REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Pravila delovanja overitelja SIMoD-CA-Restricted, javni del

(Javna pravila SIMoD-CA-Restricted)

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-Restricted, JAVNI DEL

(JAVNA PRAVILA SIMoD-CA-Restricted)

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 obrambe države.

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.

Overitelji SIMoD-PKI delujejo 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 ter tretje osebe, ki se zanašajo na digitalna potrdila in drugi overitelji, ki se želijo povezovati z infrastrukturo javnih ključev na MO.

Ta dokument predstavlja javni del pravil delovanja overitelja SIMoD-CA-Restricted. Dokument podaja opis overiteljeve infrastrukture, postopkov overitelja SIMoD-CA-Restricted 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 tega dokumenta upoštevati še določila Politike SIMoD-PKI.

Overitelj SIMoD-CA-Restricted deluje kot podrejeni overitelj korenskega overitelja SIMoD-CA-Root in izdaja digitalna potrdil za potrebe uporabnikov in aplikacij v omrežju klasificiranem za prenos podatkov stopnje tajnosti INTERNO (angl. Restricted). Pravila delovanja overitelja SIMoD-CA-Restricted opisujejo izdajanje in upravljanje digitalnih potrdil za zagotavljanje varnostnih storitev pri hranjenju in prenosu podatkov z ali brez stopnje tajnosti; za digitalno podpisovanje datotek, sporočil in elektronskih obrazcev; preverjanje istovetnosti oseb in gradnikov informacijske infrastrukture kot so strežniki, usmerjevalniki, požarne pregrade in imeniki. Overitelj SIMoD-CA-Restricted izdaja digitalna potrdila v skladu s Politiko SIMoD-PKI, ki združuje pet osnovnih politik za digitalna potrdila, ki se med seboj ločijo glede na stopnjo zaupanja v digitalno potrdilo in namen uporabe oziroma storitev, kot je navedeno v spodnji tabeli:

Stopnja zaupanja	Namen uporabe oziroma storitev
VISOKA	Digitalna potrdila za preverjanje digitalnega podpisa za storitve prepoznavanja in preverjanja istovetnosti, celovitosti in nezanikanja.
VISOKA	Digitalna potrdila za šifriranje[1] za storitve zagotavljanja tajnosti, oziroma zaupnosti.

[1] Javni ključ iz digitalnega potrdila za šifriranje se uporablja za izmenjavo simetričnih šifrirnih ključev pri zagotavljanju zaupnosti podatkov v elektronski obliki.

VISOKA	Digitalna potrdila za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe[2].
SREDNJA	Digitalna potrdila za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe.
VISOKA	Digitalna potrdila za izdajatelje časovnih žigov.

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

- upravljana digitalna potrdila (tip A), imenovana tudi *Entrust ID*[3];
- neupravljana digitalna potrdila (tip B), imenovana tudi spletna[4] ali WEB[5] digitalna potrdila in
- digitalna potrdila za izdajatelje časovnih žigov.

V okviru upravljanih digitalnih potrdil oziroma *Entrust ID* overitelj SIMoD-CA-Restricted izdaja naslednje skupine potrdil tipa A, ki vključujejo od 1 do 3 digitalna potrdila:

Upravljana digitalna potrdila oziroma *Entrust ID*			
Tip	Namen uporabe	Stopnja zaupanja v potrdilo	Identifikacijska oznaka politike
A1	Digitalno potrdilo za preverjanje digitalnega podpisa za storitve prepoznavanja in preverjanja istovetnosti, celovitosti in nezanikanja.	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.1.0
	Digitalno potrdilo za šifriranje za storitve zagotavljanja tajnosti, oziroma zaupnosti	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.2.0
A2	Digitalno potrdilo za preverjanje digitalnega podpisa za storitve prepoznavanja in preverjanja istovetnosti, celovitosti in nezanikanja.	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.1.0
	Digitalno potrdilo za šifriranje za storitve zagotavljanja tajnosti, oziroma zaupnosti	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.2.0
	Digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.3.0
A3	Digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.3.0
A4	Digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe	SREDNJA	1.3.6.1.4.1.22295.10.1.1.1.2.3.0

[2] Brez omejitve uporabe v smislu varnostnih storitev in aplikacij.

[3] Ime *Entrust ID* izhaja iz konkretnega poimenovanja upravljanih digitalnih potrdil v okviru uporabljene tehnološke rešitve overitelja SIMoD-CA-Restricted. *Entrust* je zaščiteno ime podjetja Entrust.

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

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

V okviru neupravljanih oziroma spletnih digitalnih potrdil overitelj SIMoD-CA-Restricted izdaja imetnikom naslednja digitalna potrdila:

Neupravljana oziroma spletna digitalna potrdila			
Tip	Namen uporabe	Stopnja zaupanja v potrdilo	Identifikacijska oznaka politike
B1	Digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.3.0
B2	Digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe	SREDNJA	1.3.6.1.4.1.22295.10.1.1.1.2.3.0

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

Namen uporabe	Stopnja zaupanja v potrdilo	Identifikacijska oznaka politike
Digitalna potrdila za izdajatelje časovnih žigov	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.4.0

1.2. Naziv dokumenta in identifikacijska oznaka

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

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-Restricted (1.3.6.1.4.1.22295[6].<storitev>.<overitelj>) je tako določen po pravilu:

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

<vrsta dokumenta>.<verzija>.

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

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

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-Restricted se torej določi po pravilu:

1.3.6.1.4.1.22295.10.3.<vrsta dokumenta>.<verzija>

in ima vrednost 1.3.6.1.4.1.22295.10.3.2.0. Identifikacijska oznaka se uporablja za enolično označevanje dokumenta in njegove verzije. Oznaka se ne uporablja za označevanje digitalnih potrdil.

