REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Pravila delovanja overitelja SIMoD-CA-Root, javni del

(Javna pravila SIMoD-CA-Root)

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 in 2/01) ter v skladu s 7. odstavkom poglavja 1.1. Pregled Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije izdajam

PRAVILA DELOVANJA OVERITELJA SIMoD-CA-Root, JAVNI DEL

(JAVNA PRAVILA SIMoD-CA-Root)

1. UVOD

1.1. Pregled

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

V okviru SIMoD-PKI deluje korenski overitelj SIMoD-CA-Root (angl.: **S**lovenian **M**inistry **o**f **D**efence **Root C**ertification **A**uthority), podrejeni overitelji digitalnih potrdil in izdajatelji varnih časovnih žigov, v nadaljevanju overitelji SIMoD-PKI.

SIMoD-CA-Root deluje v skladu s Politiko SIMoD-PKI, ki predpisuje zahteve za digitalna potrdila, nivo zaupanja v njih, zahteve za tehnične lastnosti in raven varnosti infrastrukture overiteljev, postopke za upravljanje z digitalnimi potrdili, ter določa obveznosti in odgovornosti, ki jih morajo izpolnjevati overitelji, imetniki in tretje osebe, ki se zanašajo na digitalna potrdila, ter drugi overitelji, ki se želijo povezovati z infrastrukturo javnih ključev na MO.

Pričujoči dokument predstavlja javni del pravil delovanja SIMoD-CA-Root korenskega overitelja. Dokument podaja opis overiteljeve infrastrukture, postopkov overitelja kot korenskega overitelja, ter izpolnjevanje zahtev Politike SIMoD-PKI. Zainteresirane strani, ki potrebujejo informacije za oceno zaupanja v SIMoD-PKI kot celoto, oceno zaupanja v digitalna potrdila imetnikov, ali informacije o podrejenem overitelju, morajo poleg pričujočega dokumenta upoštevati še določila Politike SIMoD-PKI ter javnih pravil delovanja podrejenih overiteljev.

SIMoD-CA-Root kot korenski overitelj predstavlja vrh hierarhične infrastrukture overiteljev SIMoD-PKI. SIMoD-CA-Root izdaja digitalna potrdila:

- podrejenim overiteljem, ki izdajajo potrdila v skladu s Politiko SIMoD-PKI;
- medsebojno priznanim overiteljem; ter
- operativnemu osebju za potrebe upravljanja SIMoD-CA-Root infrastrukture.

1.2. Naziv dokumenta in identifikacijska oznaka

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

Identifikacijska oznaka dokumenta (angl. Policy Object Identifier; Policy OID) je določena v skladu s pravili dodeljevanja identifikacijskih oznak (Politika SIMoD-PKI, poglavje 1.2. Naziv dokumenta). Prvi del identifikacijske oznake Javnih pravil SIMoD-CA-Root (1.3.6.1.4.1.22295[1].<storitev>.<overitelj>) je tako določen po pravilu:

1 Identifikacijaka oznaka MO registrirana pri www.iana.org (http://www.iana.org/assignments/enterprise-numbers)

Del identifikacijske oznake	Vrednost	
1.3.6.1.4.1.22295	enolična identifikacijska oznaka MO	
storitev	1..100	storitve PKI:
	10	storitve SIMoD-PKI
	101..1000	druge storitve v MO
overitelj	1	SIMoD-PKI
	2	SIMoD-CA-Root
	3	SIMoD-CA-Restricted
	...	rezervirano za ostale overitelje SIMoD-PKI

Overitelj SIMoD-CA-Root izbere za preostale vrednosti identifikacijske oznake Javnih pravil SIMoD-CA-Root naslednja parametra:

<vrsta dokumenta>.<verzija>.

V tabeli je postopek določanja preostalih vrednosti identifikacijske oznake za Javna pravila SIMoD-CA-Root:

Del identifikacijske oznake	Vrednost	
vrsta dokumenta	1	Pravila delovanja v smislu politike izdajanja digitalnih potrdil (angl. Certificate Policy)
	2	Pravila delovanja v smislu pravil delovanja overitelja (angl. Certification Practicies Statement)
	…	rezervirano za ostale dokumente in druge namene
verzija	zaporedna številka izdaje dokumenta	

Identifikacijska oznaka Javnih pravil SIMoD-CA-Root se torej določi po pravilu:

1.3.6.1.4.1.22295.10.2.<vrsta dokumenta>.<verzija>

in ima vrednost 1.3.6.1.4.1.22295.10.2.2.0. Identifikacijska oznaka se uporablja za enolično označevanje dokumenta in njegove verzije. Oznaka se ne uporablja za označevanje digitalnih potrdil.

Oblika dokumenta je napisana v skladu z RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy in sicer v smislu in kontekstu pravil delovanja overitelja (angl. Certification Practice Statement) v skladu z RFC 3647[2] v odnosu na Politiko SIMoD-PKI.

1.3. Udeleženci infrastrukture javnih ključev

1.3.1. Overitelji

V okviru SIMoD-PKI deluje korenski overitelj SIMoD-CA-Root, podrejeni overitelji digitalnih potrdil in izdajatelji varnih časovnih žigov, v nadaljevanju overitelji SIMoD-PKI.

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

1.3.1.1. Svet za upravljanje z infrastrukturo javnih ključev na MO

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

[2] RFC 3647, Poglavje 3.4. Certification Practice Statement in Certification Practice Statement

- nadzira izdelavo, vodi postopek potrditve, ocenjuje predlagane spremembe, predlaga uveljavitve sprememb in načrtuje postopek uveljavitve sprememb Politike SIMoD-PKI;
- ocenjuje in potrjuje skladnost pravil delovanja posameznega overitelja s Politiko SIMoD-PKI;
- imenuje operativno osebje overiteljev SIMoD-PKI;
- operativnemu osebju daje usmeritve in navodila za odpravljanje pomanjkljivosti, ugotovljene v nadzoru skladnosti delovanja s Politiko SIMoD-PKI in pravili delovanja posameznega overitelja oziroma uveljavlja druge ustrezne ukrepe, kot je npr. preklic overiteljevega potrdila;
- ocenjuje ustreznost politik digitalnih potrdil drugih overiteljev s Politiko SIMoD-PKI 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-Root

Operativno osebje overitelja SIMoD-CA-Root 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-Root.

1.3.2. Prijavna služba

SIMoD-CA-Root nima vzpostavljene prijavne službe.

1.3.3. Imetniki digitalnih potrdil

SIMoD-CA-Root izdaja digitalna potrdila podrejenim overiteljem, izdajateljem časovnih žigov in medsebojno priznanim overiteljem. Podrejeni overitelji, izdajatelji časovnih žigov ali medsebojno priznani drugi overitelji so s tehničnega stališča tudi imetniki digitalnih potrdil, vendar se v skladu s Politiko SIMoD-PKI 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.

SIMoD-CA-Root ne izdaja digitalnih potrdil imetnikom.

SIMoD-CA-Root izdaja poleg digitalnih potrdil za podrejene overitelje in medsebojno priznane overitelje tudi digitalna potrdila operativnemu osebju, izključno za potrebe upravljanja z overiteljevo infrastrukturo. Postopki upravljanja teh digitalnih potrdil so določeni v notranjih pravilih SIMoD-CA-Root in niso obravnavani v nadaljevanju pričujočega dokumenta.

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 samopodpisano potrdilo SIMoD-CA-Root overitelja.

Tretje osebe so:

- imetniki digitalnih potrdil overiteljev SIMoD-PKI;
- imetniki digitalnih potrdil overiteljev, ki so medsebojno priznani s SIMoD-PKI;
- podrejeni overitelji;
- subjekti, ki nimajo digitalnega potrdila enega od overiteljev SIMoD-PKI, a se zanašajo na digitalna potrdila, ki so jih je izdali overitelji SIMoD-PKI.

1.3.5. Posredno odgovorni organi

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

1.4. Namen uporabe digitalnih potrdil

SIMoD-CA-Root deluje kot korenski overitelj digitalnih potrdil podrejenih overiteljev SIMoD-PKI ter medsebojno priznanih overiteljev.

Nameni uporabe digitalnih potrdil, ki jih podrejeni overitelji izdajajo imetnikom, so določeni v Politiki SIMoD-PKI in pravilih delovanja posameznega overitelja.

1.4.1. Dovoljena uporaba digitalnih potrdil

Digitalna potrdila, ki jih izdaja SIMoD-CA-Root in digitalna potrdila, ki jih podrejeni overitelji izdajajo imetnikom, so namenjena izključno službeni uporabi v MO.

1.4.2. Nedovoljena uporaba digitalnih potrdil

Ni relevantno.

1.5. Upravljanje s pravili delovanja SIMoD-CA-Root

1.5.1. Organ, ki upravlja s pričujočim dokumentom

1.5.1.1. Svet za upravljanje z infrastrukturo javnih ključev na MO

Svet za upravljanje z infrastrukturo javnih ključev na MOima v zvezi upravljanjem z dokumentom Javna pravila SIMoD-CA-Root obveznost nadzirati izdelavo, voditi postopek potrditve, ocenjevati predlagane spremembe, predlagati uveljavitve sprememb in načrtovati postopek uveljavitve sprememb Politike SIMoD-PKI.

1.5.1.2. Operativno osebje overitelja

Operativno osebje overitelja SIMoD-CA-Root v okviru svojih nalog svetuje Svetu za upravljanje z infrastrukturo javnih ključev na MO glede organizacijskih in tehničnih zadev, ter predlaga spremembe Politike SIMoD-PKI in pravil delovanja SIMoD-CA-Root.

1.5.2. Kontaktna oseba

Naslov:	Republika Slovenija Ministrstvo za obrambo Direktorat za obrambne zadeve Urad za informatiko in komunikacije Svet za upravljanje z infrastrukturo javnih ključev na MO Vojkova cesta 55, 1000 Ljubljana
Telefon:	01 230 5270, 01 230 5314
Fax:	01 471 2701
Spletni naslov:	http://www.simod-pki.mors.si
Naslov elektronske pošte:	simod-pki@mors.si

Zgoraj navedeni kontaktni naslov Sveta za upravljanje z infrastrukturo javnih ključev na MO se uporablja tudi kot kontaktni naslov operativnega osebja SIMoD-CA-Root.

1.5.3. Odgovorni organ za odobritev skladnosti pravil delovanja overitelja SIMoD-CA-Root s Politiko SIMoD-PKI

Skladnosti pravil delovanja overitelja SIMoD-CA-Root s Politiko SIMoD-PKI potrjuje Svet za upravljanje z infrastrukturo javnih ključev na MO.

1.5.4. Postopek odobritve pravil delovanja overitelja SIMoD-CA-Root

V okviru postopka odobritve pravil delovanja overitelja se preveri:

- skladnost pravil delovanja overitelja SIMoD-CA-Root z zahtevami Politike SIMoD-PKI;
- overiteljevo infrastrukturo in postopke, glede na določila Politike SIMoD-PKI, ter javni in zaupni del overiteljevih pravil delovanja.

1.6. Pojmi in kratice

Glej dodatek KRATICE IN POJMI.

2. ODGOVORNOST ZA OBJAVE IN REPOZITORIJ

2.1. Repozitoriji

Repozitorij je storitev objavljanja digitalnih potrdil, registrov preklicanih potrdil ter drugih podatkov tretjim osebam. Repozitorij sestavlja več imenikov in spletnih strežnikov.

Repozitorij je stalno dostopen. V primeru odpovedi dostopa pristopi operativno osebje overitelja k odpravljanju napake v najkrajšem možnem času, ne glede na to, da rezervna kopija imenika normalno obratuje.

Stalna dostopnost imenika v okviru infrastrukture javnih ključev na MO je zagotovljena z več vstopnimi točkami v imenik oz. več ekvivalentnih imenikov, tako da je vsakemu uporabniku zagotovljen dostop do potrdil in list preklicanih potrdil. Položaj imenikov v KIS MO in SV je tak, da je zagotovljen dostop do imeniških storitev vsem uporabnikom ne glede na njihov položaj v segmentiranem omrežju. Zagotovljeno je medsebojno usklajevanje imenikov z namenom, da imajo vsi uporabniki dostopen vsaj en ažuren imenik.

Razen v izjemnih primerih, ko je določeni omrežni segment zaradi trenutne napake ali nezmožnosti povezave izoliran, so potrdila in liste preklicanih potrdil dostopne uporabnikom v skladu z zahtevami Politike SIMoD-PKI.

Pri povezovanju z drugimi KIS, ki niso pod upravljanjem MO in SV, se morajo opredeliti tudi načini in postopki zagotavljanja dostopnosti repozitorija uporabnikom drugih KIS.

2.2. Objave informacij o digitalnih potrdilih

Politika SIMoD-PKI, Javna pravila SIMoD-CA-Root, ter javna pravila delovanja podrejenih overiteljev, so objavljena na spletni strani: http://www.simod-pki.mors.si. Vsebina spletnih strani je zaščitena pred nepooblaščenim spreminjanjem.

Na navedeni spletni strani so objavljeni tudi drugi javno dostopni podatki, kot so digitalno potrdilo korenskega overitelja, liste preklicih potrdil ter javne objave overiteljev.

Overitelji v imenikih objavljajo naslednje podatke:

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

Imeniki so dostopni po protokolu LDAP.

