

6.6. Tehnični nadzor življenjskega cikla overitelja

6.6.1. Nadzor razvoja sistema

Strojna oprema, operacijski sistemi in programska oprema overitelja SIMoD-CA-Restricted so komercialni proizvodi.

6.6.2. Upravljanje varnosti

Overitelj SIMoD-CA-Restricted evidentira postopke inštalacije, sprememb konfiguracije in nadgradenj za vse svoje informacijske in komunikacijske komponente.

Operativno osebje overitelja SIMoD-CA-Restricted periodično in ob vsaki namestitvi nove verzije ali popravka preverja celovitost operacijskega sistema in aplikativne programske opreme overitelja.

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 SIMoD-CA-Restricted 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 overitelja SIMoD-CA-Restricted oziroma upravljanje varnosti skozi celoten življenjski je v skladu z 6.6.2 Upravljanje varnosti.

6.7. Varnostne kontrole na ravni računalniškega omrežja

Komunikacijsko informacijski sistemi overitelja SIMoD-CA-Restricted delujejo v izoliranem omrežju, ki je z drugimi omrežji KIS MO in SV povezan preko varnostnih pregrad. Varnostna pravila na varnostnih pregradah dovoljujejo prehod samo protokolom, potrebnim za dostop do storitev overitelja SIMoD-CA-Restricted.

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

Overitelj SIMoD-CA-Restricted izdaja digitalna potrdila X.509 verzije 3 v skladu s priporočilom [9] RFC 3280, ki vsebujejo naslednja osnovna polja:

Ime osnovnega polja	Slovensko ime ali opis	Vrednost
version	verzija potrdila X.509	*v3*
serialNumber	enolična serijska številka	enolična serijska številka
signature	algoritem za podpis potrdila, podpis potrdila	*sha1WithRSAEncryption*, podpis potrdila s strani overitelja
issuer	izdajatelj	razločevalno ime izdajatelja digitalnega potrdila
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 [9] RFC 3280 uporabljena v digitalnih potrdilih korenskega overitelja SIMoD-CA-Root, overitelja SIMoD-CA-Restricted in izdajateljev časovnega žiga so:

Ime razširitvenega polja / prevod ali opis	Digitalno potrdilo SIMoD-CA-Root	Digitalno potrdilo SIMoD-CA-Restricted	Digitalna potrdila za izdajatelje varnih časovnih žigov
Authority Key Identifier / odtis javnega ključa overitelja	Ni uporabljeno	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Root, s katerim je podpisano potrdilo	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Restricted, s katerim je podpisano potrdilo
Subject Key Identifier / odtis imetnikovega javnega ključa	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Root	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Restricted	SHA-1 odtis javnega ključa izdajatelja časovnega žiga
Key Usage / namen uporabe ključa	**Kritično** keyCertSign cRLSign	**Kritično** keyCertSign cRLSign	**Kritično** digitalSignature
extended Key Usage / razširjen namen uporabe	Ni uporabljeno	Ni uporabljeno	**Kritično** id-kp-timeStamping
Private Key Usage Period / veljavnost zasebnega ključa	V skladu s 6.3.2 *Not Before*: *Not After*:	V skladu s 6.3.2 *Not Before*: *Not After*:	V skladu s 6.3.2 *Not Before*: *Not After*:
certificatePolicies / oznaka politike potrdila	Ni uporabljeno	Ni uporabljeno	*id-ce-certificatePolicie*s[21]
policyIdentifier / enolična oznaka politike			Skladno s 1.2. in 7.1.6 *OID: 1.3.6.1.4.1.22295.10.1.1.1.5.4.1*
policyQualifier / podatki o politiki			*Qualifiers OID* *Qualifier: »http:/www.simod-pki.mors.si/«*
CRL Distribution Point / naslovi registra preklicanih potrdil	Ni uporabljeno	LDAP in http URL naslov registra preklicanih potrdil SIMoD-CA-Root	LDAP in http URL naslov registra preklicanih potrdil SIMoD-CA-Restricted
subject Alternative Name / alternativno ime imetnika	Ni uporabljeno	Ni uporabljeno	Ni uporabljeno
Basic Constraints / osnovne omejitve	**Kritično** CA =: True pathLenConstraint = 1	**Kritično** CA =: True pathLenConstraint = 0	**Kritično** CA =: False