Za označevanje digitalnih potrdil se uporabljajo identifikacijske oznake politik (angl. Policy OIDs), kot so določene v Politiki SIMoD-PKI:

Stopnja zaupanja	Namen uporabe oziroma storitev	Identifikacijska oznaka politike
VISOKA	Digitalna potrdila za preverjanje digitalnega podpisa za storitve prepoznavanja in preverjanja istovetnosti, celovitosti in nezanikanja	1.3.6.1.4.1.22295.10.1.1.1.1.1.0
VISOKA	Digitalna potrdila za šifriranje za storitve zagotavljanja tajnosti, oziroma zaupnosti	1.3.6.1.4.1.22295.10.1.1.1.1.2.0
VISOKA	Digitalna potrdila za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe.	1.3.6.1.4.1.22295.10.1.1.1.1.3.0
SREDNJA	Digitalna potrdila za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe.	1.3.6.1.4.1.22295.10.1.1.1.2.3.0
VISOKA	Digitalna potrdila za izdajatelje časovnih žigov	1.3.6.1.4.1.22295.10.1.1.1.1.4.0

Dokument je napisan 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[7]) 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. Overitelj SIMoD-CA-Restricted deluje kot podrejeni overitelj korenskega overitelja SIMoD-CA-Root in izdaja digitalna potrdil za potrebe uporabnikov in aplikacij v omrežju klasificiranem za prenos podatkov stopnje tajnosti INTERNO (angl. Restricted).

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.

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

1.3.1.1. Svet za upravljanje z infrastrukturo javnih ključev na MO

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

- nadzira izdelavo, vodi postopek potrditve, ocenjuje predlagane spremembe, predlaga uveljavitve sprememb in načrtuje postopek uveljavitve sprememb Politike SIMoD-PKI;
- ocenjuje in potrjuje skladnost pravil delovanja posameznega overitelja s Politiko SIMoD-PKI;
- 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-Restricted

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

1.3.2. Prijavna služba

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

1.3.3. Imetniki digitalnih potrdil

Imetniki digitalnih potrdil so:

a) zaposleni v MO;
b) zaposleni v institucijah, ki opravljajo naloge, ki so povezane z obrambo;
c) notranje organizacijske enote in organi v sestavi MO[8] (v nadaljevanju organizacijske enote MO) ter poveljniki enot na ravni poveljniških dolžnosti v SV;
d) institucije[9], ki opravljajo naloge, ki so povezane z obrambo;
e) strežniki[10] in druga strojna ter programska oprema;
f) izdajatelji[11] časovnih žigov in podobni ponudniki storitev overjanja.

Izdajo digitalnih potrdil subjektom iz točk c) in d) odobrava Svet za upravljanje z infrastrukturo javnih ključev na MO.

[8] Odgovorna oseba za digitalno potrdilo je vodja notranje organizacijske enote MO. Odgovorna oseba ima za digitalno potrdilo za notranje organizacijske enote enake obveznosti kot imetnik digitalnega potrdila za zaposlene v MO.

[9] Odgovorna oseba za digitalno potrdilo je predstojnik institucije. Odgovorna oseba ima za digitalno potrdilo za institucije, ki opravljajo naloge, ki so povezane z obrambo, enake obveznosti kot imetnik digitalnega potrdila za zaposlene v institucijah, ki opravljajo naloge, ki so povezane z obrambo.

[10] Odgovorna oseba za digitalno potrdilo je vodja notranje organizacijske enote MO, ki upravlja s strežniki in drugo strojno ter programsko opremo. Odgovorna oseba ima za digitalno potrdilo za strežnik, drugo strojno ali programsko opremo, enake obveznosti kot imetnik digitalnega potrdila za zaposlene v MO.

[11] Odgovorna oseba za digitalno potrdilo je vodja notranje organizacijske enote MO, ki upravlja z izdajateljem časovnega žiga ali podobnim ponudnikom storitev overjanja. Odgovorna oseba ima za digitalno potrdilo za izdajatelja časovnega žiga ali podobnega ponudnika storitev overjanja enake obveznosti kot imetnik digitalnega potrdila za zaposlene v MO.

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 javni ključ, oziroma digitalno potrdilo SIMoD-CA-Root korenskega overitelja.

Tretje osebe so:

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

1.3.5. Posredno odgovorni organi

Overitelj SIMoD-CA-Restricted deluje kot del KIS MO in SV in dela 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

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

Infrastruktura javnih ključev na MO, v okviru katere deluje SIMoD-CA-Restricted, omogoča pet osnovnih varnostnih storitev:

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

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

1.4.1. Dovoljena uporaba digitalnih potrdil

1.4.1.1. Stopnja zaupanja v digitalno potrdilo

Digitalno potrdilo nedvoumno povezuje imetnika digitalnega potrdila z njegovim javnim ključem. Celovitost in varnost povezave med imetnikom in njegovim javnim ključem je ocenjena s stopnjo zaupanja v digitalno potrdilo. Stopnja zaupanja je odvisna od strogosti registracijskih postopkov, postopkov pri upravljanju z digitalnimi potrdili in pripadajočimi zasebnimi ključi, zahtev glede osebja, fizičnega in tehničnega varovanja infrastrukture javnih ključev ter varovanja zasebnih ključev. Omenjeni ukrepi so za vse vrste digitalnih potrdil, ki jih izdaja SIMoD-CA-Restricted enaki. Razlika v stopnji zaupanja izhaja samo iz načina varovanja zasebnih ključev na strani imetnikov.

SIMoD-CA-Restricted izdaja digitalna potrdila z VISOKO in SREDNJO stopnjo zaupanja. Stopnja zaupanja je določena glede na postopek identifikacije in preverjanja istovetnosti imetnika, ter stopnje varovanja zasebnih ključev, kot je navedeno v spodnji tabeli:

Stopnja zaupanja	Namen uporabe oziroma storitev	Postopek identifikacije in preverjanja istovetnosti imetnika, ter stopnja varovanja zasebnih ključev
VISOKA	Digitalna potrdila za preverjanje digitalnega podpisa za storitve prepoznavanja in preverjanja istovetnosti, celovitosti in nezanikanja	Osebna identifikacija imetnika v postopku registracije. Obvezno generiranje in uporaba kriptografskih ključev na pametni kartici ali v strojnem kriptografskem modulu.
VISOKA	Digitalna potrdila za šifriranje za storitve zagotavljanja tajnosti oziroma zaupnosti	Osebna identifikacija imetnika v postopku registracije. Obvezno generiranje in uporaba kriptografskih ključev na pametni kartici ali v strojnem kriptografskem modulu.
VISOKA	Digitalna potrdila za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe	Osebna identifikacija imetnika v postopku registracije. Obvezno generiranje in uporaba kriptografskih ključev na pametni kartici, ali v strojnem kriptografskem modulu.
SREDNJA	Digitalna potrdila za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe	Osebna identifikacija imetnika v postopku registracije. Priporočeno generiranje in uporaba kriptografskih ključev na pametni kartici ali v strojnem kriptografskem modulu.
VISOKA	Digitalna potrdila za izdajatelje časovnih žigov	Osebna identifikacija skrbnika sistema v postopku registracije. Obvezno generiranje in uporaba kriptografskih ključev v strojnem kriptografskem modulu.