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

SIMoD-CA-Root si pridržuje pravico, da nekaterih podatkov ne objavi v vseh imenikih repozitorija.

2.3. Čas in pogostost objav

Overitelj objavi digitalno potrdilo takoj, ko ga izda. Overitelj uvrsti preklicano digitalno potrdilo v register preklicanih potrdil takoj po opravljenem preklicu. Objava registrov preklicanih potrdil je v skladu s poglavji 4.9.5 Čas od vloge za preklic do preklica in 4.9.7 Pogostost objav registrov preklicanih potrdil.

2.4. Dostop do podatkov v repozitoriju

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

Pravila delovanja SIMoD-CA-Root in njegovo digitalno potrdilo, je možno pridobiti tudi direktno od Sveta za upravljanje z infrastrukturo javnih ključev na MO, če je to potrebno zaradi inšpekcijskega nadzora, akreditacije ali medsebojnega povezovanja.

Repozitorij ima vzpostavljene mehanizme za zagotavljanje celovitosti in razpoložljivosti podatkov.

3. PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI

3.1. Določanje imen

3.1.1. Vrste imen

Vsako izdano X.509v3 digitalno potrdilo vsebuje polje *Subject* z edinstvenim razločevalnim imenom - X.501 DN (angl.: Distinguished Name, DN) v skladu z RFC3280. Digitalna potrdila, izdana podrejenim overiteljem, lahko vsebujejo tudi alternativno ime overitelja vsebovano v polju *SubjectAlteranteName,* tudi v skladu z RFC3280. Razločevalno ime je v digitalno potrdilo zapisano v obliki X.501 UTF8String in ni nikdar prazno.

3.1.2. Potreba po smiselnosti imen

Splošno ime (angl. Common Name, CN) mora enolično identificirati podrejenega overitelja.

SIMoD-CA-Root izdaja le digitalna potrdila podrejenim overiteljem, ki imajo v polju *Subject* razločevalno ime iz imenskega prostora, ki ga odobri Svet za upravljanje z infrastrukturo javnih ključev na MO.

Predlog za splošno ime je del prošnje za izdajo potrdila. Svet za upravljanje z infrastrukturo javnih ključev na MO lahko zavrne predlog za splošno ime, če je neprimerno, zavajajoče za tretje osebe, oziroma pripada neki drugi pravni ali fizični osebi ali je v nasprotju z veljavnimi predpisi.

3.1.3. Anonimnost imetnikov in uporaba psevdonimov

Dovoljena je samo uporaba imen skladno s poglavjem 3.1.2 Potreba po smiselnosti imen. Uporaba psevdonimov ni dovoljena. SIMoD-CA-Root ne izdaja digitalnih potrdil z zakrito identiteto oziroma mehanizmi zagotavljanja anonimnosti.

3.1.4. Pravila za interpretacijo različnih oblik imen

Imena se interpretirajo v skladu z definicijami v poglavju 3.1.1 Vrste imen, 3.1.2 Potreba po smiselnosti imen in 7.1.4 Oblike imen.

3.1.5. Edinstvenost imen

Razločevalna imena - X.501 DN (angl. Distinguished Name, DN) so edinstvena in enolično identificirajo podrejenega overitelja.

3.1.6. Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk

Uporaba zaščitenih znamk v imenih je dovoljena samo nosilcem zaščitenih znamk. SIMoD-CA-Root ne sme zavestno izdati digitalnega potrdila z imenom, ki vsebuje zaščiteno znamko naročniku, ki ni nosilec zaščitene znamke. Operativno osebje SIMoD-CA-Root overitelja ni dolžno preverjati pravic do uporabe zaščitenih znamk, niti razčiščevati sporov glede zaščitenih znamk. Prosilcem ni dovoljeno zahtevati imen, ki bi kršila intelektualne ali avtorske pravice drugih, čeprav se v okviru infrastrukture javnih ključev na MO tega ne preverja niti ne bo Svet za upravljanje z infrastrukturo javnih ključev na MO ali SIMoD-CA-Root posredoval v takšnih sporih. Svet za upravljanje z infrastrukturo javnih ključev na MO in operativno osebje SIMoD-CA-Root overitelja si pridržujeta pravico zavrniti izdajo digitalnega potrdila ali preklicati izdana digitalna potrdila udeležencev spora.

3.2. Prva registracija

3.2.1. Metode dokazovanja lastništva zasebnega ključa

SIMoD-CA-Root preverja lastništvo zasebnega ključa, ki odgovarja javnemu ključu vsebovanem v zahtevku. V ta namen morajo prosilci za izdajo digitalnega potrdila

podrejenemu overitelju predložiti zahtevek v obliki PKCS#10 v skladu z RSA PKCS#10 Certification Request Syntax Standard.

Preverjanje lastništva zasebnega ključa ob izdaji digitalnih potrdil operativnemu osebju SIMoD-CA-Root se preverja z uporabo protokola PKIX-CMP v skladu z RFC 4210 Internet X.509 Public Key Infrastructure (PKI) Certificate Management protocol (CMP) ali PKCS#10 v skladu z RSA PKCS#10 Certification Request Syntax Standard.

3.2.2. Preverjanje istovetnosti notranje organizacijske enote in institucije, ki je povezana z obrambo države

Prošnja za izdajo digitalnega potrdila podrejenemu overitelju mora vsebovati uradni naziv notranje organizacijske enote MO ter ime odgovorne osebe, ki je praviloma vodja notranje organizacijske enote.

SIMoD-CA-Root ne izdaja digitalnih potrdil zunanjim institucijam, ki so povezane z obrambo države.

Istovetnost notranje organizacijske enote preverja Svet za upravljanje z infrastrukturo javnih ključev na MO, ki v primeru pozitivnega preverjanja istovetnosti posreduje informacijo in odobritev izdaje potrdila operativnemu osebju SIMoD-CA-Root.

Svet za upravljanje z infrastrukturo javnih ključev na MO preveri podatke in istovetnost odgovorne osebe iz prejšnjega odstavka ali pooblaščene osebe enako kot za fizične osebe skladno s poglavjem 3.2.3 Preverjanje istovetnosti za fizične osebe.

Svet za upravljanje z infrastrukturo javnih ključev na MO lahko za preverjanje istovetnosti notranje organizacijske enote zadolži organ, ki izvaja naloge prijavne službe v skladu s Politiko SIMoD-PKI.

3.2.3. Preverjanje istovetnosti za fizične osebe

3.2.3.1. Digitalna potrdila za zaposlene

SIMoD-CA-Root izdaja digitalna potrdila le zaposlenim v MO, ki izvajajo naloge operativnega osebja SIMoD-CA-Root. Svet za upravljanje z infrastrukturo javnih ključev na MO preveri pristnost podatkov bodočega imetnika v kadrovski evidenci MO in izvede osebno identifikacijo na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list, ali vozniško dovoljenje) pred dodelitvijo ene od nalog operativnega osebja SIMoD-CA-Root. Dodelitev naloge operativnega osebja SIMoD-CA-Root določeni fizični osebi zaposleni v MO je hkrati tudi odobritev za izdajo digitalnega potrdila.

Svet za upravljanje z infrastrukturo javnih ključev na MO lahko za preverjanje istovetnosti fizične osebe zadolži organ, ki izvaja naloge prijavne službe v skladu s Politiko SIMoD-PKI.

3.2.3.2. Digitalna potrdila za poveljniške dolžnosti v SV

Ni relevantno.

3.2.3.3. Digitalna potrdila za podrejene overitelje, strežnike, drugo strojno in programsko opremo ter izdajatelje časovnega žiga

Prosilec za izdajo digitalnega potrdila podrejenemu overitelju mora Svetu za upravljanje z infrastrukturo javnih ključev na MO preložiti podatke o osebi, ki bo v postopku izdaje digitalnega potrdila overitelju predala zahtevek z javnim ključem, za katerega se izdaja digitalno potrdilo, ter podatke o vodji notranje organizacijske enote MO, v okviru katere deluje podrejeni overitelj. Istovetnost osebe se preveri v skladu s poglavjem 3.2.3.1 Digitalna potrdila za zaposlene.

SIMoD-CA-Root ne izdaja digitalnih potrdil za strežnike, drugo strojno ali programsko opremo ter izdajatelje časovnega žiga.

3.2.4. Podatki o naročniku, ki se ne preverjajo

Ni relevantno.

3.2.5. Preverjanje pooblastil

Preverjanje pooblastil za pridobitev digitalnega potrdila se izvaja v okviru postopkov preverjanja identitete, skladno s poglavjem 3.2.3 Preverjanje istovetnosti za fizične osebe.

3.2.6. Merila za medsebojno povezovanje

Infrastruktura javnih ključev na MO dovoljuje medsebojno povezovanje z drugimi infrastrukturami javnih ključev. Medsebojno povezovanje je mogoče samo na nivoju korenskega overitelja SIMoD-CA-Root. Način in pogoji medsebojnega povezovanja bodo določeni s pogodbo o medsebojnem zaupanju overiteljev. Pogodba o medsebojnem zaupanju overiteljev je obvezna za vse možne načine medsebojnega povezovanja.

Minimalni pogoji za medsebojno povezovanje:

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

3.3. Preverjanje istovetnosti pri obnovi[3] digitalnega potrdila

3.3.1. Preverjanje istovetnosti pri rutinski obnovi digitalnih potrdil

3.3.1.1. Preverjanje istovetnosti pri obnovi digitalnih potrdil z uporabo PKIX-CMP protokola

Obnovo digitalnih potrdil, ki so bila izdana z uporabo PKIX-CMP (RFC 4210) protokola, je mogoče izvesti brez ponovitve postopka identifikacije, dokler oseba izvaja naloge operativnega osebja SIMoD-CA-Root. Po prenehanju izvajanja nalog se digitalno potrdilo deaktivira in onemogoči obnavljanje. Po prenehanju izvajanja nalog in ponovnem prevzemu funkcije operativnega osebja SIMoD-CA-Root je pred obnovo potrdila potrebno ponoviti postopek za pridobitev novega digitalnega potrdila in identifikacije v skladu s poglavjem 3.2.3 Preverjanje istovetnosti za fizične osebe.

Obnova digitalnega potrdila se samodejno izvrši pred pretekom veljavnosti digitalnega potrdila, kot je opisano v poglavju 4.7. Obnova digitalnih potrdil.

3.3.1.2. Preverjanje istovetnosti pri obnovi potrdil z uporabo PKCS#10 protokola

Samodejna obnova digitalnih potrdil,[4] izdanih podrejenim overiteljem z uporabo PKCS#10 protokola, ni možna. Potrebno je ponoviti postopek za pridobitev novega potrdila in identifikacije v skladu s poglavji 3.2.2 Preverjanje istovetnosti notranje organizacijske enote in institucije, ki je povezana z obrambo države in 3.2.3 Preverjanje istovetnosti za fizične osebe.

3.3.2. Preverjanje istovetnosti za obnovo digitalnega potrdila po preklicu

Obnova digitalnega potrdila po preklicu ni mogoča. Za ponovno pridobitev digitalnega potrdila po preklicu za podrejene overitelje in medsebojno priznane overitelje se izvede postopek za izdajo novega digitalnega potrdila in opravi identifikacijo kot ob prvi pridobitvi digitalnega potrdila v skladu s poglavji 3.2.2 Preverjanje istovetnosti notranje organizacijske enote in institucije, ki je povezana z obrambo države in 3.2.3 Preverjanje istovetnosti za fizične osebe.

[3] obnova potrdila ali podaljšanje veljavnosti potrdila ali podaljšanje veljavnosti potrdila ob rutinski zamenjavi ključev
[4] podrejenim overiteljem, izdajateljem časovnih žigov in medsebojno priznanim overiteljem

3.4. Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila

Oseba, ki želi preklicati digitalno potrdilo podrejenega overitelja ali medsebojno priznanega overitelja, se mora identificirati po enakem postopku kot pri prvi pridobitvi potrdila v skladu s poglavji 3.2.2 Preverjanje istovetnosti notranje organizacijske enote in institucije, ki je povezana z obrambo države, 3.2.3. Preverjanje istovetnosti za fizične osebe in 3.2.6 Merila za medsebojno povezovanje.

4. UPRAVLJANJE Z DIGITALNIMI POTRDILI

4.1. Prošnja za izdajo digitalnega potrdila

4.1.1. Kdo lahko zaprosi za izdajo digitalnega potrdila

SIMoD-CA-Root izda digitalno potrdilo podrejenemu overitelju ali medsebojno priznanemu overitelju le na predlog oziroma odobritev Sveta za upravljanje z infrastrukturo javnih ključev na MO.

SIMoD-CA-Root izda digitalno potrdilo operativnemu osebju po odobritvi Sveta za upravljanje z infrastrukturo javnih ključev na MO glede na dodeljene naloge v okviru SIMoD-CA-Root.

4.1.2. Postopek obdelave vloge in odgovornosti

Prosilec za izdajo digitalnega potrdila podrejenemu overitelju pošlje Svetu za upravljanje z infrastrukturo javnih ključev na MO prošnjo za izdajo digitalnega potrdila, ki mora vsebovati:

- obrazložitev, oziroma utemeljitev prošnje;
- Pravila delovanja overitelja, javni del;
- podatke o vodji notranje organizacijske enote MO, v okviru katere deluje podrejeni overitelj;
- podatke o osebi, ki bo v postopku izdaje digitalnega potrdila predala overitelju zahtevek z javnim ključem, za katerega se izdaja digitalno potrdilo;
- predlog razločevalnega imena digitalnega potrdila, če ni razviden iz pravil delovanja overitelja;
- predlog alternativnega imena digitalnega potrdila (po potrebi).