[21] Podrobneje opisano v Pravilih delovanja izdajatelja časovnega žiga

Imetniška digitalna potrdila, ki jih izdaja overitelj SIMoD-CA-Restricted, vsebujejo naslednja razširitvena polja po priporočilu [9] RFC 3280:

Ime razširitvenega polja / prevod ali opis	Potrdilo za preverjanje digitalnega podpisa	Potrdilo za šifriranje	Potrdilo za preverjanje digitalnega podpisa in šifriranje
Authority Key Identifier / odtis javnega ključa overitelja	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Restricted, s katerim je podpisano potrdilo	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Restricted, s katerim je podpisano potrdilo	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Restricted, s katerim je podpisano potrdilo
Subject Key Identifier / odtis imetnikovega javnega ključa	SHA-1 odtis imetnikovega javnega ključa	SHA-1 odtis imetnikovega javnega ključa	SHA-1 odtis imetnikovega javnega ključa
Key Usage / namen uporabe ključa	**Kritično** digitalSignature	**Kritično** keyEncipherment	**Kritično** DigitalSignature keyEncipherment
extended Key Usage / razširjen namen uporabe	Ni uporabljeno	Ni uporabljeno	Ni uporabljeno
Private Key Usage Period / veljavnost zasebnega ključa	V skladu s poglavjem 6.3.2 *Not Before*: *Not After*:	V skladu s poglavjem 6.3.2 *Not Before*: *Not After*:	V skladu s poglavjem 6.3.2 *Not Before*: *Not After*:
certificatePolicies / oznaka politike potrdila	*[1]Certificate Policy:*	*[1]Certificate Policy:*	*[1]Certificate Policy:*
policyIdentifier / enolična oznaka politike	Skladno s 1.2. in 7.1.6 *Policy Identifier=*	Skladno s 1.2. in 7.1.6 *Policy Identifier=*	Skladno s 1.2. in 7.1.6 *Policy Identifier=*
policyQualifier / podatki o politiki	*[1,1]Policy Qualifier Info:* *Policy Qualifier Id=CPS* *Qualifier:* *http:/www.simod-pki.mors.si/*	*[1,1]Policy Qualifier Info:* *Policy Qualifier Id=CPS* *Qualifier:* *http:/www.simod-pki.mors.si/*	*[1,1]Policy Qualifier Info:* *Policy Qualifier Id=CPS* *Qualifier:* *http:/www.simod-pki.mors.si/*
CRL Distribution Point / naslovi registra preklicanih potrdil	LDAP in http URL naslov registra preklicanih potrdil SIMoD-CA-Restricted	LDAP in http URL naslov registra preklicanih potrdil SIMoD-CA-Restricted	LDAP in http URL naslov registra preklicanih potrdil SIMoD-CA-Restricted
subject Alternative Name / alternativno ime imetnika	• *rfc822Name* – naslov elektronske pošte in/ali • *OtherName, Permanent Identifier* in/ali • *DNS Name* in/ali • druga standardna polja	• *rfc822Name* – naslov elektronske pošte in/ali • *OtherName, Permanent Identifier* in/ali • *DNS Name* in/ali • druga standardna polja	• *rfc822Name* – naslov elektronske pošte in/ali • *OtherName, Permanent Identifier* in/ali • *DNS Name* in/ali • druga standardna polja
Basic Constraints / osnovne omejitve	**Kritično** CA =: False	**Kritično** CA =: False	**Kritično** CA =: False

Kvailficirana potrdila, skladna z [5] ETSI TS 101 456, vsebujejo izjavo, da ustrezajo profilu kvalificiranih potrdil po priporočilu [6] 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*

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 3.1.2 Potreba po smiselnosti imen.

7.1.6. Identifikacijska oznaka politik

Digitalno potrdilo, ki ga izda overitelj SIMoD-CA-Restricted, vsebuje v polju *certificatePolicies* vsaj eno identifikacijsko oznako politike.

Kvalificirana potrdila imajo skladno s priporočilom [5] ETSI TS 101 456 v polju *certificatePolicies*, *policyIdentifier* poleg oznake politike overitelja SIMoD-CA-Restricted 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 *Policy Constrains* 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 [9] RFC 3280.