Pri izbiri vrste digitalnega potrdila, ki naj se uporabi, je odločilna vrednost podatkov, ocena ogroženosti okolja in obstoječa zaščita KIS.

1.4.1.2. Vrednost podatkov

Vrednost podatkov se določa glede na njihovo pomembnost za doseganje cilja (npr. na vojaškem področju za izpolnitev bojne naloge, na finančnem področju pa glede na znesek transakcij) ter stopnjo tajnosti. Stopnja tajnosti podatkov se določa na podlagi ocene možnih škodljivih posledic, ki bi nastale, če bi prišlo do nepooblaščenega razkritja tajnega podatka.

Pravila delovanja overitelja predvidevajo, v skladu s Politiko SIMoD-PKI, spodaj navedeno razvrstitev podatkov:

<table>
<tr><td colspan="3">Vrste podatkov</td><td rowspan="2">Pomembnost</td><td rowspan="2">Stopnja tajnosti</td></tr>
<tr><td>Finančne transakcije</td><td colspan="2">Obrambne zadeve, konkretne bojne naloge</td></tr>
<tr><td></td><td colspan="2">administrativni podatki</td><td>NIZKA</td><td>brez interno
zaupno (redko)</td></tr>
<tr><td rowspan="2">finančne transakcije malih vrednosti (npr. pisarniški material, knjige, potni stroški, nakazila plačil…)</td><td colspan="2">podporne naloge</td><td rowspan="2">SREDNJA</td><td>brez interno</td></tr>
<tr><td rowspan="2">Pomembni podatki</td><td>podkategorija 3:
podatki pomembni za izvajanje krovnih nalog na ravni nižjih organizacijskih enot</td><td>zaupno</td></tr>
<tr><td>finančne transakcije velikih vrednosti (npr. letala, stavbe…)</td><td>podkategorija 2:
• ukrepi za pripravljenost;
• jedrska varnost;
• elektronsko bojevanje;
• izvidovanje;
• transportne poti;
• varnost, zdravstvena oskrba;
• policijsko nadzorstvo;
• varovanje informacij;
• modernizacija.</td><td>tajno
strogo tajno</td></tr>
<tr><td></td><td>podkategorija 1:
• obveščevalni podatki;
• kriptografski material;
• poveljevanje vojski;
• oborožitev in vojaški sistemi;
• sistemi nujni za izpolnitev bojne ali obveščevalne naloge.</td><td>VISOKA</td><td>brez interno
zaupno
tajno
strogo tajno</td></tr>
</table>

V zadnjem stolpcu so navedene običajne stopnje tajnosti za podatke določene pomembnosti. Pomembnost in stopnja tajnosti podatkov v splošnem nista medsebojno determinirani.

1.4.1.3. Grožnja

Grožnja je vsaka možnost dogodka, ki lahko povzroči škodo. V KIS škoda pomeni popolno ali delno uničenje, nerazpoložljivost, razkritje ali spremembo podatkov ali procesov oziroma delov procesov. Grožnje vključujejo naravne nesreče, fizično uničenje, vdore v sistem, zlorabe avtorizacijskih postopkov, človeške napake, spremljanje prometa, prisluškovanje ter napake v strojni in programski opremi. Pri obvladovanju groženj je treba upoštevati škodno moč grožnje, v kolikšni meri lahko grožnjo toleriramo in možnost njene odprave.

1.4.1.4. Stopnja zaščite KIS v MO in SV

KIS MO in SV je ločen na več varovanih KIS, akreditiranih za ustrezno stopnjo tajnosti glede na tajnost podatkov, ki se v posameznem KIS obdelujejo.

KIS MO in SV je razdeljen na več omrežij, ki so selektivno ločena glede na stopnjo tajnosti (JAVNO, INTERNO, TAJNO) podatkov, ki se v posameznem omrežju obdelujejo. Omrežja so zaščitena z zaščitnimi mehanizmi na komunikacijski ravni, kot so šifrirne naprave v omrežju oziroma na povezavah med deli omrežja, fizična izolacija, požarne pregrade in sistemi za nadzor vdorov. Ti mehanizmi zagotavljajo izgradnjo omrežij znotraj KIS MO in SV različnih ravni varnosti.

Digitalna potrdila, ki jih izdaja SIMoD-CA-Restricted je dovoljeno uporabljati v vseh omrežjih znotraj KIS MO in SV.

1.4.1.5. Smernice za odločitev o uporabi digitalnih potrdil ustrezne stopnje zaupanja

Poglavje podaja smernice za uporabo digitalnih potrdil obeh stopenj zaupanja iz poglavja 1.4.1.1 Stopnja zaupanja v digitalno potrdilo. Odločitev o uporabi digitalnega potrdila ustrezne stopnje zaupanja mora biti rezultat konkretne študije, ki upošteva konkretno okolje uporabe ter vključuje obvladovanje tveganj. Študija upošteva dejstvo ali gre za tajne, osebne ali druge podatke, ki glede na pomembnost, zahtevo po celovitosti in razpoložljivosti, zahtevajo uporabo digitalnih potrdil določene stopnje zaupanja. Ustreznost odločitve potrdi projektna skupina ali odgovorni organ, ki izda dovoljenje za obratovanje informacijske rešitve.

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

1.4.1.6. Dovoljena uporaba digitalnih potrdil z VISOKO stopnjo zaupanja

Uporaba digitalnih potrdil VISOKE stopnje zaupanja zagotavlja:

- celovitost, preverjanje istovetnosti, selektivno kontrolo dostopa in nezanikanja vsem pomembnim podatkom vseh stopenj tajnosti;
- zaupnost podatkov s stopnjo tajnosti do vključno INTERNO;
- selektivno omejevanje dostopa[12] do stopnje tajnosti TAJNO (angl. Comunity of interest - COI separation);
- upravljanje z varnostnimi parametri v KIS. Upravljanje z varnostnimi parametri pomeni upravljanje s šifrirnimi ključi naprav v KIS (usmerjevalniki, šifrirne naprave), daljinski nadzor in upravljanje z napravami;
- preverjanje istovetnosti naprav v KIS.