Svet za upravljanje z infrastrukturo javnih ključev na MO lahko po lastni presoji pred odobritvijo izdaje digitalnega potrdila od prosilca zahteva:

- kopijo ali vpogled v zaupni del pravil delovanja overitelja;
- kopijo poročila varnostnega pregleda infrastrukture.

Svet za upravljanje z infrastrukturo javnih ključev na MO v primeru odobritve izda operativnemu osebju SIMoD-CA-Root nalog za izdajo digitalnega potrdila, ki vsebuje dopis z odobritvijo, ter priloge:

- javni del pravil delovanja overitelja;
- podatke o vodji notranje organizacijske enote MO, v okviru katere deluje podrejeni overitelj;
- podatke o osebi, ki bo v postopku izdaje digitalnega potrdila predala overitelju zahtevek z javnim ključem,za katerega se izdaja digitalno potrdilo;
- predlog razločevalnega imena digitalnega potrdila, če ni razviden iz pravil delovanja overitelja;
- predlog alternativnega imena digitalnega potrdila (po potrebi).

4.2. Obdelava vloge za izdajo digitalnega potrdila

4.2.1. Postopki identifikacije in avtentikacije

Preverjanje identitete prosilca in pravilnosti podatkov izvaja Svet za upravljanje z infrastrukturo javnih ključev na MO v skladu s poglavji 3.2. Prva registracija. Odobrene prošnje posreduje operativnemu osebju SIMoD-CA-Root.

Operativno osebje overitelja ne izvaja nalog preverjanja identitete prosilca in pravilnosti podatkov ampak izvede le postopek izdaje digitalnega potrdila.

4.2.2. Odobritev ali zavrnitev izdaje digitalnega potrdila

Prošnja za izdajo digitalnega potrdila ne obvezuje k izdaji digitalnega potrdila.

Odobritev ali zavrnitev izdaje digitalnega potrdila je odgovornost in pravica Sveta za upravljanje z infrastrukturo javnih ključev na MO. Obvestilo o zavrnitvi ali odobritvi digitalnega potrdila pošlje Svet za upravljanje z infrastrukturo javnih ključev na MO prosilcu in operativnemu osebju SIMoD-CA-Root v pisni obliki.

4.2.3. Čas za obdelavo vloge za izdajo digitalnega potrdila

Najdaljši čas med oddajo prošnje za izdajo digitalnega potrdila Svetu za upravljanje z infrastrukturo javnih ključev na MO in izdajo obvestila o odobritvi ali zavrnitvi ni daljši od 21 dni. Prosilec ima po prejemu odobritve na voljo 30 dni, da izvede postopek generiranja para ključev ter predloži SIMoD-CA-Root zahtevek z javnim ključem, za katerega se izdaja digitalno potrdilo.

4.3. Izdaja digitalnega potrdila

4.3.1. Postopki overitelja SIMoD-CA-Root ob izdaji potrdil

Operativno osebje SIMoD-CA-Root začne s postopkom izdaje digitalnega potrdila po prejemu odobritve s strani Sveta za upravljanje z infrastrukturo javnih ključev na MO, in sicer:

- preveri identiteto osebe, ki v postopku izdaje digitalnega potrdila preda overitelju zahtevek z javnim ključem, za katerega se izdaja digitalno potrdilo in preveri ujemanje s podatki, vsebovanimi v odobritvi prejeti s strani Sveta za upravljanje z infrastrukturo javnih ključev na MO. Identiteta se preveri na osnovi vsaj dveh dokumentov, od katerih je eden uradni osebni dokument s sliko in eden službena izkaznica MO;
- preveri integriteto PKCS#10 zahtevka za izdajo digitalnega potrdila;
- preveri istovetnost podrejenega overitelja, ter primerja podatke s podatki v odobritvi;
- izda digitalno potrdilo, če so izpolnjeni vsi pogoji;
- zapiše digitalno potrdilo in vsebino ASN.1 strukture potrdila v berljivi obliki na trajni medij in ga preda osebi, ki je predala zahtevek.

SIMoD-CA-Root v zaupnem delu pravil pripravi formalni opis postopka ter vsebino zapisnika izdaje digitalnega potrdila.

4.3.1.1. Dostava zasebnega ključa imetniku

Ni relevantno. Podrejeni overitelji SIMoD-PKI sami generirajo zasebne ključe.

4.3.1.2. Dostava overiteljevega javnega ključa imetniku

Javni ključ overitelja SIMoD-CA-Root oziroma overiteljevo digitalno potrdilo, ki vsebuje overiteljev javni ključ, se izroči na trajnem mediju pooblaščeni osebi podrejenega overitelja hkrati z izdanim digitalnim potrdilom, ali na zahtevo. Medij vsebuje poleg digitalnega potrdila overitelja tudi odtis (angl. hash) overiteljevega potrdila ter izpis vsebine ASN.1 strukture overiteljevega potrdila v berljivi obliki.

Razen ob prevzemu svojega digitalnega potrdila se lahko overiteljevo digitalno potrdilo pridobi kadarkoli iz imenika, ob čemer se mora obvezno preveriti istovetnost overitelja SIMoD-CA-Root in celovitost digitalnega potrdila.

4.3.2. Obvestilo naročnikom o izdaji digitalnega potrdila

SIMoD-CA-Root pisno obvesti kontaktno osebo, navedeno v pravilih delovanja overitelja, ali drugo kontaktno osebo, če je bila navedena v prošnji za izdajo digitalnega potrdila.

4.4. Prevzem digitalnega potrdila

Prosilec prevzame digitalno potrdilo, kot je opisano v poglavju 4.3. Izdaja digitalnega potrdila.

4.4.1. Postopek potrditve prevzema digitalnega potrdila

Subjekt, kateremu je SIMoD-CA-Root izdal digitalno potrdilo, je dolžan preveriti istovetnost digitalnega potrdila na osnovi korenskega digitalnega potrdila overitelja SIMoD-CA-Root kot tudi vsebino digitalnega potrdila. S prvo uporabo, oziroma če subjekt 3 (tri) dni od prevzema digitalnega potrdila overitelja SIMoD-CA-Root ne obvesti o morebitnih napakah velja, da je subjekt potrdil točnost podatkov v digitalnem potrdilu in da prevzema tudi vse obveznosti in jamstva iz poglavja 9.6.3 Odgovornost in jamstva imetnikov digitalnih potrdil.

4.4.2. Objava digitalnega potrdila

Podrejeni overitelji so dolžni objaviti izdano digitalno potrdilo v repozitoriju v skladu z zahtevami Politike SIMoD-PKI in določili pravil delovanja posameznega podrejenega overitelja.

4.4.3. Obveščanje drugih udeležencev o izdaji digitalnega potrdila

Ni predvideno.

4.5. Uporaba ključev in digitalnih potrdil

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

4.5.1. Uporaba s strani imetnikov

4.5.1.1. Zasebni ključi in digitalna potrdila overiteljev

Overitelj SIMoD-CA-Root uporablja svoj zasebni ključ samo za podpisovanje:

- digitalnih potrdil neposredno podrejenim overiteljem;
- digitalnih potrdil medsebojno priznanih overiteljev, ki niso del infrastrukture javnih ključev na MO;
- registrov preklicanih potrdil ter
- digitalnih potrdil operativnega osebja overitelja SIMoD-CA-Root.

Overitelj SIMoD-CA-Root ne izdaja uporabniških digitalnih potrdil.

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

Operativno osebje overitelja SIMoD-CA-Root uporablja digitalna potrdila in pripadajoče ključe izključno za izvajanje nalog upravljanja z infrastrukturo overitelja. V primeru, da overiteljevi zaposleni potrebujejo ključe oz. digitalna potrdila kot uporabniki oz. za druge namene, kot je upravljanje z overiteljevo infrastrukturo, morajo zaprositi za izdajo uporabniškega digitalnega potrdila pri ustreznem podrejenem overitelju.

4.5.1.2. Zasebni ključi in digitalna potrdila prijavne službe

Ni relevantno. SIMoD-CA-Root nima vzpostavljene prijavne službe.

4.5.1.3. Imetniški zasebni ključi in digitalna potrdila

Podrejeni overitelji lahko uporabljajo zasebne ključe in digitalna potrdila v skladu z določili poglavja 4.5.1.1 Zasebni ključi in digitalna potrdila overiteljev.

SIMoD-CA-Root ne hrani zasebnih ključev podrejenih overiteljev.

4.5.2. Uporaba digitalnih potrdil s strani tretjih oseb

Pred uporabo digitalnega potrdila je tretja oseba dolžna preveriti ali je digitalno potrdilo ustrezno za predvideno uporabo. Tretja oseba lahko uporablja digitalno potrdilo le za namene, določene v Politiki SIMoD-PKI.

4.6. Obnova digitalnih potrdil brez spremembe javnega ključa

Obnova digitalnih potrdil brez spremembe javnega ključa v infrastrukturi javnih ključev na MO ni dovoljena.

4.7. Obnova[5] digitalnih potrdil

4.7.1. Okoliščine obnove digitalnih potrdil

Samodejna obnova digitalnih potrdil, izdanih podrejenim overiteljem, ni možna. Za obnovo je potrebno ponoviti postopke od 4.1. Prošnja za izdajo digitalnega potrdila do 4.4. Prevzem digitalnega potrdila.

Veljavnost digitalnih potrdil in pripadajočih zasebnih ključev je določena v poglavju 6.3.2 Obdobje veljavnosti ključev in digitalnih potrdil.

Za obnovo digitalnega potrdila po preklicu je potrebno ponoviti postopke od 4.1. Prošnja za izdajo digitalnega potrdila do 4.4. Prevzem digitalnega potrdila.

4.7.2. Kdo lahko zahteva obnovo digitalnega potrdila

Za obnovo digitalnega potrdila lahko zaprosijo 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 obnovo digitalnih potrdil

Obnova digitalnih potrdil izdanih podrejenim overiteljem poteka po istem postopku kot prevzem prvega potrdila (poglavja od 4.1. Prošnja za izdajo digitalnega potrdila do 4.4. Prevzem digitalnega potrdila).

Za obnovljena digitalna potrdila veljata Politika SIMoD-PKI in Javna pravila SIMoD-CA-Root, veljavna ob datumu izdaje obnovljenega digitalnega potrdila.

4.7.4. Obvestilo imetniku o izdaji novega digitalnega potrdila

Enako kot 4.3.2 Obvestilo naročnikom o izdaji digitalnega potrdila.

4.7.5. Postopek potrditve prevzema obnovljenega digitalnega potrdila

Enako kot 4.4.1 Postopek potrditve prevzema digitalnega potrdila.

4.7.6. Objava obnovljenega 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 digitalnih potrdil, izdanih podrejenim overiteljem zaradi spremembe podatkov vsebovanih v digitalnem potrdilu, ni možna. Vsaka sprememba vsebine digitalnega potrdila navedenih subjektov ima za posledico izdajo novega digitalnega potrdila in se izvede po istem postopku, kot prevzem prvega potrdila (poglavja od 4.1. Prošnja za izdajo digitalnega potrdila do 4.4. Prevzem digitalnega potrdila).

[5] obnova potrdila ali podaljšanje veljavnosti potrdila ali podaljšanje veljavnosti potrdila ob rutinski zamenjavi ključev

4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila

Poglavje opisuje okoliščine in postopke preklica digitalnih potrdil podrejenih overiteljev in digitalnih potrdil o priznavanju drugega overitelja. Preklic samopodpisanega potrdila overitelja SIMoD-CA-Root je opisan v poglavju 4.9.12 Posebne zahteve glede zlorabe ključa.

4.9.1. Okoliščine preklica

4.9.1.1. Okoliščine preklica imetniških digitalnih potrdil

Ni relevantno.

4.9.1.2. Okoliščine preklica potrdila o priznavanju drugega overitelja

V primeru medsebojnega priznavanja overitelj SIMoD-CA-Root prekliče potrdilo o priznavanju drugega overitelja iz naslednjih razlogov:

- dejanska ali domnevna zloraba zasebnih ključev drugega overitelja;
- spremembe podatkov o drugem overitelju, tako da je potrebno izdati novo potrdilo o priznavanju drugega overitelja;
- ob preklicu samopodpisanega potrdila drugega overitelja;
- v drugih primerih, določenih v pogodbi o medsebojnem priznavanju;
- neizpolnjevanje obvez iz pogodbe o medsebojnem priznavanju.

4.9.1.3. Okoliščine preklica potrdil podrejenih overiteljev

Vzroki za preklic digitalnih potrdil podrejenih overiteljev so:

- domnevna ali dejanska zloraba zasebnega ključa;
- nezmožnost pravočasne ponovne vzpostavitve delovanja po okvari oziroma nesreči (7 dni za storitve preklica digitalnih potrdil);
- odločitev inšpekcije;
- prenehanje delovanja podrejenega overitelja;
- preklic SIMoD-CA-Root potrdila;
- druge okoliščine, ki lahko ogrozijo zaupanje v overiteljevo potrdilo.

4.9.2. Kdo lahko zahteva preklic

4.9.2.1. Kdo lahko zahteva preklic imetniškega digitalnega potrdila

Ni relevantno.