7.2. Profil registrov preklicanih potrdil

7.2.1. Verzija registrov preklicanih potrdil

Overitelj SIMoD-CA-Restricted izdaja registre preklicanih potrdil verzije 2 v skladu s priporočilom [9] 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*, podpis
Issuer	izdajatelj	razločevalno ime overitelja SIMoD-CA-Restricted
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

Overitelj SIMoD-CA-Restricted izdajajo registre preklicanih potrdil verzije 2 v skladu s priporočilom [9] 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 SIMoD-CA-Restricted

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 SIMoD-CA-Restricted s Politiko SIMoD-PKI in Pravili delovanja overitelja SIMoD-CA-Restricted, 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 SIMoD-CA-Restricted s Politiko SIMoD-PKI in pravili delovanja overitelja SIMoD-CA-Restricted, 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 SIMoD-CA-Restricted.

Zunanja inšpekcijska služba preverja samo skladnost delovanja overitelja s Politiko SIMoD-PKI in Pravili delovanja overitelja SIMoD-CA-Restricted.

Svet za upravljanje z infrastrukturo javnih ključev na MO ob nameri medsebojnega priznavanja z drugimi overitelji zagotovi drugim overiteljem jamstva, da overitelj SIMoD-CA-Restricted 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 SIMoD-CA-Restricted 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 SIMoD-CA-Restricted 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 SIMoD-CA-Restricted do naslednje predvidene inšpekcije ali
- pred preklicem overiteljevega potrdila dodeli overitelju 30 dni za odpravo pomanjkljivosti, v tem času dovoli overitelju SIMoD-CA-Restricted 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 SIMoD-CA-Restricted 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

Overitelj SIMoD-CA-Restricted pridobi 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 [16] Zakon o varstvu osebnih podatkov.

9.4.2. Obseg osebnih podatkov, ki se obravnavajo kot zaupni

Osebne podatke določa [16] 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 [16] 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 SIMoD-CA-Restricted

Overitelj SIMoD-CA-Restricted jamči, da upravlja z digitalnimi potrdili v skladu s Politiko SIMoD-PKI in Pravili delovanja overitelja SIMoD-CA-Restricted. Overitelja SIMoD-CA-Restricted predstavlja in jamči za izpolnjevanje njegovih obveznosti Svet za upravljanje z infrastrukturo javnih ključev na MO.

9.6.2. Odgovornost in jamstva prijavne službe

Prijavna služba je odgovorna za skladnost identifikacijskih postopkov s Politiko SIMoD-PKI in Pravili delovanja overitelja SIMoD-CA-Restricted ter za točnost podatkov v zahtevkih. Za pravilnost delovanja prijavne službe jamči overitelj SIMoD-CA-Restricted 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 in Javnimi pravili SIMoD-CA-Restricted pred podpisom zahtevka za izdajo digitalnega potrdila,

- ravna v skladu s Politiko SIMoD-PKI, Javnimi pravili SIMoD-CA-Restricted in ostalimi pravnimi akti,
- spremlja obvestila overitelja SIMoD-CA-Restricted in ravna v skladu z njimi,
- je prijavni službi ali operativnemu osebju overitelja SIMoD-CA-Restricted 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 tretje osebe

Tretja oseba, ki se zanaša na digitalna potrdila overitelja SIMoD-CA-Restricted, jamči, da uporablja digitalna potrdila le za namene, določene v Politiki SIMoD-PKI in Pravilih delovanja overitelja SIMoD-CA-Restricted 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 SIMoD-CA-Restricted

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

- je bilo 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 SIMoD-CA-Restricted ali morebitni drugi pogodbi,
- imetnik ali tretja oseba ni postopala v skladu s predpisanimi postopki v Politiki SIMoD-PKI, Pravilih delovanja overitelja SIMoD-CA-Restricted, morebitni drugi pogodbi ali obvestili overitelja SIMoD-CA-Restricted,
- je nastala škoda zaradi napake v delovanju strojne ali programske opreme imetnika ali tretje osebe,
- je do ravnanja v nasprotju s Politiko SIMoD-PKI, Pravili delovanja overitelja SIMoD-CA-Restricted ali ostalimi dokumenti prišlo zaradi višje sile, to je izredne nepredvidljive okoliščine na katere udeleženci infrastrukture javnih ključev na MO ne morejo vplivati, kot so na primer naravne nesreče ali teroristična dejanja

9.8. Omejitve odgovornosti overitelja SIMoD-CA-Restricted

Overitelj SIMoD-CA-Restricted 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 overitelj SIMoD-CA-Restricted ne prevzema 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

Pravila delovanja overitelja SIMoD-CA-Restricted, javni del začnejo veljati in se uporabljati naslednji dan po podpisu.