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

1.4.1.7. Dovoljena uporaba digitalnih potrdil s SREDNJO stopnjo zaupanja

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

Uporaba digitalnih potrdil SREDNJE stopnje zaupanja zagotavlja:

- celovitost, avtentifikacijo, kontrolo dostopa, zaupnosti in nezanikanje manj pomembnih podatkov brez stopnje tajnosti za dostop do podatkov brez stopnje tajnosti (npr. spletni dostop po protokolu SSL);
- zaupnost manj pomembnih podatkov, kot so npr. osebni podatki in podobno.
- upravljanje z varnostnimi parametri v KIS. Upravljanje z varnostnimi parametri pomeni upravljanje s šifrirnimi ključi naprav v KIS (usmerjevalniki, šifrirne naprave), daljinski nadzor in upravljanje z napravami. Predpogoj je ustrezno fizično varovanje naprav, da je možnost zlorabe digitalnih potrdil majhna;
- preverjanje istovetnosti naprav v KIS, če so naprave fizično varovane, da je možnost zlorabe potrdil majhna.

Uporaba potrdil SREDNJE stopnje zaupanja ni dovoljena tam, kjer se zahteva medsebojno priznavanje overiteljev.

1.4.2. Nedovoljena uporaba digitalnih potrdil

Ni relevantno.

[12] selektivno omejevanje dostopa - ločevnaje dostopa glede na potrebo po vedenju

1.5. Upravljanje s Pravili delovanja SIMoD-CA-Restricted

1.5.1. Organ, ki upravlja s tem dokumentom

1.5.1.1. Svet za upravljanje z infrastrukturo javnih ključev na MO

Svet za upravljanje z infrastrukturo javnih ključev na MO ima v zvezi upravljanjem z dokumentom Pravila delovanja SIMoD-CA-Restricted obveznost voditi postopek potrditve, ocenjevati predlagane spremembe, predlagati uveljavitve sprememb in nadzorovati postopek uveljavitve sprememb.

1.5.1.2. Operativno osebje overitelja

Operativno osebje overitelja SIMoD-CA-Restricted 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-Restricted.

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-Restricted.

1.5.3. Odgovorni organ za odobritev skladnosti pravil delovanja overitelja SIMoD-CA-Restricted s Poltiko SIMoD-PKI

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

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

V okviru postopka odobritve pravil delovanja overitelja SIMoD-CA-Restricted se preveri:

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

Izdaja digitalnega potrdila podrejenemu overitelju SIMoD-CA-Restricted s strani SIMoD-CA-Root, je hkrati tudi potrditev skladnosti s Politiko SIMoD-PKI.

Svet za upravljanje z infrastrukturo javnih ključev na MO lahko za izvedbo postopka preverjanja pooblasti zunanjo inšpekcijsko službo oziroma organizacijo, ki mora izpolnjevati zahteve iz poglavja 8.2. Pogoji za inšpektorja.

1.6. Pojmi in kratice

Glej prilogo 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, Pravila delovanja overitelja SIMoD-CA-Root, ter Pravila delovanja overitelja SIMoD-CA-Restricted 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 SIMoD-CA-Root, liste preklicih digitalnih potrdil ter javne objave overiteljev.

Overitelj SIMoD-CA_Restricted v imenikih objavlja naslednje podatke:

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

Imeniki so dostopni po protokolu LDAP.

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

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

2.3. Čas in pogostost objav

Overitelj SIMoD-CA-Restricted objavi digitalno potrdilo takoj, ko ga izda. Overitelj SIMoD-CA-Restricted 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 overitelja SIMoD-CA-Restricted 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. Vsak imetnik ima praviloma tudi alternativno ime, določeno 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

Kratko razločevalno ime (angl. Relative Distinguished Name, RDN) mora enolično identificirati imetnika digitalnega potrdila. Edinstvenost kratkega razločevalnega imena se po potrebi doseže z uporabo oznake (na primer številke) dodane splošnemu imenu ali uporabo X.500 atributa *dnQualifier* v relativnem razločevalnem imenu.

Splošno ime v digitalnih potrdilih za zaposlene je priimek in ime osebe.

Splošno ime v digitalnih potrdilih za splošne nazive oziroma organizacijske enote MO in institucije mora enolično in nedvoumno označevati splošen naziv oziroma organizacijsko enoto ali institucijo.

Splošno ime v digitalnih potrdilih za poveljniške dolžnosti v SV mora enolično in nedvoumno označevati poveljniško dolžnost.

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

Splošno ime v digitalnih potrdilih za izdajatelje časovnih žigov mora enolično in nedvoumno označevati izdajatelja časovnega žiga.

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

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-Restricted 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

Edinstvenost kratkega imena se po potrebi zagotovi z oznako (na primer številke) dodano splošnemu imenu, ali uporabo X.500 atributa *dnQualifier* v relativnem razločevalnem imenu. V primeru uporabe X.500 atributa *dnQualifier*, je leta za vsako razločevalno ime različen.

3.1.6. Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk

Uporaba zaščitenih znamk v imenih je dovoljena samo nosilcem zaščitenih znamk. SIMoD-CA-Restricted ne sme zavestno izdati digitalnega potrdila z imenom, ki vsebuje zaščiteno

znamko naročniku, ki ni nosilec zaščitene znamke. Operativno osebje overitelja SIMoD-CA-Restricted 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 overitelj SIMoD-CA-Restricted posredoval v takšnih sporih. Svet za upravljanje z infrastrukturo javnih ključev na MO in operativno osebje overitelja SIMoD-CA-Restricted 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

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

- kot PKCS#10 zahtevek skladno z RSA PKCS#10 Certification Request Syntax Standard, ali
- po PKIX-CMP protokolu v skladu z RFC 4210 Internet X.509 Public Key Infrastructure (PKI) Certificate Management protocol (CMP).

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

Vloga za izdajo digitalnega potrdila za splošne nazive oziroma organizacijske enote MO ali institucije, ki so povezane z obrambo države, mora vsebovati uradni naziv organizacijske enote MO ali institucije, naslov ter ime odgovorne osebe, ki je praviloma vodja organizacijske enote MO oziroma predstojnik institucije.

Prijavna služba preveri podatke in istovetnost odgovorne osebe in prejšnjega odstavka, ali pooblaščene osebe, enako kot za fizične osebe skladno s poglavjem 3.2.3 Preverjanje istovetnosti za fizične osebe.