4.9.2.2. Kdo lahko zahteva preklic potrdila o priznavanju drugega overitelja

V primeru medsebojnega priznavanja lahko preklic potrdila o priznavanju drugega overitelja zahteva:

- Svet za upravljanje z infrastrukturo javnih ključev na MO;
- drugi overitelj, za katerega je SIMoD-CA-Root izdal potrdilo o priznavanju.

4.9.2.3. Kdo lahko zahteva preklic potrdil podrejenih overiteljev

Preklic overiteljevega potrdila lahko zahteva:

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

4.9.3. Postopki za preklic

Ob preklicu digitalnega potrdila bo SIMoD-CA-Root objavil preklicano digitalno potrdilo v registru preklicanih potrdil. V primeru preklica digitalnega potrdila o priznavanju drugega overitelja bo preklicano digitalno potrdilo objavljeno v registru preklicanih potrdil in na spletni strani v okviru repozitorija overitelja.

Operativno osebje overitelja obvesti o preklicu po elektronski pošti ali s pošto z vročilnico odgovorno osebo podrejenega overitelja, v primeru medsebojnega priznavanja pa odgovorno osebo drugega overitelja.

Za izdajo novega digitalnega potrdila po preklicu je potrebno ponoviti postopek kot za izdajo prvega digitalnega potrdila, v skladu s poglavji 4.1. Prošnja za izdajo digitalnega potrdila do 4.4. Prevzem digitalnega potrdila.

V poglavjih 4.9.3.1 do 4.9.3.3 so opisani postopki preklica digitalnih potrdi.

4.9.3.1. Postopki preklica digitalnih potrdil imetnikov

Ni relevantno.

4.9.3.2. Postopki preklica potrdila o priznavanju drugega overitelja

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

Postopek za preklic digitalnega potrdila o priznavanju drugega overitelja je dogovorjen v pogodbi o medsebojnem priznavanju.

4.9.3.3. Postopki preklica potrdil podrejenih overiteljev

Zahtevek za preklic se lahko odda osebno ali pisno na kontaktni naslov naveden v poglavju 1.5.2 Kontaktna oseba.

Podrejeni overitelj je dolžan izvesti naslednje postopke:

- preklicati vsa veljavna digitalna potrdila;
- zagotoviti razpoložljivost registrov preklicanih potrdil vsaj še devetdeset (90) dni od preklica svojega potrdila;
- objaviti preklic potrdila v repozitoriju overitelja;
- ustvariti nove ključe overitelja;
- zaprositi za izdajo novega digitalnega potrdila;
- izdati imetnikom nova digitalna potrdila.

O preklicu digitalnega mora podrejeni overitelj takoj po elektronski pošti, če to ni mogoče pa telefonsko in pisno, obvestil:

- Svet za upravljanje z infrastrukturo javnih ključev na MO;
- celotno operativno osebje;
- vse imetnike oziroma odgovorne osebe;
- nadrejenega overitelja SIMoD-CA-Root.

4.9.4. Čas za posredovanje vloge za preklic

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

4.9.5. Čas od vloge za preklic do preklica

4.9.5.1. Čas za preklic imetniškega digitalnega potrdila

Ni relevantno.

4.9.5.2. Čas za preklic potrdila o priznavanju drugega overitelja

V primeru medsebojnega priznavanja overitelj SIMoD-CA-Root prekliče potrdilo o priznavanju drugega overitelja takoj, oziroma najkasneje v 8 urah, če so okoliščine preklica:

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

V primeru medsebojnega priznavanja overitelj SIMoD-CA-Root prekliče potrdilo o priznavanju drugega overitelja v roku 24 ur, če je okoliščina preklica sprememba podatkov o drugem overitelju, tako da je potrebno izdati novo potrdilo o priznavanju drugega overitelja.

24-urni rok velja za primere, ko je bila sprememba v času oddaje vloge že v veljavi. V primerih, ko je bila vloga oddana pred uveljavitvijo spremembe, ki pogojuje preklic digitalnega potrdila o medsebojnem priznavanju, se preklic opravi na dan uveljavitve spremembe, če je bila vloga oddana najmanj 24 ur pred uveljavitvijo spremembe, oziroma najkasneje v 24 urah po uveljavitvi spremembe, če je bila vloga podana manj kot 24 ur pred uveljavitvijo spremembe.

4.9.5.3. Čas za preklic potrdila podrejenega overitelja

Overitelj SIMoD-CA-Root prekliče digitalno potrdilo podrejenega overitelja takoj, ko prejme zahtevek, ali v roku, ki ga določi Svet za upravljanje z infrastrukturo javnih ključev na MO.

4.9.6. Obveza preverjanja registra preklicanih potrdil

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

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

V primeru, da tretja oseba ne more preveriti statusa digitalnega potrdila v registru preklicanih potrdil, je možnost, da:

- zavrne uporabo digitalnega potrdila in ne izvrši akcije;
- 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

Overitelj SIMoD-CA-Root objavlja nov register preklicanih potrdil vsaj na dvaindevetdeset (92) dni.

Ob preklicu digitalnega potrdila se izda in objavi nov register preklicanih potrdil takoj po izvedenem preklicu.

4.9.8. Dovoljene zakasnitve pri objavi registrov preklicanih potrdil

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

Overitelj SIMoD-CA-Root izda nov register preklicanih potrdil vsaj toliko časa pred iztekom veljavnosti starega, da je zagotovljen prenos registra do vseh komponent repozitorija še pred iztekom veljavnosti starega registra.

4.9.9. Storitev sprotnega preverjanje statusa digitalnih potrdil

Storitev (angl. 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

V primeru domnevne ali dejanske zlorabe zasebnega ključa korenskega overitelja SIMoD-CA-Root bo le ta izvedel naslednje postopke:

- preklical vsa digitalna potrdila;

- zagotavljal razpoložljivost registrov preklicanih potrdil vsaj še devetdeset (90) dni od preklica svojega samopodpisanega potrdila;
- objavil preklic potrdila v ustreznem registru preklicanih overiteljev;
- ustvaril nove ključe in generiral novo samopodpisano potrdilo;
- izdal podrejenim overiteljem in izdajateljem časovnih žigov nova digitalna potrdila.

SIMoD-CA-Root bo o preklicu samopodpisanega potrdila takoj po elektronski pošti, če to ni mogoče, pa telefonsko in pisno, obvestil:

- Svet za upravljanje z infrastrukturo javnih ključev na MO;
- celotno operativno osebje;
- vse imetnike oziroma odgovorne osebe;
- morebitne medsebojno priznane overitelje;
- podrejene overitelje;
- ministrstvo, pristojno za registracijo overiteljev v Republiki Sloveniji.

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 omejitev.

4.10. Storitve objavljanja statusa digitalnih potrdil

4.10.1.Tehnične lastnosti storitve

Status digitalnih potrdil je mogoče preveriti v registrih preklicanih potrdil, ki so dostopni v repozitoriju in na spletni strani iz poglavja 2.2. Objave informacij o digitalnih potrdilih. Naslov registra preklicanih potrdil je vključen v vsa digitalna potrdila, ki jih izda SIMoD-CA-Root in podrejeni overitelji SIMoD-PKI.

4.10.2.Razpoložljivost storitve

Razpoložljivost storitve je zagotovljena v skladu z določili v poglavju 2.1. Repozitoriji.

4.10.3.Dodatne možnosti

Niso na voljo.

4.11. Predčasna ukinitev veljavnosti digitalnih potrdil

Ni relevantno.

4.12. Postopki dela za varnostno kopiranje in odkrivanje zasebnega ključa

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

SIMoD-CA-Root zagotavlja varnostno kopiranje svojega zasebnega ključa (angl. Key backup) v skladu s poglavjem 6.2.4 Varnostno kopiranje zasebnih ključev.

4.12.1.Postopki povrnitve zgodovine ključev in odkrivanje kopije zasebnega ključa za dešifriranje

4.12.1.1. Povrnitev zgodovine ključev za dešifriranje

Ni relevantno. SIMoD-CA-Root ne izdaja digitalnih potrdil za šifriranje.

4.12.1.2. Odkrivanje kopije ključev za dešifriranje

Ni relevantno. SIMoD-CA-Root ne izdaja digitalnih potrdil za šifriranje.

4.12.2.Zaščita odkritega zasebnega ključa in postopek prenosa

Ni relevantno. SIMoD-CA-Root ne izdaja digitalnih potrdil za šifriranje.

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

5.1. Fizično varovanje

5.1.1. Lokacija in konstrukcija prostorov ter fizični dostop

Dejavnosti overitelja SIMoD-CA-Root se izvajajo v ustrezno varovanih prostorih in na varni lokaciji.

Prostori izpolnjujejo pogoje za namestitev komunikacijske in informacijske opreme ter arhivskih medijev skladno z Zakonom o tajnih podatkih in predpisih, sprejetih na njegovi podlagi. Komunikacijska in informacijska oprema overitelja SIMoD-CA-Root je nameščena v prostorih varnostnega območja II. stopnje.

5.1.2. Fizični dostop

Nadzor fizičnega dostopa izvaja pristojna služba MO.

Nadzor nad vstopom se izvaja z uporabo tehničnih sredstev, ki preprečujejo nepooblaščen vstop. Vstop je dovoljen samo operativnemu osebju overitelja SIMoD-CA-Root. Druge osebe, ki izkažejo upravičeni interes, smejo vstopiti v prostore samo v spremstvu operativnega osebja overitelja SIMoD-CA-Root.

Preden operativno osebje overitelja zapusti prostore overitelja, mora preveriti:

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

5.1.3. Napajanje in klimatske naprave

Overitelj SIMoD-CA-Root se aktivira samo po potrebi, oziroma v času operativnih posegov, zato posebni sistemi za napajanje in klimatska naprava nista potrebna.

5.1.4. Zaščita pred poplavo

Prostori s komunikacijsko in informacijsko opremo overitelja SIMoD-CA-Root se nahajajo na lokaciji, kjer je verjetnost poplave zelo majhna.

5.1.5. Zaščita pred ognjem

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

5.1.6. Shranjevanje medijev

Mediji z varnostnimi kopijami in arhiv podatkov stopnje tajnosti ZAUPNO in TAJNO so hranjeni v ustrezni protivlomni omari.

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

5.1.7. Odstranjevanje odpadkov

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

V primeru, da medijev ni mogoče varno izbrisati ali uničiti v prostorih overitelja SIMoD-CA-Root, 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-Root uporablja oddaljeno lokacijo za varno hranjenje varnostnih kopij in arhivskih podatkov. Podatki, mediji ali naprave so na oddaljeni lokaciji shranjeni v varovanih prostorih, ki zagotavljajo enako raven varnosti, kot je v prostorih overitelja SIMoD-CA-Root.

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-Root

5.2.1.1. Operativno osebje

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

- upravljanje z digitalnimi potrdili;
- upravljanje s programsko in strojno opremo overitelja SIMoD-CA-Root;
- varovanje in nadzor komunikacijskega sistema.

Da se izogne namernemu ali nenamernemu ogrožanju varnosti overitelja SIMoD-CA-Root, je posamezni operativni osebi dovoljeno opravljanje nalog samo znotraj ene zaključene organizacijske skupine. Posamezna oseba, ki izvaja naloge v okviru operativnega osebja overitelja SIMoD-CA-Root, lahko opravlja naloge tudi za druge overitelje SIMoD-PKI.

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

- prvi varnostni inženir;
- drugi varnostni inženir;
- administratorji potrdil.

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

- prvi administrator overitelja;
- administratorji overitelja.

V organizacijski skupini za varovanje in nadzor komunikacijskega sistema overitelja SIMoD-CA-Root so:

- prvi administrator komunikacijskega sistema;
- 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-Root.

5.2.1.2. Prijavna služba

Ni relevantno. SIMoD-CA-Root nima vzpostavljene prijavne službe.

5.2.1.3. Druge funkcije

Pristojne organizacijske enote v MO skrbijo za:

- fizično varovanje in nadzor prostorov overitelja SIMoD-CA-Root;
- 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-Root.

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-Root.

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-Root:

- generiranje kriptografskih ključev overitelja SIMoD-CA-Root;
- preklic overiteljevega potrdila;
- spreminjanje gesel aplikacije za delo z overiteljem SIMoD-CA-Root;
- 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;
- ukinitev obvezne prisotnosti vsaj dveh oseb za izvedbo zgoraj navedenih operacij.

Izvršitev katerekoli zgoraj navedene naloge mora odobriti prvi varnostni inženir.

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

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

5.2.3. Preverjanje istovetnosti operativnega osebja

Operativno osebje overitelja SIMoD-CA-Root izkaže svojo istovetnost:

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

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

- pripadati eni sami fizični osebi;
- 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-Root:

- mora biti ustrezno usposobljeno in o tem imeti dokazila;
- mora imeti za opravljanje nalog pri overitelju SIMoD-CA-Root imenovanje Sveta za upravljanje z infrastrukturo javnih ključev na MO;
- ne sme opravljati drugih nalog, ki bi bile v nasprotju z opravljanjem nalog v okviru infrastrukture javnih ključev na MO;

- mora imeti opravljanje nalog v okviru infrastrukture javnih ključev na MO navedene v sistemizaciji delovnega mesta;
- ne sme biti na prejšnjih podobnih dolžnostih (npr. skrbnik kriptografskih naprav, varnostni inženir v informacijskem sistemu) razrešeno nalog zaradi malomarnosti ali neizpolnjevanja obveznosti;
- mora imeti dovoljenje za dostop do tajnih podatkov najmanj TAJNO.