9.10.2.Prenehanje veljavnosti

Veljavnost dokumenta ni časovna omejena in velja do objave nove verzije, oziroma do prenehanja delovanja overitelja SIMoD-CA-Restricted.

9.10.3.Posledice prenehanja veljavnosti

Po prenehanju veljavnosti Pravil delovanja overitelja SIMoD-CA-Restricted zaradi objave nove verzije imetniki praviloma uporabljajo obstoječa potrdila v skladu z določili Pravil delovanja overitelja SIMoD-CA-Restricted, po kateri so bila izdana. V primeru, da zaradi spremenjenih okoliščin to ne bo več mogoče, bo overitelj SIMoD-CA-Restricted ob izdaji nove verzije o tem obvestil imetnike.

9.11. Obvestila in komuniciranje z udeleženci

Obvestila overitelja SIMoD-CA-Restricted so objavljena na spletni strani: http://www.simod-pki.mors.si.

9.12. Spreminjanje dokumenta

9.12.1.Postopke uveljavitve spremembe

Svet za upravljanje z infrastrukturo javnih ključev na MO predlaga spremembe in sprejema Javna pravila SIMoD-CA-Restricted.

9.12.2.Postopek obveščanja in rok za pripombe

Spremembe Javnih pravil SIMoD-CA-Restricted 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.

9.12.3.Spremembe, ki zahtevajo novo identifikacijsko oznako politike

Svet za upravljanje z infrastrukturo javnih ključev na MO odloči, ali so spremembe vsebine Javnih pravil SIMoD-CA-Restricted tolikšne, da zahtevajo objavo novih Javnih pravil SIMoD-CA- Restricted 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

Overitelj SIMoD-CA-Restricted deluje 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]	Politika SIMoD-PKI	Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, Verzija 2.0., št. 382-5/2006-109, datum: 24.08.2010
[4]	Pravila SIMoD-CA-Root	Pravila delovanja overitelja SIMoD-CA-Root, ver. 2.0
[5]	ETSI TS 101 456	Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates
[6]	ETSI TS 101 862	Qualified Certificate profile
[7]	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
[8]	RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[9]	RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[10]	RFC 4043	Internet X.509 Public Key Infrastructure Permanent Id
[11]	RFC 4210	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
[12]	PKCS#10	Certification Request Syntax Standard

9.15. Ostala relevantna zakonodaja

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

[13]	ETSI TS 102 023	Policy requirements for time-stamping authorities
[14]	ZObr	Zakon o obrambi (Uradni list RS, št. 103/04 – UPB1)
[15]	ZTP	Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – UPB2, 9/10)
[16]	Zakon o varstvu osebnih podatkov	(Uradni list RS, št. 94/07 – UPB1)

9.16. Razne določbe

Poleg Javnih pravil SIMoD-CA-Restricted opredeljujejo delovanje overitelja SIMoD-CA-Restricted še naslednji dokumenti:

A.1. Postopkovnik o objavljanju imenikov digitalnih potrdil overiteljev infrastrukture javnih ključev na Ministrstvu za obrambo

A.2. Načrt varovanja tajnih podatkov v prostorih Centralnega registra NATO/EU

A.3. Postopkovnik o hranjenju varnostno občutljivega materiala v infrastrukturi javnih ključev na MO

A.4. Postopek tvorjenja prvega para ključev ključev overitelja SIMoD-CA-Restricted

A.5. Postopek obnove ključev overitelja SIMoD-CA-Restricted

A.6. Postopkovnik o tehnični arhitekturi infrastrukture SIMoD-PKI

A.7. Postopkovnik o izdelavi varnostnih kopij strežnikov infrastrukture SIMoD-PKI

A.8. Varnostna okrepitev HP-UX strežnikov

A.9. Pravila delovanja overitelja SIMoD-CA-Restricted, zaupni del

9.17. Končne določbe

Ta Pravila delovanja overitelja SIMoD-CA-Restricted, javni del začnejo veljati in se uporabljati v skladu s poglavjem 9.10.1 Začetek veljavnosti.

Številka: 382-5/2006-121

Datum: 23.11.2010

Mag. Jurij Bertok
Sekretar
Vodja Sveta za upravljanje z infrastrukturo javnih ključev na MO