3.2.3. Preverjanje istovetnosti za fizične osebe

3.2.3.1. Digitalna potrdila za zaposlene

Za pridobitev digitalnega potrdila za zaposlene v MO morata bodoči imetnik in vodja njegove organizacijske enote MO pravilno izpolniti in podpisati vlogo za izdajo digitalnega potrdila. Prijavna služba 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).

Za pridobitev digitalnega potrdila za zaposlene v institucijah, ki so povezane z obrambo države, morata bodoči imetnik in predstojnik institucije pravilno izpolniti in podpisati vlogo za izdajo digitalnega potrdila. Prijavna služba preveri istovetnost bodočega imetnika z osebno identifikacijo na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list ali vozniško dovoljenje). Prijavna služba lahko zahteva dodatna dokazila, da je bodoči imetnik zaposlen v instituciji, ki je povezana z obrambo države.

3.2.3.2. Digitalna potrdila za poveljniške dolžnosti v SV

Za pridobitev digitalnega potrdila za poveljniške dolžnosti v SV morata nosilec poveljniške dolžnosti v SV in njegov neposredno nadrejeni poveljnik pravilno izpolniti in podpisati vlogo za izdajo digitalnega potrdila. Prijavna služba preveri pristnost podatkov bodočega imetnika v kadrovski evidenci MO in izvede osebno identifikacijo bodočega imetnika na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list ali vozniško dovoljenje). Prijavna služba lahko zahteva dodatna dokazila, da je bodoči imetnik res nosilec poveljniške vloge.

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

Za pridobitev digitalnega potrdila za strežnike, izdajatelje časovnega žiga ter drugo strojno ali programsko opremo MO, morata vodja organizacijske enote MO in skrbnik naprave ali programske opreme pravilno izpolniti in podpisati vlogo. Prijavna služba preveri pristnost podatkov skrbnika v kadrovski evidenci MO in izvede osebno identifikacijo skrbnika na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list ali vozniško dovoljenje).

Za pridobitev digitalnega potrdila za strežnike, izdajatelje časovnega žiga ter drugo strojno ali programsko opremo institucij, ki so povezane z obrambo države, morata predstojnik institucije in skrbnik naprave ali programske opreme pravilno izpolniti in podpisati vlogo. Prijavna služba preveri istovetnost skrbnika z osebno identifikacijo na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list ali vozniško dovoljenje). Prijavna služba lahko zahteva dodatna dokazila, da je bodoči skrbnik zaposlen v instituciji, ki je povezana z obrambo države.

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 na prijavni službi, 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[13] 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 dvakrat (2x) zaporedoma.

Po drugi samodejni obnovi je potrebno ponoviti postopek za pridobitev novega digitalnega potrdila in identifikacije v skladu s poglavji 3.2.2 Preverjanje istovetnosti organizacijske enote

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

MO in institucije, ki je povezana z obrambo države in 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.

V primeru, da samodejna obnova digitalnega potrdila ni možna (npr. imetnik v časovnem oknu za rutinsko izmenjavo ključev ni bil povezan z infrastrukturo javnih ključev), je potrebno ponoviti postopek za pridobitev novega digitalnega potrdila in identifikacije v skladu s poglavji 3.2.2 Preverjanje istovetnosti organizacijske enote MO in institucije, ki je povezana z obrambo države in 3.2.3 Preverjanje istovetnosti za fizične osebe.

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

Samodejna obnova digitalnih potrdil izdanih 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 organizacijske enote MO 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 je potrebno izpolniti vlogo za izdajo novega digitalnega potrdila in opraviti identifikacijo kot ob prvi pridobitvi digitalnega potrdila v skladu s poglavji 3.2.2 Preverjanje istovetnosti organizacijske enote MO in institucije, ki je povezana z obrambo države in 3.2.3 Preverjanje istovetnosti za fizične osebe.

3.4. Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila

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

- z digitalno podpisano vlogo za preklic;
- po enakem postopku kot pri prvi registraciji (v skladu s poglavji 3.2.2 Preverjanje istovetnosti organizacijske enote MO in institucije, ki je povezana z obrambo države in 3.2.3. Preverjanje istovetnosti za fizične osebe, ali
- s skrivnim geslom, izbranem pri postopku registracije.

4. UPRAVLJANJE Z DIGITALNIMI POTRDILI

4.1. Prošnja za izdajo digitalnega potrdila

4.1.1. Kdo lahko zaprosi za izdajo digitalnega potrdila

Vlogo za izdajo digitalnega potrdila za zaposlene oddajo fizične osebe, katerih ime bo navedeno v polju *Subject* v digitalnem potrdilu. Vlogo morata podpisati bodoči imetnik in predstojnik njegove organizacijske enote vsaj na ravni vodje sektorja za organizacijske enote MO oziroma predstojniki institucij, ki so povezane z obrambo države.

Vlogo za izdajo digitalnega potrdila za splošne nazive oziroma organizacijske enote MO ali institucije, ki opravljajo naloge, ki so povezane z obrambo države, izpolnijo predstojniki organizacijske enote vsaj na ravni vodje sektorja za organizacijske enote MO oziroma predstojniki institucij, ki so povezane z obrambo države. Vlogo oddajo prijavni službi osebno ali preko pooblaščene osebe.

Vlogo za izdajo digitalnega potrdila za poveljniške dolžnosti v SV oddajo nosilci poveljniške dolžnosti. Vlogo morata podpisati bodoči imetnik in njegov nadrejeni poveljnik.

Vlogo za izdajo digitalnih potrdil za strežnike in drugo strojno ter programsko opremo, s katero upravlja MO ali institucije, ki opravljajo naloge, ki so povezane z obrambo države, oddajo skrbniki opreme. Vlogo morata podpisati bodoči skrbnik in predstojnik organizacijske enote ali institucije, ki upravlja s strežnikom, drugo strojno oziroma programsko opremo.

Vlogo za izdajo digitalnih potrdil za izdajatelje časovnih žigov oddajo skrbniki opreme. Vlogo morata podpisati bodoči skrbnik in predstojnik organizacijske enote, ki je ponudnik oziroma upravljavec storitve.

Vloga za izdajo digitalnega potrdila vsebuje tudi obvestilo o vseh pomembnih okoliščinah uporabe potrdila.

4.1.2. Postopek obdelave vloge in odgovornosti

Bodoči imetnik vloži izpolnjeno in podpisano vlogo za izdajo digitalnega potrdila v prijavno službo osebno. Uporabnikom infrastrukture javnih ključev na MO so obrazci za vloge in navodila za izpolnjevanje in oddajo dostopni na spletni strani v KIS MO in SV: http://www.simod-pki.mors.si. Prijavna služba deluje v okviru rednega delovnega časa oziroma uradnih ur.