5.3.2. Dovoljenja za dostop do tajnih podatkov

V skladu z Zakonom o tajnih podatkih.

5.3.3. Usposabljanje osebja

5.3.3.1. Usposabljanje osebja overitelja

Operativno osebje overitelja SIMoD-CA-Root se redno usposablja na naslednjih področjih:

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

5.3.3.2. Usposabljanje osebja za pomoč uporabnikom

Ni relevantno.

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

5.3.7. Zunanji izvajalci

Zunanji izvajalci morajo za izvajanje posegov izpolnjevati vse pogoje, določene v Zakonu o tajnih podatkih oziroma implementacijo pravil na lokacijah overitelja.

5.3.8. Dokumentacija za osebje overitelja

Operativnemu osebju overitelja SIMoD-CA-Root so na voljo interni priročniki, originalna dokumentacija programske in strojne opreme ter priročniki šolanj, glede na njihovo funkcijo in načrt izobraževanja.

5.4. Postopki varnostnih pregledov sistema

Overitelj SIMoD-CA-Root ima vzpostavljen stalen nadzor svoje infrastrukture v okviru katerega se preverja:

- ali je infrastruktura fizično varna,
- ali vsi varnostni sistemi nemoteno delujejo,
- ali je prišlo do vdora nepooblaščenih oseb do overiteljeve opreme in podatkov.

5.4.1. Vrste beleženih dogodkov

Overitelj SIMoD-CA-Root beleži naslednje vrste dogodkov:

- dogodki na operacijskem sistemu, programski in strojni opremi overitelja SIMoD-CA-Root;
- dogodki v zvezi s ključi overitelja SIMoD-CA-Root;
- dogodki v zvezi z digitalnimi potrdili - izdaja, prevzem, obnova in preklic;
- dogodki v zvezi z varnostno politiko in upravljanjem informacijskega sistema overitelja SIMoD-CA-Root.

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

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

- dogodke v zvezi s fizičnim dostopom do sistemov overitelja SIMoD-CA-Root ter fizično lokacijo;
- kadrovske spremembe operativnega osebja overitelja SIMoD-CA-Root;
- dogodke, povezane z uničevanjem občutljivega materiala (na primer kriptografskega materiala oziroma ključev in nosilcev ključev, osebnih identifikacijskih podatkov uporabljenih v postopkih preverjanja identitete prosilcev za izdajo digitalnega potrdila).

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

5.4.2. Pogostost pregleda dnevnikov beleženih dogodkov

Operativno osebje overitelja SIMoD-CA-Root pregleduje dnevnike beleženih dogodkov ob vsakem zagonu sistema. Pregled vključuje:

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

Operativno osebje overitelja SIMoD-CA-Root izvaja redne preglede beleženih dogodkov in sicer najmanj enkrat letno. Redni pregled vključuje:

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

5.4.3. Obdobje hranjenja dnevnikov beleženih dogodkov

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

5.4.4. Zaščita dnevnikov beleženih dogodkov

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

Dostop do dnevnikov beleženih dogodkov je dovoljen samo pooblaščenim osebam:

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

Za dnevnike na operacijskem sistemu so uporabljene zaščite, kot jih le-ta dopušča. 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, ki se zbirajo v elektronski obliki, se izdeluje v okviru rednega varnostnega kopiranja sistemov. Ob izdelavi varnostne kopije se en izvod varnostne kopije dnevnikov v elektronski obliki in dnevnikov, ki se vodijo na papirju prenese na oddaljeno lokacijo, kot določeno v 5.1.8 Hranjenje na oddaljeni lokaciji.

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 tem ni treba obvestiti.

5.4.8. Ocena in odprava ranljivosti

Dnevnike beleženih dogodkov pregleduje operativno osebje overitelja 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-Root hrani naslednje podatke:

- dnevnike beleženih dogodkov iz poglavja 5.4.1 Vrste beleženih dogodkov;
- odobritve Sveta za upravljanje z infrastrukturo javnih ključev na MO o izdaji digitalnih potrdil in spremljajoče dokumente;
- dokumentacijo o izvedbi postopka izdaje digitalnih potrdil;
- korespondenco s subjekti, katerim je overitelj SIMoD-CA-Root izdal digitalno potrdilo;
- digitalna potrdila in liste preklicanih potrdil;
- verzije pravil delovanja overitelja SIMoD-CA-Root, tako javnih kot tudi zaupnih delov;
- zasebne dešifrirne ključe v skladu s poglavjem 6.2.4 Varnostno kopiranje zasebnih ključev.

5.5.2. Obdobje hranjenja arhiva

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

Overitelj SIMoD-CA-Root hrani odobritve Sveta za upravljanje z infrastrukturo javnih ključev na MO o izdaji digitalnih potrdil in spremljajoče dokumente, korespondenco s subjekti, katerim je overitelj izdal digitalno potrdilo najmanj pet (5) let od zaključka zadeve, ki je vezana na odobritve Sveta za upravljanje z infrastrukturo javnih ključev na MO, korespondenco ali pogodbo, oziroma od zadnjega dne veljavnosti digitalnega potrdila, ki je povezano s hranjenim dokumentom.

Digitalna potrdila se hranijo vsaj pet (5) let po preteku veljavnosti zadnjega digitalnega potrdila izdanega subjektu.

5.5.3. Zaščita arhiva

Podatki, ki sodijo v dokumentarno gradivo (odobritve Sveta za upravljanje z infrastrukturo javnih ključev na MO o izdaji digitalnih potrdil in spremljajoči dokumenti, dokumentacija o izvedbi postopka izdaje digitalnih potrdil, korespondenca s subjekti, katerim je overitelj SIMoD-CA-Root izdal digitalno potrdilo in verzije pravil delovanja overitelja SIMoD-CA-Root, tako javni kot tudi zaupni deli), se hranijo in arhivirajo v skladu s postopki dela z dokumentarnim gradivom na MO.

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-Root.

5.5.4. Varnostna kopija arhiva

Podatkom, ki sodijo v dokumentarno gradivo (odobritve Sveta za upravljanje z infrastrukturo javnih ključev na MO o izdaji digitalnih potrdil in spremljajoči dokumenti, dokumentacija o izvedbi postopka izdaje digitalnih potrdil, korespondenca s subjekti, katerim je overitelj

SIMoD-CA-Root izdal digitalno potrdilo in verzije pravil delovanja overitelja SIMoD-CA-Root, tako javni kot tudi zaupni deli), se zagotavlja razpoložljivost v skladu s postopki dela z dokumentarnim gradivom na MO.

Ob izdelavi arhiva podatkov, ki se beležijo v okviru informacijskega sistema (avtomatsko generirani dnevniki beleženih dogodkov, digitalna potrdila in liste preklicanih potrdil) 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-Root v okviru svojih delovnih nalog,
- inšpektorju.

Postopek priprave arhivskih podatkov je del zaupnega dela pravil delovanja overitelja SIMoD-CA-Root.

5.6. Obnova digitalnih potrdil overiteljev

5.6.1. Obnova samopodpisanega potrdila korenskega overitelja SIMoD-CA-Root

Veljavnost samopodpisanega SIMoD-CA-Root korenskega potrdila overitelja SIMoD-CA-Root je vedno daljša, kot je veljavnost kateregakoli izdanega digitalnega potrdila, 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-Root se vedno uporablja krajše obdobje kot je veljavnost pripadajočega overiteljevega potrdila.

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

Če ob zamenjavi overiteljevega para ključev ne bo objavljeno drugače, ostaneta v veljavi Politika SIMoD-PKI in Pravila delovanja SIMoD-CA-Root.

Obnova digitalnega potrdila overitelja SIMoD-CA-Root se izvede po formalnem, podrobno predpisanem in nadzorovanem postopku. Posamezne korake postopka izvaja operativno osebje overitelja SIMoD-CA-Root. Poleg operativnega osebja overitelja SIMoD-CA-Root so prisotne tudi zaupanja vredne priče, ki nadzorujejo izvajanje postopka. Postopek je podrobno opisan v zaupnem delu pravilih delovanja overitelja SIMoD-CA-Root. Izvedba postopka je podrobno dokumentirana v zapisniku, ki ga podpišejo vsi prisotni.

Tretje osebe prejmejo nov overiteljev javni ključ v obliki digitalnega potrdila, kot je določeno v 6.1.4 Dostava overiteljevega javnega ključa tretjim osebam.

5.6.2. Obnova potrdil podrejenih overiteljev v SIMoD-PKI

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

Za podpisovanje digitalnih potrdil se vedno uporablja najnovejši overiteljev zasebni ključ. Za preverjanje veljavnosti digitalnih potrdil pa se uporablja predhodno overiteljevo potrdilo vse dokler ne poteče veljavnost zadnjega digitalnega potrdila, podpisanega s starim zasebnim

overiteljevim ključem. Zasebni ključ overitelja se vedno uporablja krajše obdobje kot je veljavnost pripadajočega overiteljevega potrdila.

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

Obnova digitalnih potrdil podrejenih overiteljev se izvede po formalnem, podrobno predpisanem in nadzorovanem postopku. Posamezne korake postopka izvaja operativno osebje SIMoD-CA-Root overitelja in podrejenega overitelja. Poleg operativnega osebja overiteljev so prisotne tudi zaupanja vredne priče, ki nadzorujejo izvajanje postopka. Postopek je podrobno opisan v zaupnem delu pravil delovanja overitelja SIMoD-CA-Root in podrejenih overiteljev. Izvedba postopka je podrobno dokumentirana v zapisniku, ki ga podpišejo vsi prisotni.

Tretje osebe prejmejo nov overiteljev javni ključ v obliki digitalnega potrdila, kot je določeno v 6.1.4 Dostava overiteljevega javnega ključa tretjim osebam.

5.7. Zagotavljanje kontinuitete delovanja ob okvarah, nesrečah ali zlorabi zasebnega ključa overitelja

5.7.1. Postopki v primeru okvar in zlorab

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

5.7.2. Uničenje programske, strojne opreme ali podatkov overitelja

V primeru okvare strojne ali programske opreme oziroma podatkov, pri kateri zasebni ključ overitelja ni bil uničen, bodo storitve overitelja vzpostavljene nazaj v najkrajšem možnem času. Overitelj bo v najkrajšem možnem času vzpostavil vsaj funkcionalnost preklicevanja digitalnih potrdil in objavljanja registra preklicanih potrdil. Skrajni rok za vzpostavitev storitve preklicevanja digitalnih potrdil in objavljanja registra preklicanih potrdil je en teden (7 dni). Po tem roku bo overitelj objavil preklic svojega potrdila in ukrepal v skladu s poglavji 4.9.12 Posebne zahteve glede zlorabe ključa in 4.9.3.3 Postopki preklica potrdil podrejenih overiteljev.

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 poglavji 4.9.12 Posebne zahteve glede zlorabe ključa in 4.9.3.3 Postopki preklica potrdil podrejenih overiteljev. 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

5.7.3.1. Postopki ob zlorabi zasebnega ključa podrejenega overitelja

Postopki ob zlorabi zasebnega ključa overitelja so predpisani v poglavju 4.9.3.3 Postopki preklica potrdil podrejenih overiteljev.

5.7.3.2. Postopki ob zlorabi zasebnega ključa korenskega overitelja

Postopki ob zlorabi zasebnega ključa korenskega overitelja SIMoD-CA-Root so predpisani v poglavju 4.9.12 Posebne zahteve glede zlorabe ključa.

5.7.4. Naravne in druge nesreče

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

5.8. Prenehanje delovanja overitelja

Vzroki za prenehanje delovanja overitelja so podani v poglavju 4.9.1.3 Okoliščine preklica potrdil podrejenih overiteljev oziroma 4.9.12 Posebne zahteve glede zlorabe ključa. Odločitev o prenehanju delovanja izda Svet za upravljanje z infrastrukturo javnih ključev na MO.

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

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

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

Overitelj bo izvedel naslednje postopke:

- preklical vsa digitalna potrdila;
- zagotavljal razpoložljivost registrov preklicanih potrdil vsaj še devetdeset (90) dni od preklica svojega samopodpisanega potrdila;
- objavil preklic potrdila v ustreznem registru preklicanih overiteljev.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev para ključev

6.1.1. Generiranje para ključev

Ključi overitelja SIMoD-CA-Root se generirajo po formalnem, podrobno predpisanem in nadzorovanem postopku. Posamezne korake postopka izvaja operativno osebje overitelja SIMoD-CA-Root. Poleg operativnega osebja overitelja SIMoD-CA-Root so prisotne tudi zaupanja vredne priče, ki nadzorujejo izvajanje postopka. Postopek je podrobno opisan v zaupnem delu pravil delovanja overitelja SIMoD-CA-Root. Izvedba postopka se podrobno dokumentira v zapisniku, ki ga podpišejo vsi prisotni.

Par ključev podrejenih overiteljev se vedno generira pri podrejenem overitelju v ustreznem varnostnem kriptografskem modulu in pod njegovo izključno kontrolo.

6.1.2. Dostava zasebnega ključa imetniku

Ni relevantno. SIMoD-CA-Root ne generira zasebnih ključev subjektov, katerim izdaja digitalna potrdila.