Izpolnjene vloge preveri prijavna služba in jih odobri oziroma v primeru pomanjkljivih podatkov ali neupravičenosti do digitalnega potrdila zavrne. Po uspešnem preverjanju podatkov in potrjeni upravičenosti do digitalnega potrdila, izvede prijavna služba postopke preverjanja istovetnosti v skladu s poglavjem 3.2.2 Preverjanje istovetnosti organizacijske enote MO in institucije, ki je povezana z obrambo države oziroma 3.2.3 Preverjanje istovetnosti za fizične osebe. Odobrene vloge prijavna služba na varen način (v zapečateni kuverti) posreduje operativnemu osebju overitelja SIMoD-CA-Restricted.

Operativno osebje overitelja SIMoD-CA-Restricted izvede rezervacijo razločevalnega imena in generiranje aktivacijskih podatkov.

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

Aktivacijske podatke mora bodoči imetnik do prevzema digitalnega potrdila ustrezno varovati.

4.2. Obdelava vloge za izdajo digitalnega potrdila

4.2.1. Postopek identifikacije in avtentikacije

Preverjanje identitete prosilca in pravilnosti podatkov izvaja prijavna služba v skladu s poglavji 3.2. Prva registracija. Odobrene vloge prijavna služba na varen način posreduje operativnemu osebju overitelja SIMoD-CA-Restricted.

Operativno osebje overitelja SIMoD-CA-Restricted ne izvaja nalog preverjanja identitete prosilca in pravilnosti podatkov. Operativno osebje overitelja SIMoD-CA-Restricted izvede rezervacijo razločevalnega imena in generiranje aktivacijskih podatkov - referenčne številke in avtorizacijske kode.

4.2.2. Odobritev ali zavrnitev izdaje digitalnega potrdila

Prošnja za izdajo digitalnega potrdila ne obvezuje overitelja SIMoD-CA-Restricted k izdaji digitalnega potrdila.

Odobritev ali zavrnitev izdaje digitalnega potrdila je odgovornost in pravica prijavne službe. Obvestilo o zavrnitvi digitalnega potrdila pošlje naročniku prijavna služba po elektronski pošti, odobritev vloge pa prijavna služba posreduje operativnemu osebju overitelja SIMoD-CA-Restricted. Naročnik je o odobritvi digitalnega potrdila obveščen hkrati s prejemom dela aktivacijskih podatkov.

4.2.3. Čas za obdelavo vloge za izdajo digitalnega potrdila

Overitelj SIMoD-CA-Restricted bo obvestil naročnika o odobritvi ali zavrnitvi izdaje digitalnega potrdila najkasneje v enaindvajsetih (21) dneh po oddaji vloge za izdajo digitalnega potrdila prijavni službi.

Bodoči imetnik ima za prevzem digitalnega potrdila na voljo trideset (30) dni od izdaje aktivacijskih podatkov.

4.3. Izdaja digitalnega potrdila

4.3.1. Postopki overitelja ob izdaji potrdil

Operativno osebje overitelja SIMoD-CA-Restricted začne s postopki izdajanja digitalnega potrdila po prejemu odobrene vloge od prijavne službe.

4.3.1.1. Dostava zasebnega ključa imetniku

Glej poglavje 6.1.2 Dostava zasebnega ključa imetniku.

4.3.1.2. Dostava overiteljevega javnega ključa imetniku

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

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

Razen ob prevzemu svojega potrdila, lahko overiteljevo digitalno potrdilo uporabniki pridobijo kadarkoli iz imenika, vendar je njihova obveznost, da preverijo istovetnost overitelja SIMoD-CA-Root in celovitost overiteljevega potrdila.

4.3.2. Obvestilo naročnikom o izdaji digitalnega potrdila

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

4.4. Prevzem digitalnega potrdila

Izdaja digitalnega potrdila je neločljivo povezana s prevzemom digitalnega potrdila. Bodoči imetnik lahko prevzame digitalno potrdilo samo z ustreznimi aktivacijskimi podatki. Veljavnost aktivacijskih podatkov je časovno omejena (glej poglavje 4.2.3 Čas za obdelavo vloge za izdajo digitalnega potrdila). Po preteku njihove veljavnosti je treba ponoviti postopek, opisan v poglavju 4.1. Prošnja za izdajo digitalnega potrdila.

Tehnični postopek prevzema je odvisen od tipa potrdila in programske opreme na strani uporabnika.

Prevzem upravljanih (tip A) digitalnih potrdil se izvaja z uporabo Entrust programske opreme. Navodila za namestitev in uporabo Entrust programske opreme se nahajajo na spletni strani overitelja na naslovu http://www.simod-pki.mors.si.

Prevzem neupravljanih (tip B) digitalnih potrdil se izvaja preko spletnega vmesnika. Spletni naslov vmesnika, ter navodila za prevzem, so dostopna na spletnem naslovu http://www.simod-pki.mors.si.

4.4.1. Postopek potrditve prevzema digitalnega potrdila

Ob prevzemu digitalnega potrdila je imetnik dolžan preveriti istovetnost digitalnega potrdila na osnovi SIMoD-CA-Root korenskega digitalnega potrdila in vsebino digitalnega potrdila. S prvo uporabo oziroma, če imetnik 8 (osem) dni od prevzema digitalnega potrdila overitelja SIMoD-CA-Restricted ne obvesti o morebitnih napakah velja, da je imetnik potrdil točnost podatkov v digitalnem potrdilu in da prevzema tudi vse obveznosti in jamstva iz poglavja 9.6.3 Odgovornost in jamstva imetnikov digitalnih potrdil.

4.4.2. Objava digitalnega potrdila

Digitalna potrdila javnih ključev za zagotavljanje zaupnosti se po izdaji objavijo v imenikih iz poglavja 2.2. Objave informacij o digitalnih potrdilih. Overitelj SIMoD-CA-Restricted praviloma ne objavlja digitalnih potrdil javnih ključev za preverjanje podpisa.

4.4.3. Obveščanje drugih udeležencev o izdaji digitalnega potrdila

Ni predvideno.

4.5. Uporaba ključev in digitalnih potrdil

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

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, za podpisovanje digitalnih potrdil medsebojno priznanih overiteljev, ki niso del infrastrukture javnih ključev na MO, registrov preklicanih digitalnih potrdil in digitalnih potrdil operativnega osebja overitelja SIMoD-CA-Root. Overitelj SIMoD-CA-Root ne izdaja uporabniških digitalnih potrdil.

SIMoD-CA-Restricted, kot podrejeni overitelj korenskega overitelja SIMoD-CA-Root, uporablja svoje zasebne ključe samo za podpisovanje digitalnih potrdil, ki jih izdaja imetnikom (glej poglavje 1.3.3 Imetniki digitalnih potrdil), operativnemu osebju overitelja SIMoD-CA-Restricted, osebju prijavne službe in za podpisovanje registrov preklicanih potrdil.

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

4.5.1.2. Zasebni ključi in digitalna potrdila prijavne službe

Osebje prijavne službe lahko uporablja digitalno potrdilo SIMoD-CA-Restricted ali drugega overitelja SIMoD-PKI, izdano za izvajanje nalog prijavne službe, samo za te namene. V primeru, da zaposleni prijavne službe potrebujejo ključe oz. digitalna potrdila kot uporabniki oziroma za druge namene, kot je delo v prijavni službi, morajo zaprositi za izdajo uporabniškega digitalnega potrdila.

4.5.1.3. Imetniški zasebni ključi in digitalna potrdila

Imetniki lahko uporabljajo ključe in digitalna potrdila samo za namene, ki so definirani v Politiki SIMoD-PKI in Pravilih delovanja SIMoD-CA-Restricted.

Imetniki so dolžni varovati svoje zasebne ključe in pametne kartice ali drugačne nosilce zasebnih ključev in upoštevati vse ukrepe, da se prepreči izguba, razkritje, sprememba ali nepooblaščena uporaba.

Zasebni ključ za podpisovanje se hrani samo pri imetniku.

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 in Pravilih delovanja SIMoD-CA-Restricted.

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[14] digitalnih potrdil

4.7.1. Okoliščine obnove digitalnih potrdil

Digitalnega potrdila po preklicu ni možno samodejno obnoviti. Potrebno je ponoviti postopke od 4.1. Prošnja za izdajo digitalnega potrdila do 4.4. Prevzem digitalnega potrdila.

Samodejna obnova digitalnih potrdil je možna samo za veljavna digitalna potrdila izdana po PKIX-CMP protokolu pred pretekom njihove veljavnosti. Veljavnost digitalnih potrdil in pripadajočih zasebnih ključev je določena v poglavju 6.3.2 Obdobje veljavnosti ključev.

Samodejna obnova digitalnih potrdil izdanih na osnovi PKCS#10 protokola, oziroma zahtevka, ni možna. Za obnovo 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

Generiranje novih parov ključev ob obnovi digitalnega potrdila se izvaja samodejno po protokolu PKIX-CMP, kot je definiran v RFC 4210, ob prvi uporabi digitalnega potrdila z neposrednim dostopom do overiteljeve infrastrukture v obdobju stotih (100) dni pred zadnjim dnem veljavnosti zasebnega ključa. Generiranje novih parov ključev je možno samo v primeru, če je digitalno potrdilo, ki ga trenutno poseduje imetnik, veljavno. Imetniki, ki nimajo veljavnega digitalnega potrdila, morajo pridobiti novo digitalno potrdilo[15] oziroma ponoviti postopke od 4.1. Prošnja za izdajo digitalnega potrdila do 4.4. Prevzem digitalnega potrdila.

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

[15] V primeru, da uporabnik želi dešifrirati podatke, zaščitene z neveljavnim potrdilom, mora na vlogi za izdajo nevega potrdila obvezno izbrati še “Povrnitev zgodovine ključev za dešifriranje”, glej poglavje 4.12.1.1 Povrnitev zgodovine ključev za dešifriranje.

Samodejno obnovo digitalnih potrdil po PKIX-CMP protokolu brez preverjanja istovetnosti je možno izvesti dvakrat (2x) zaporedoma (poglavje 3.3.1.1 Preverjanje istovetnosti pri obnovi digitalnih potrdil z uporabo PKIX-CMP protokola).

Obnova digitalnih potrdil izdanih z uporabo PKCS#10 zahtevka, poteka po istem postopku kot prevzem prvega potrdila (poglavja od 4.1. Prošnja za izdajo digitalnega potrdila do 4.4. Prevzem digitalnega potrdila).

Obnova digitalnih potrdil izdajateljev časovnih žigov je izvedena pod kontrolo operativnega osebja izdajatelja časovnih žigov in operativnega osebja overitelja SIMoD-CA-Restricted.

Za obnovljena digitalna potrdila veljata Politika SIMoD-PKI in Pravila delovanja SIMoD-CA-Restricted, veljavna ob datumu generiranja novih parov ključev.

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 je možna samo za digitalna potrdila izdana po PKIX-CMP protokolu. Imetniki lahko zaprosijo za spremembo digitalnega potrdila v sledečih primerih:

- kadar se spremenijo podatki vsebovani v razločevalnem imenu (na primer priimek);
- zaradi spremembe naslova elektronske pošte, vsebovanega v *subjectAlternativeName* razširitvenem polju digitalnega potrdila.

Sprememba vsebine digitalnega potrdila 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).

4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila

4.9.1. Okoliščine preklica

4.9.1.1. Okoliščine preklica imetniških digitalnih potrdil

Razlogi za preklic digitalnih potrdil imetnikov so:

- dejanska ali domnevna zloraba zasebnih ključev;
- prenehanje delovnega razmerja imetnika;
- prenehanje delovanja organizacijske enote MO, ukinitev poveljniške dolžnosti oziroma prenehanje delovanja institucije, ki je povezana z obrambo države;
- sprememba statusa imetnika, zaposlenega v instituciji, ki je povezana z obrambo države, ki ima za posledico dejstvo, da imetnik ne opravlja več nalog povezanih z obrambo države;
- sprememba statusa institucije, ki je povezana z obrambo države, ki ima za posledico dejstvo, da institucija ne opravlja več nalog, povezanih z obrambo države;
- neizpolnjevanje obveznosti Politike SIMoD-PKI ali Pravil delovanja SIMoD-CA-Restricted.

Razlog za preklic digitalnih potrdil izdajateljev časovnih žigov je lahko tudi prenehanje delovanja izdajatelja časovnih žigov.

Razlog za preklic digitalnih potrdil imetnikov je lahko tudi sprememba podatkov, ki so vsebovani v digitalnem potrdilu, ob pogojih iz poglavja 4.8. Sprememba digitalnega potrdila.