6.1.3. Dostava imetnikovega javnega ključa overitelju

Ni relevantno.

6.1.4. Dostava overiteljevega javnega ključa tretjim osebam

Javni ključ overitelja 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 pridobijo tudi kadarkoli iz imenika ali na spletnih straneh (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 podrejenih overiteljev v SIMoD-PKI je 2048 bitov.

6.1.6. Parametri za generiranje javnih ključev in preverjanje parametrov

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

6.1.7. Namen uporabe ključev

Namen uporabe ključev oziroma digitalnih potrdil je določen v razširitvenem polju *keyUsage* in *extKeyUsage*. Uporaba polja *keyUsage* in *extKeyUsage* je predpisana v priporočilu X.509 v.3 oziroma RFC 3280.

Za podpisovanje digitalnih potrdil in registrov preklicanih potrdil se uporabljajo samo zasebni ključi SIMoD-CA-Root in podrejenih overiteljev SIMoD-PKI.

Dovoljene vrednosti razširitvenega polja za digitalna potrdila overiteljev so:

- KeyCertSign;
- CRLSign.

6.2. Zaščita zasebnih ključev in tehnične kontrole kriptografskih modulov

6.2.1. Standardi za kriptografski modul

Generiranje SIMoD-CA-Root overiteljevih parov kriptografskih ključev za podpisovanje digitalnih potrdil se izvaja v strojnem varnostnem kriptografskem modulu, ki ima potrdilo o skladnosti s FIPS 140-2 Level 3.

Podrejeni overitelji so dolžni za generiranje kriptografskih parov ključev za podpisovanje digitalnih potrdil uporabljati strojne varnostne kriptografske module, ki imajo potrdilo o skladnosti z enim od sledečih standardov:

- FIPS 140-1 ali FIPS 140-2 Level 3 ali višji;
- CEN CWA 14167-2, 14167-3 ali 14167-4;
- ISO/IEC 15408 Level EAL4 ali višji.

6.2.1.1. Kriptografski moduli izdajateljev časovnega žiga

Ni relevantno.

6.2.1.2. Pametne kartice za uporabniška digitalna potrdila

Overitelj SIMoD-CA-Root ne izdaja digitalnih potrdil končnim uporabnikom.

Operativno osebje overitelja SIMoD-CA-Root uporablja pametne kartice ali podobne nosilce ključev stopnje varnosti FIPS 140-2 level 2.

6.2.1.3. Programsko hranjenje zasebnih ključev

Ni relevantno. Overitelj SIMoD-CA-Root ne izdaja digitalnih potrdil za ključe, ki se hranijo v programskih modulih.

6.2.2. Nadzor zasebnega ključa overitelja z več pooblaščenimi osebami

Za operacije, kjer se upravlja z zasebnim ključem overitelja SIMoD-CA-Root oziroma za upravljanje z varnostnim kriptografskim modulom, je vedno potrebna prisotnost in odobritev vsaj dveh oseb z ustreznimi pooblastili, ki izkažeta svojo istovetnost s pametno kartico s porazdeljenim ključem kriptografskega modula in skrivnim geslom kartice.

6.2.3. Odkrivanje zasebnega ključa

Odkrivanje zasebnega ključa SIMoD-CA-Root overitelja ni možno. Tehnična izvedba varnostnega kriptografskega modula ne omogoča prikaza zasebnega ključa v nešifrirani obliki.

Odkrivanje zasebnega ključa podrejenih overiteljev ni dovoljeno.

6.2.4. Varnostno kopiranje zasebnih ključev

Varnostna kopija zasebnega ključa overitelja SIMoD-CA-Root se zagotavlja z varnostnimi mehanizmi varnostnega kriptografskega modula. Varnostna kopija je zaščitena s šifriranjem pred izvozom iz varnostnega kriptografskega modula. Dešifrirni ključ je porazdeljen na N[6] od M[7] administratorskih pametnih karticah varnostnega kriptografskega modula.

SIMoD-CA-Root ne hrani kopij zasebnih ključev podrejenih overiteljev, katerim je izdal digitalna potrdila.

6.2.5. Arhiviranje zasebnega ključa

Zasebni ključ overitelja SIMoD-CA-Root se ne arhivira.

[6] N mora biti večje ali enako 2
[7] M mora biti večje ali enako 3

6.2.6. Zapis zasebnega ključa v kriptografski modul in iz njega

Overiteljev zasebni ključ je generiran v varnostnem kriptografskem modulu. Tehnična izvedba varnostnega kriptografskega modula ne omogoča izvoza in prikaza zasebnega ključa overitelja v nešifrirani obliki.

6.2.7. Hranjenje zasebnega ključev v kriptografskem modulu

Zasebni ključi overitelja SIMoD-CA-Root so hranjeni na varnostnem kriptografskem modulu in v varnostni kopiji na disku v šifrirani obliki in se nikdar ne pojavijo izven modula v nešifrirani obliki.

Zasebni ključi podrejenih overiteljev se morajo hraniti na varnostnem kriptografskem modulu, ali v varnostni kopiji v šifrirani obliki in se nikdar ne smejo pojaviti izven modula v nešifrirani obliki.

6.2.8. Postopek za aktiviranje zasebnega ključa

Zasebni ključ overitelja SIMoD-CA-Root se aktivira ob zagonu overiteljeve aplikativne programske opreme. Za aktiviranje je potrebno predložiti operatersko pametno kartico varnostnega kriptografskega modula ter geslo administratorja overitelja.

6.2.9. Postopek za deaktiviranje zasebnega ključa

Zasebni ključ overitelja se deaktivira z zaustavitvijo aplikativne programske opreme overitelja SIMoD-CA-Root.

6.2.10. Postopek za uničenje zasebnega ključa

Zasebni ključi overitelja SIMoD-CA-Root se uničijo, ko jim poteče obdobje uporabe oziroma se ne uporabljajo več iz drugih razlogov. Ob uničenju ključev se uničijo aktivne kopije na varnostnem kriptografskem modulu in vse varnostne kopije.

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

6.2.11. Stopnja varnosti kriptografskih modulov

Opisano v poglavju 6.2.1 Standardi za kriptografski modul.

6.3. Ostali vidiki upravljanja s pari ključev

6.3.1. Arhiviranje javnega ključa

Overitelj SIMoD-CA-Root arhivira svoj javni ključ za verifikacijo podpisa in izdana digitalna potrdila kot del arhiviranja digitalnih potrdil (glej poglavje 5.5. Arhiviranje podatkov).

6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil

Veljavnost javnih in zasebnih ključev overiteljev:

Vrsta potrdila	Ključ	Veljavnost
SIMoD-CA-Root	zasebni	šest (6) let
	javni	dvanajst (12) let
podrejeni overitelji SIMoD-PKI	zasebni	tri (3) leta
	javni	šest (6) let

Obnova digitalnih potrdil, ki je povezana z veljavnostjo ključev, je opisana v poglavju 4.7. Obnova digitalnih potrdil in 5.6. Obnova digitalnih potrdil overiteljev.

6.4. Aktivacijski podatki

6.4.1. Generiranje in instalacija aktivacijskih podatkov

Ni relevantno.

6.4.1.1. Aktivacija pametnih kartic

Operativno osebje potrebuje za aktiviranje pametne kartice geslo, oziroma PIN kodo, ki jo določi samo.

6.4.1.2. Začetna aktivacija pametnih kartic

Za začetno aktiviranje pametnih kartic operativnega osebja niso potrebni nobeni aktivacijski podatki.

6.4.2. Zaščita aktivacijskih podatkov

Ni relevantno.

6.4.3. Drugi vidiki aktivacijskih podatkov

Ni relevantno.

6.5. Varnostne zahteve za računalnike

6.5.1. Specifične tehnične varnostne zahteve za računalnike

Overitelj SIMoD-CA-Root ima v sistemski in aplikativni programski opremi overitelja implementirane tehnične varnostne kontrole, ki vključujejo:

- kontrolo dostopa do overiteljevih storitev;
- delitev nalog med operativnim osebjem overitelja SIMoD-CA-Root;
- preverjanje istovetnosti operativnega osebja overitelja SIMoD-CA-Root;
- šifriranje zaupnih podatkov v bazi overitelja SIMoD-CA-Root;
- varnostne beležke vseh varnostno relevantnih dogodkov;
- varen arhiv in varno hranjenje varnostnih beležk;
- vzpostavljene mehanizme restavriranja sistema, ključev overitelja SIMoD-CA-Root ter baze podatkov overitelja SIMoD-CA-Root.

6.5.2. Raven varnostne zaščite računalnikov

Informacijski sistem overitelja SIMoD-CA-Root za upravljanje z digitalnimi potrdili dosega raven varnostne zaščite računalnikov vsaj EAL 3.

6.6. Tehnični nadzor življenjskega cikla overitelja

6.6.1. Nadzor razvoja sistema

Strojna oprema, operacijski sistem ter programska oprema overitelja SIMoD-CA-Root so komercialni proizvodi.

6.6.2. Upravljanje varnosti

Overitelj SIMoD-CA-Root evidentira postopke inštalacije, sprememb konfiguracije in nadgradnje za vse komponente infrastrukture.

Operativno osebje overitelja SIMoD-CA-Root 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 koda programske opreme overitelja SIMoD-CA-Root 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 komunikacijsko informacijskih sistemov overitelja SIMoD-CA-Root, oziroma upravljanje varnosti skozi celoten življenjski cikel je v skladu z 6.6.2 Upravljanje varnosti.

6.7. Varnostne kontrole na ravni računalniškega omrežja

Korenski overitelj SIMoD-CA-Root ni povezan v nobeno računalniško omrežje.

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-Root izdaja digitalna potrdila X.509 Version 3 v skladu s priporočili RFC3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Digitalno potrdilo overitelja SIMoD-CA-Root in digitalna potrdila podrejenih overiteljev vsebujejo naslednja osnovna polja:

Polje (Field)	Potrdilo overitelja SOMoD-CA-Root	Potrdilo podrejenega overitelja
X.509 verzija (Version)	2 (kar pomeni verzijo 3)	2 (kar pomeni verzijo 3)
Serijska številka (Serial Number)	Enolična serijska številka na nivoju SIMoD-CA-Root	Enolična serijska številka na nivoju SIMoD-CA-Root
Overiteljev podpis (Signature)	sha1WithRSAEncryption	sha1WithRSAEncryption
Overitelj (Issuer)	razločevalno ime SIMoD-CA-Root	razločevalno ime SIMoD-CA-Root
Obdobje veljavnosti (Validity)	dvanajst (12) let <pričetek veljavnosti po GMT> <konec veljavnosti po GMT>	šest (6) let <pričetek veljavnosti po GMT> <konec veljavnosti po GMT>
Imetnik (Subject)	razločevalno ime SIMoD-CA-Root	razločevalno ime podrejenega overitelja
Algoritem za javni ključ (Subject Public Key Information)	rsaEncryption	rsaEncryption

7.1.2. Razširitvena polja

Razširitvena polja so namenjena uporabi dodatnih atributov v X.509v3 potrdilih. Overitelj SIMoD-CA-Root izdaja digitalna potrdila, ki vsebujejo standardna razširitvena polja v skladu s priporočili RFC 3280. Polja vsebovana v digitalnih potrdilih, ter vsebina polj so podani v spodnji tabeli. Polja definirana v RFC 3280, ki niso navedena v tabelah, se ne uporabljajo.

Digitalno potrdilo korenskega overitelja SIMoD-CA-Root in digitalna potrdila podrejenih overiteljev vsebujejo naslednja razširitvena polja:

Polje (Field)	Potrdilo overitelja SOMoD-CA-Root	Potrdilo podrejenega overitelja
odtis javnega ključa overitelja (authority Key Identifier)	Ni uporabljeno	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Root,s katerim je podpisano potrdilo
odtis imetnikovega javnega ključa (subject Key Identifier)	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Root	SHA-1 odtis javnega ključa podrejenega overitelja
namen uporabe ključa (key Usage)	**Kritično** keyCertSign cRLSign	**Kritično** keyCertSign cRLSign
razširjen namen uporabe (extended Key Usage)	Ni uporabljeno	Ni uporabljeno
obdobje veljavnosti zasebnega ključa (privateKeyUsagePeriod)	šest (6) let <pričetek veljavnosti po GMT> <konec veljavnosti po GMT>	tri (3) leta <pričetek veljavnosti po GMT> <konec veljavnosti po GMT>
OID oznaka tipa potrdila (certificate Policies)	Ni uporabljeno	Ni uporabljeno
naslovi registra preklicanih potrdil (CRL Distribution Points)	Ni uporabljeno	LDAP in http URL naslov registra preklicanih potrdil podrejenega overitelja
Alternativno ime imetnika (subject Alternative Name)	Ni uporabljeno	Ni uporabljeno
Osnovne omejitve (basicConstraint)	**Kritično** CA =: True pathLenConstraint = 1	**Kritično** CA =: True pathLenConstraint = 0

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

7.1.3. Identifikacijske oznake algoritmov

Kriptografska algoritma, uporabljena v digitalnih potrdilih, imata naslednji identifikacijski oznaki:

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.

Upravitelj imenika lahko določi dodatne omejitve glede imen.

7.1.6. Identifikacijska oznaka politik

Vsako digitalno potrdilo, ki ga izda overitelj v okviru infrastrukture javnih ključev na MO, vsebuje eno samo identifikacijsko oznako politike.

7.1.7. Način uporabe razširitvenega polja za omejitev uporabe politik

Z namenom, 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

Politika SIMoD-PKI ne predvideva uporabe razširitvenega polja za specifične podatke *Policy Qualifiers extension* za objavo spletnega naslova, kjer bi bila objavljena politika oziroma druge informacije za uporabnike.

Politika SIMoD-PKI uporablja polje *UserNotice* za objavo omejitve odgovornosti z naslednjim besedilom: *"Uporaba potrdil omejena na namene, definirane v Politiki SIMoD-PKI."*

7.1.9. Procesiranje oznake kritičnosti razširitvenih polj

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

7.2. Profil registrov preklicanih potrdil

7.2.1. Verzija registrov preklicanih potrdil

Registri preklicanih potrdil so v skladu s priporočili RFC 3280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, verzija 2.

Registri preklicanih potrdil vsebujejo naslednja osnovna polja:

Osnovno polje - angleški naziv	Osnovno polje - slovenski opis	Vrednost
Version	verzija	v2
Signature	overiteljev podpis registra	<podpis registra s strani overitelja SIMoD-CA_Root>
Issuer	izdajatelj	<razločevalno ime SIMoD-CA-Root>
thisUpdate	čas izdaje registra	<čas izdaje po GMT>
nextUpdate	čas izdaje naslednjega registra	<čas naslednje izdaje po GMT>
revokedCertificate	serijske številke preklicanih potrdil	<serijske številke preklicanih potrdil>

7.2.2. Razširitvena polja registrov preklicanih potrdil

Uporabniške aplikacije morajo pravilno procesirati razširitvena polja po priporočilu RFC3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, ki so podana v naslednji tabeli:

Razširitveno polje - angleški naziv	Razširitveno polje - slovenski opis	Vrednost
CRLNumber	serijska številka registra	<serijska številka registra>
reasonCode		se ne uporablja
holdInstructionCode		se ne uporablja
invalidityDate	predviden čas kompromitiranja ključa	<čas po GMT>
issuingDistributionPoint		ker imenik ni edini način za pridobitev CRL-ja, se ne uporablja

certificateIssuer		se ne uporablja
deltaCRLIndicator		se ne uporablja

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

Inšpekcijski nadzor preverja skladnost delovanja overitelja SIMoD-CA-Root v okviru infrastrukture javnih ključev na MO z Zakonom o elektronskem poslovanju in elektronskem podpisu in Politiko SIMoD-PKI.

Svet za upravljanje z infrastrukturo javnih ključev na MO ob nameri medsebojnega priznavanja z drugimi overitelji zagotovi drugim overiteljem jamstva, da overitelj SIMoD-CA-Root izpolnjuje zahteve iz Politike SIMoD-PKI ter zahteva od drugih overiteljev enako potrdilo, 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.

8.1. Pogostost inšpekcije

Inšpekcijski nadzor skladnosti delovanja z Zakonom o elektronskem poslovanju in elektronskem podpisu se preverja skladno z zakonodajo Republike Slovenije.

Skladnost delovanja s Politiko SIMoD-PKI se izvede pred pričetkom delovanja overitelja SIMoD-CA-Root in vsaj enkrat letno.

Svet za upravljanje z infrastrukturo javnih ključev na MO lahko za izvedbo inšpekcijskega nadzora pooblasti zunanjo inšpekcijsko službo oziroma organizacijo z ustreznim znanjem in izkušnjami s področja infrastrukture javnih ključev. V ta namen določena zunanja inšpekcijska služba preverja samo skladnost s Politiko SIMoD-PKI.

8.2. Pogoji za inšpektorja

Izvajalec inšpekcijskega nadzora mora imeti ustrezno dovoljenje za dostop do tajnih podatkov. Kadar se inšpekcijski nadzor izvaja nad delovanjem celotnega sistema overitelja SIMoD-CA-Root, je potrebno dovoljenje stopnje TAJNO.

8.3. Relacija med inšpektorjem in overiteljem SIMoD-CA-Root

Inšpektor mora biti neodvisen od infrastrukture javnih ključev na MO.

8.4. Področja inšpekcije

Inšpekcijski nadzor preverja skladnost delovanja overitelja SIMoD-CA-Root z Zakonom o elektronskem poslovanju in elektronskem podpisu in Politiko SIMoD-PKI.

8.5. Postopki po opravljeni inšpekciji

V primeru ugotovljenih nepravilnosti bo operativno osebje SIMoD-CA-Root pripravilo 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-Root 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-Root do naslednje predvidene inšpekcije ali
- pred preklicem overiteljevega potrdila dodeli overitelju SIMoD-CA-Root 30 dni za odpravo pomanjkljivosti, v tem času dovoli overitelju delovanje ali
- ukaže preklic overiteljevega potrdila.

8.6. Prejemniki ugotovitev o inšpekciji

Ugotovitve inšpekcijskega nadzora mora inšpektor poslati Svetu za upravljanje z infrastrukturo javnih ključev na MO in operativnemu osebju overitelja SIMoD-CA-Root.

Overitelj SIMoD-CA-Root se na osnovi ugotovitev inšpektorja odloči, ali je potrebno obvestiti imetnike in tretje stran. Obvestilo imetnikom in tretjim stranem objavi v skladu s poglavjem 9.11. Obvestila in komuniciranje z udeleženci.

Način in podrobnosti o izmenjavi 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. Ob izdaji in obnovi digitalnega potrdila

Ni predpisano.

9.1.2. Ob dostopu do digitalnega potrdila

Ni predpisano.

9.1.3. Ob preverjanju preklicanosti oziroma statusa potrdila

Ni predpisano.

9.1.4. Druge storitve

Ni predpisano.

9.1.5. Povračilo stroškov

Ni predpisano.

9.2. Finančna odgovornost

9.2.1. Zavarovanje odgovornosti

Ministrstvo za obrambo ima glede delovanja overiteljev infrastrukture javnih ključev na MO ustrezno zavarovano svojo odgovornost po Zakonu o elektronskem poslovanju in elektronskem podpisu ter Uredbi 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

Ni predpisano.

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-Root pridobi osebne podatke v postopku preverjanja prošenj za izdajo digitalnega potrdila, ki ga izvede Svet za upravljanje z infrastrukturo javnih ključev na MO. Pridobljeni podatki se uporabljajo izključno za potrebe izdaje in upravljanja digitalnih potrdil. Osebni podatki se hranijo v overiteljevem arhivu v skladu z Zakonom o varstvu osebnih podatkov Republike Slovenije.

9.4.2. Obseg osebnih podatkov, ki se obravnavajo kot zaupni

Kot osebni podatki se obravnavajo podatki določeni v Zakonu o varstvu osebnih podatkov Republike Slovenije.

9.4.3. Osebni podatki, ki se ne obravnavajo kot zaupni

Podatki, objavljeni v digitalnem potrdilu in repozitoriju overiteljev, se ne obravnavajo kot zaupni.

9.4.4. Odgovornost glede varovanja osebnih podatkov

Za varovanje osebnih podatkov v skladu z Zakonom o varstvu osebnih podatkov Republike Slovenije so odgovorni subjekti pristojni za preverjanje istovetnosti določeni v poglavjih 3.2.2 Preverjanje istovetnosti notranje organizacijske enote in institucije, ki je povezana z obrambo države in 3.2.3 Preverjanje istovetnosti za fizične osebe.

9.4.5. Dovoljenje za uporabo osebnih podatkov

Svet za upravljanje z infrastrukturo javnih ključev na MO mora od prosilcev za izdajo digitalnega potrdila podrejenim overiteljem in operativnega osebja overitelja SIMoD-CA-Root pridobiti dovoljenje za uporabo osebnih podatkov v postopku preverjanja identitete.

9.4.6. Posredovanje osebnih podatkov v sodnih in upravnih postopkih

V skladu z Zakonom o varstvu osebnih podatkov Republike Slovenije.

9.4.7. Druge okoliščine posredovanja osebnih podatkov

Ni predpisano.

9.5. Zaščita intelektualne lastnine

Ministrstvo za obrambo Republike Slovenije je lastnik digitalnih potrdil in zasebnih ključev, ki so bili izdani v okviru infrastrukture javnih ključev na MO.

9.6. Odgovornosti in jamstva

9.6.1. Odgovornosti in jamstva overitelja

Overitelj SIMoD-CA-Root jamči, da upravlja z digitalnimi potrdili, upravlja z repozitorijem in izdaja registre preklicanih potrdil v skladu s Politiko SIMoD-PKI. Overitelja SIMoD-CA-Root predstavlja, odgovarja in jamči za izpolnjevanje njegovih obveznosti Svet za upravljanje z infrastrukturo javnih ključev na MO.

9.6.2. Odgovornost in jamstva prijavne službe

Overitelj SIMoD-CA-Root nima vzpostavljene prijavne službe. Za skladnost identifikacijskih postopkov s Politiko SIMoD-PKI in točnost podatkov v prošnjah za izdajo digitalnih potrdil overitelja SIMoD-CA-Root odgovarja in jamči Svet za upravljanje z infrastrukturo javnih ključev na MO, kot je določeno v poglavju 9.6.1 Odgovornosti in jamstva overitelja.

9.6.3. Odgovornost in jamstva imetnikov digitalnih potrdil

Imetniki digitalnih potrdil podrejenih overiteljev so dolžni upoštevati določila Politike SIMoD-PKI, poglavje 9.6.3 Odgovornost in jamstva imetnikov digitalnih potrdil.

9.6.4. Odgovornost in jamstva tretjih oseb

Tretje osebe, ki se zanašajo na digitalna potrdila SIMoD-PKI, so dolžne upoštevati določila Politike SIMoD-PKI, poglavje 9.6.4 Odgovornost in jamstva tretje osebe.

9.6.5. Odgovornost in jamstva drugih udeležencev

Ni relevantno.

9.7. Zanikanje odgovornosti overitelja

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

- je bilo potrdilo izdano kot rezultat napake, neverodostojnosti podatkov v vlogi ali drugih dejanj naročnika oziroma imetnika ali katerekoli druge fizične ali pravne osebe, overitelj pa je postopal v skladu z lastnimi pravili delovanja in predpisi;
- je veljavnost digitalnega potrdila pretekla;
- je bilo digitalno potrdilo uporabljeno po preklicu in objavi v registru preklicanih potrdil;
- je bilo digitalno potrdilo spremenjeno ali kakor koli drugače modificirano;
- 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, ali pa v nasprotju s pravnimi akti;
- imetnik ali tretja oseba ni postopala v skladu s predpisanimi postopki v Politiki SIMoD-PKI ali morebitni drugi pogodbi;
- je nastala škoda zaradi napake v delovanju strojne ali programske opreme imetnika ali tretje osebe.

9.8. Omejitve odgovornosti overitelja

Overitelj jamči za vrednost posameznega pravnega posla do vrednosti 100.000,00 SIT.

9.9. Zavarovanje pred škodo zaradi neizpolnjevanja obveznosti

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

9.10. Začetek in prenehanje veljavnosti

9.10.1.Začetek veljavnosti

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

9.10.2.Prenehanje veljavnosti

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

9.10.3.Posledice prenehanja veljavnosti

Po prenehanju veljavnosti Pravil delovanja overitelja SIMoD-CA-Root zaradi objave nove verzije se obstoječa potrdila uporabljajo v skladu z določili Pravil delovanja overitelja SIMoD-CA-Root, po kateri so bila izdana. V primeru da zaradi spremenjenih okoliščin to ne bo več

mogoče, bo overitelj SIMoD-CA-Root ob izdaji nove verzije o tem obvestil vse upravičeno zainteresirane.

Posledice prenehanja veljavnosti Pravil delovanja overitelja SIMoD-CA-Root v primeru prenehanja delovanja overitelja SIMoD-CA-Root so določene v poglavju 5.8. Prenehanje delovanja overitelja.

9.11. Obvestila in komuniciranje z udeleženci

Obvestila udeležencem infrastrukture javnih ključev na MO so objavljena na spletni strani: http://www.simod-pki.mors.si, če ni drugače določeno v drugih poglavjih pričujočega dokumenta.

9.12. Spreminjanje dokumenta

9.12.1.Postopek uveljavitve spremembe

Svet za upravljanje z infrastrukturo javnih ključev na MO odobri spremembe Pravil delovanja overitelja SIMoD-CA-Root in jih predlaga ministru v sprejem.

9.12.2.Postopek obveščanja in rok za pripombe

Za vsa področja iz teh Javnih pravil SIMoD-CA-Root velja obveznost obveščanja o spremembah osem dni (8) dni pred uporabo sprememb Javnih pravil SIMoD-CA-Root na način, določen v 9.11. Obvestila in komuniciranje z udeleženci. Izjema je vnos uredniških in tipografskih popravkov, ki smiselno ne vplivajo na vsebino Javnih pravil SIMoD-CA-Root.

Svet za upravljanje z infrastrukturo javnih ključev na MO o spremembah Javnih pravil SIMoD-CA-Root medsebojno priznane overitelje obvesti najmanj osem (8) dni pred uporabo sprememb. Ministrstvo, pristojno za informacijsko družbo, Svet za upravljanje z infrastrukturo javnih ključev na MO o spremembah obvesti v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu.

9.12.3.Spremembe, ki zahtevajo novo identifikacijsko oznako politike

Svet za upravljanje z infrastrukturo javnih ključev na MO po lastni presoji odloči, ali so spremembe vsebine Pravil delovanja SIMoD-CA-Root tolikšne, da zahtevajo objavo novih Pravil delovanja overitelja SIMoD-CA-Root z novo identifikacijsko oznako.

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

Delovanje infrastrukture javnih ključev na MO je v skladu z zakonodajo Republike Slovenije navedeno v poglavju 9.15. Skladnost s pravnimi akti.

9.15. Skladnost s pravnimi akti

Overitelj SIMoD-PKI-Root delujejo v skladu z:

- Zakonom o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 – uradno prečiščeno besedilo);
- Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01);
- Zakonom o obrambi (Uradni list RS, št. 103/04 – uradno prečiščeno besedilo);

- Zakonom o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo);
- Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 86/04).

9.16. Splošne določbe

9.16.1.Ostali obvezujoči dokumenti

Poleg teh Pravil delovanja overitelja SIMoD-CA-Root in Politike SIMoD-PKI, so vsi udeleženci infrastrukture javnih ključev na MO dolžni upoštevati tudi določila pravil overitelja, ki je izdal digitalno potrdilo, izjavo uporabnika, podpisano ob oddaji vloge za pridobitev digitalnega potrdila, veljavne predpise na območju Republike Slovenije ter določila morebitnih drugih dokumentov, ki jih določi overitelj v svojih pravilih delovanja.

9.16.2. Prenos pravic in obveznosti

Ni predpisano.

9.16.3.Spremembe okoliščin delovanja

Če postane zaradi spremenjenih okoliščin delovanja ali spremembe zakonodaje del Pravil delovanja overitelja SIMoD-CA-Root nepravilen ali neveljaven, ostanejo ostali deli Pravil delovanja overitelja SIMoD-CA-Root veljavni vse dokler se ne objavi sprememba. Postopek spremembe Pravil delovanja overitelja SIMoD-CA-Root je opisan v poglavju 9.12. Spreminjanje dokumenta.

9.16.4. Uveljavljanje (povračila stroškov v primeru sporov in izjeme)

Zahtevki za povračila stroškov v primeru sporov so obravnavajo v skladu z veljavnimi predpisi MO.

O dovoljenih odstopanjih od posameznih določil Pravil delovanja overitelja SIMoD-CA-Root v izjemnih primerih odloča Svet za upravljanje z infrastrukturo javnih ključev na MO za vsak primer posebej na podlagi pisnega zahtevka, ki mora vsebovati obrazložitev, previden čas trajanja odstopanja in načrt odprave neskladja.

9.16.5. Višje sile

Višja sila so izredne nepredvidljive okoliščine, na katere udeleženci infrastrukture javnih ključev na MO ne morejo vplivati (na primer naravne nesreče, terorizem, …). Kot višja sila se štejejo tudi spremembe zakonodaje ali tehnologije (na primer razbitje kriptografskega algoritma), ki vplivajo na delovanje infrastrukture javnih ključev na MO.

Noben udeleženec ne more uveljavljati zahtevkov, ki mu po tem ali po ostalih obvezujočih dokumentih pripadajo, če je do ravnanja v nasprotju s tem ali ostalimi dokumenti prišlo zaradi višje sile.

Če postane zaradi višje sile delovanje overitelja SIMoD-CA-Root trajno nemogoče, bo overitelj SIMoD-CA-Root postopal kot je določeno v poglavju 5.8. Prenehanje delovanja overitelja.

9.17. Ostale določbe

SIMoD-PKI deluje v skladu s priporočili EU in NATO.

Oblika in vsebina dokumenta Politika P je usklajena z:

- RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework;
- ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates.

10. KONČNE DOLOČBE

Pravila delovanja overitelja SIMoD-CA-Root, javni del, začnejo veljati naslednji dan po podpisu, uporabljati pa se začnejo trideseti (30) dan po podpisu.

Šifra: 382-5/2006-12
Datum: 17.7.2006

Karl Erjavec
Minister

KRATICE IN POJMI

Kratice

Kratica	Opis
CN	Splošno ime objekta v imeniku (angl.: Common Name).
CRL	Register preklicanih potrdil (angl.: Certificate Revocation List).
DN	Razločevalno ime objekta v imeniku, tudi polno ime objekta v imeniku (angl.: Distinguished Name).
ETSI	Evropski inštitut za standardizacijo na področju telekomunikacij; izdal serijo standardov s področja elektronskega podpisa in delovanja overiteljev (angl.: 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 (angl.: Federal Information Processing Standards).
FIPS 140-2	Serija standardov FIPS za kriptografske module.
IETF	Združenje strokovnjakov s področja Internetnih tehnologij. Izdelujejo serije priporočil (angl.: Internet Engineering Task Force).
ISO	Mednarodna organizacija za standardizacijo (angl.: International Standardization Organization).
ITU-T	Mednarodna organizacija za standardizacijo na področju telekomunikacij (angl.: 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 (angl. Internet Engineering Task Force) priporočilu RFC 1777 (LDAP, angl. Leightweight Directory Access Protocol).
MO	Ministrstvo za obrambo
PKCS	Priporočila podjetja RSA Security za uporabo asimetričnih kriprografskih algoritmov (angl.: Public Key Cryptographic Standards).
PKCS#1	Osnovna pravila za formatiranje podatkov ob implememtaciji 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 (angl.: Public Key Infrastructure).
PKIX	Delovna skupina za področje infrastrukture javnih ključev v okviru IETF(angl.: Internet Engineering Task Force). Izdala serijo priporočil za digitalna potrdila in registre preklicanih potrdil (angl.: Public Key Infrastrukture X.509).
PKIX- CMP	Postopek izmenjave podatkov, ki se nanašajo na digitalna potrdila med subjekti infrastrukture overitelja (angl.: PKIX Certificate Management protocol). Vključuje PKCS#7 in PKCS#10.

RDN	Kratko razločevalno ime objekta v imeniku, praviloma sestavljeno in splošnega imena (angl. Common Name, CN) in serijske številke (angl., serialNumber)
RFC	Priporočila, ki jih izdaja IETF.
RFC 3280	Priporočilo, ki določa elemente potrdil in regista preklicanih potrdil.
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 4210	Priporočilo, ki določa postopke za izmenjavo podatkov, ki se nanašajo na digitalna potrdila. Vsebuje PKIX-CMP.
RSA	Eden prvih nesimetričnih kriptografskih sistemov, patentiran leta 1983, imenovan po odkriteljih: Rivest, Shamir in Adelman.
SIMoD-CA-Root	Overitelj digitalnih potrdil na Ministrstvu za obrambo Republike Slovenije (angl.: Slovenian Ministry of Defense Certification Authority).
SIMoD-PKI	Infrastruktura javnih ključev Ministratsva za obrambo Republike Slovenije (angl. **S**loven**i**an **M**inistry **o**f **D**efence **P**ublic **K**ey **I**nfrastructure - SIMoD-PKI)
SV	Slovenska vojska
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.
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 – uradno prečiščeno besedilo)

Pojmi

Izraz	Definicija
Časovni žig	Je elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša v navedenem času.
Digitalni podpis	Je dodan podatek ali kriptografsko preoblikovanje, ki omogoča, da prejemnik podatkov preveri njihov izvor in integriteto, ter s tem prepreči poneverbo.
Digitalno potrdilo	Je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto.
Digitalno potrdilo za šifriranje	Je digitalno potrdilo, ki se uporablja za izmenjavo simetričnih šifrirnih ključev pri zagotavljanju tajnosti podatkov v elektronski obliki.
Digitalno potrdilo za verifikacijo podpisa	Je digitalno potrdilo, ki se uporablja za verifikacijo digitalnega podpisa, preverjanje istovetnosti uporabnikov in preverjanje celovitosti podatkov v elektronski obliki.
Elektronski podpis	Je 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	Je niz podatkov, ki so poslani ali prejeti na elektronski način, kar vključuje predvsem elektronsko izmenjavo podatkov in elektronsko pošto.
Imenik	Je 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	Je določena fizična oseba, navedena v digitalnem potrdilu v polju »Subject« kot lastnik zasebnega ključa, ki ustreza javnemu ključu, vsebovanem v digitalnem potrdilu oziroma pooblaščena oseba za uporabo potrdila za splošne nazive ter poveljniške dolžnosti v Slovenski vojski.
Informacijski sistem	Je 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 del notranjih pravil overitelja	Po Uredbi o pogojih za elektronsko poslovanje in elektronsko podpisovanje vsebuje javni del notranjih pravil overitelja “bistvene določbe, ki vplivajo na odnos med overiteljem in imetniki od njega izdanih potrdil ter tretjimi osebami, ki se zanašajo na ta potrdila”. Pravila delovanja overitelja SIMoD-CA-Root, javni del, predstavljajo Javni del notranjih pravil overitelja SIMoD-CA-Root.
Javni ključ	Polovica para ključev, ki je lahko javno objavljen.
Javni komunikacijsko informacijski sistem	Je komunikacijsko informacijski sistem, katerega storitve so namenjene javni uporabi.
Komunikacijski sistem	Je skupek naprav in postopkov, ki omogočajo prenos informacij. Primeri takih sistemov so telekomunikacijski sistemi in računalniška omrežja.
Komunikacijsko informacijski sistem	Je skupen izraz za komunikacijski in informacijski sistem.
Kvalificirano digitalno potrdilo	Je digitalno potrdilo, ki izpolnjuje zahteve iz 28. člena ZEPEP. Izda ga overitelj, ki deluje v skladu z zahtevami iz 28. do 36. člena ZEPEP.
LDAP	Protokol za dostop do podatkov v imeniku (angl. Lightweight Data Access Protocol).
Naročnik potrdila	Je fizična ali pravna oseba, ki z vlogo zaprosi za izdajo digitalnega potrdila.
Naslovnik elektronskega sporočila	Je oseba, ki ji je pošiljatelj namenil elektronsko sporočilo.
Nevarovani KIS	KIS, ki ni akreditiran za nobeno stopnjo tajnosti glede na tajnost podatkov, ki se v KIS obdelujejo.
Ogrožanje	Je dejanska ali domnevna možnost razkritja tajnih podatkov, izgube celovitosti ali razpoložljivosti podatkov.
Oprema za elektronsko podpisovanje	Je 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	Je fizična ali pravna oseba, ki izdaja digitalna potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi.

Par ključev	Je par asimetričnih kriptografskih ključev, ki ga sestavljata zasebni ključ in javni ključ.
Podatki v elektronski obliki	So podatki, ki so oblikovani, shranjeni, poslani, prejeti ali izmenljivi na elektronski način.
Podatki za elektronsko podpisovanje	So edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa.
Podatki za preverjanje elektronskega podpisa	So edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa.
Podpisnik	Je oseba, ki ustvari ali je v njenem imenu in v skladu z njeno voljo ustvarjen elektronski podpis.
Politika digitalnih potrdil	Je nabor pravil, ki posledično definira uporabnost digitalnih potrdil v določeni skupini uporabnikov in/ali za določen nabor aplikacij s skupnimi varnostnimi zahtevami (RFC 3647).
Pošiljatelj elektronskega sporočila	Je 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	Je oseba, ki je prejela elektronsko sporočilo; posrednik elektronskega sporočila se ne šteje za prejemnika tega elektronskega sporočila.
Prijavna služba	Je služba oziroma organizacija, ki po pooblastilu overitelja sprejema vloge in preverja istovetnosti bodočih imetnikov.
Repozitorij	Je skladišče oziroma odlagališče objektov, vključno z digitalnimi potrdili. Repozitorij sestavljata imenik in spletne strani.
Selektivno omejevanje dostopa	Ločevanje dostopa glede na upravičen interes.
Sredstvo za preverjanje elektronskega podpisa	Je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa.
Sredstvo za elektronsko podpisovanje	Je nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa.
Sredstvo za varno elektronsko podpisovanje	Je sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve iz 37. člena ZEPEP.
Šifrirni (kriptografski) ključ	Je 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	Je subjekt, ki ni aktivno udeležen v storitev, vendar zaupa izvajalcu in rezultatu storitve.
Uporabnik	Je naročnik ali imetnik digitalnega potrdila.

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.
Varovani KIS	KIS, akreditiran za ustrezno stopnjo tajnosti glede na tajnost podatkov, ki se v KIS obdelujejo.
Vloge	So obrazci overitelja za pridobitev ali preklic digitalnega potrdila, povrnitev zgodovine dešifrirnih ključev osebnega digitalnega potrdila.
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	Polovica para ključev, ki mora ostati skriven, da se zagotovi zaupnost, integriteta, istovetnost in nezatajljivost podatkov v elektronski obliki.
Zaupni del notranjih pravil overitelja	Po Uredbi o pogojih za elektronsko poslovanje in elektronsko podpisovanje vsebuje zaupni del notranjih pravil overitelja "določila glede prostorov, osebja, fizičnega, elektronskega in programskega varovanja infrastrukture overitelja, notranjega nadzora, ukrepanja ob nepredvidenih dogodkih in določila glede vodenja zapisov in sestave dnevnikov“.
Zloraba	Je razkritje tajnega podatka, izguba celovitosti ali razpoložljivosti podatka.
Zunanji izvajalec	Je fizična ali pravna oseba, ki za MO opravlja dela po pogodbi in ni zaposlena v MO.