4.9.1.2. Okoliščine preklica potrdila o priznavanju drugega overitelja

Ni relevantno. Medsebojno priznavanje je dovoljeno samo na nivoju korenskega overitelja SIMoD-CA-Root.

4.9.1.3. Okoliščine preklica potrdil podrejenih overiteljev

SIMoD-CA-Root lahko prekliče SIMoD-CA-Restricted overiteljevo digitalno potrdilo iz sledečih razlogov:

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

4.9.2. Kdo lahko zahteva preklic

4.9.2.1. Kdo lahko zahteva preklic imetniškega digitalnega potrdila

Zahtevo za preklic digitalnega potrdila imetnika lahko poda:

- imetnik za svoje digitalno potrdilo;
- pristojni vodja organizacijske enote MO oziroma predstojnik institucije, ki je povezana z obrambo države;
- skrbnik strežnika, druge strojne ali programske opreme, izdajatelja časovnega žiga ali podobnega ponudnika storitev overjanja;
- operativno osebje overitelja SIMoD-CA-Restricted Root, ki opravlja naloge prvega ali drugega varnostnega inženirja, če sumi, da imetnik krši pravila varnega poslovanja z digitalnim potrdilom;
- tretja oseba, če utemeljeno sumi, da je pri določenemu imetniku prišlo do zlorabe zasebnih ključev.

4.9.2.2. Kdo lahko zahteva preklic potrdila o priznavanju drugega overitelja

Ni relevantno.

4.9.2.3. Kdo lahko zahteva preklic potrdil podrejenih overiteljev

Preklic digitalnega potrdila overitelja SIMoD-CA-Restricted 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 imetnika mora overitelj SIMoD-CA-Restricted objaviti preklicano digitalno potrdilo v registru preklicanih potrdil.

Operativno osebje overitelja SIMoD-CA- Restricted obvesti o preklicu po elektronski pošti ali s priporočeno pošiljko imetnika ali odgovorno osebo.

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 potrdil.

4.9.3.1. Postopki preklica digitalnih potrdil imetnikov

Vloge za preklic se lahko posreduje na sledeče načine:

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

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

V primeru telefonsko posredovane vloge dežurna oseba posreduje vlogo za preklic operativnemu osebju overitelja SIMoD-CA-Restricted.

Preklic izvrši operativno osebje overitelja SIMoD-CA-Restricted.

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

4.9.3.2. Postopki preklica potrdila o priznavanju drugega overitelja

Preklic potrdila o priznavanju drugega overitelja izvede operativno osebje SIMoD-CA-Root overitelja v skladu s Politiko SIMoD-PKI.

4.9.3.3. Postopki preklica potrdil podrejenih overiteljev

Preklic digitalnega potrdila overitelja SIMoD-CA-Restricted se izvede v skladu s Pravili delovanja SIMoD-CA-Root.

V primeru preklica svojega digitalnega potrdila, bo overitelj SIMoD-CA-Restricted izvedel sledeče postopke:

- preklical vsa veljavna digitalna potrdila;
- zagotovil razpoložljivost registrov preklicanih potrdil vsaj še devetdeset (90) dni od preklica svojega potrdila;
- javno objavil objavil preklic svojega digitalnega potrdila;
- ustvaril nove ključe overitelja SIMoD-CA-Restricted;
- zaprosil korenskega overitelja SIMoD-CA-Root za izdajo novega digitalnega potrdila;
- izdal imetnikom nova digitalna potrdila.

Overitelj SIMoD-CA-Restricted bo po preklicu svojega 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 SIMoD-CA-Restricted;
- 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

Operativno osebje overitelja SIMoD-CA-Restricted izvede preklic v 8 urah po prejemu vloge za preklic v primeru:

- dejanske ali domnevne zlorabe zasebnih ključev;
- neizpolnjevanja obveznosti po tej politiki;
- prenehanja delovanja izdajatelja časovnih žigov.

Operativno osebje overitelja SIMoD-CA-Restricted izvede preklic v 24 urah po prejemu vloge za preklic v primeru:

- spremembe podatkov v digitalnem potrdilu;
- prenehanja delovnega razmerja imetnika;

- prenehanja delovanja organizacijske enote MO, ukinitve poveljniške dolžnosti ali prenehanja delovanja institucije, ki je povezana z obrambo države;
- spremembe statusa imetnika, zaposlenega v instituciji, ki je povezana z obrambo države, ki ima za posledico dejstvo, da imetnik ne opravlja več nalog povezanih z obrambo države;
- spremembe statusa institucije, ki je povezana z obrambo države, ki ima za posledico dejstvo, da institucija ne opravlja več nalog povezanih z obrambo države.

24-urni rok velja za primere, ko je bila sprememba v času oddaje vloge že v veljavi. V primerih, ko je bila vloga oddana pred uveljavitvijo spremembe, ki pogojuje preklic digitalnega potrdila, 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.

4.9.5.2. Čas za preklic potrdila o priznavanju drugega overitelja

Ni relevantno.

4.9.5.3. Čas za preklic potrdila podrejenega overitelja

Overitelj SIMoD-CA-Root prekliče digitalno potrdilo overitelja SIMoD-CA-Restricted, kakor tudi potrdila drugih podrejenih overiteljev takoj, ko prejme zahtevek, ali v roku, ki ga določi Svet za upravljanje z infrastrukturo javnih ključev na MO.

4.9.6. Obveza preverjanja registra preklicanih potrdil

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

Uporaba digitalnih potrdil v aplikacijah, ki ne preverjajo statusa digitalnih potrdil, praviloma ni dovoljena, razen v 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

Veljavnost registrov preklicanih potrdil, ki jih izdaja overitelj SIMoD-CA-Restricted, je 25 ur. Overitelj SIMoD-CA-Restricted objavi nov register preklicanih potrdil pred potekom veljavnosti starega.

Ob preklicu digitalnega potrdila overitelj SIMoD-CA-Restricted takoj objavi nov register preklicanih potrdil.

4.9.8. Dovoljene zakasnitve pri objavi registrov preklicanih potrdil

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

Overitelj SIMoD-CA-Restricted izda nove registre preklicanih potrdil vsaj toliko časa pred iztekom veljavnosti starih, da je zagotovljen prenos registrov do vseh komponent repozitorija še pred iztekom veljavnosti starega registra.

4.9.9. Storitev sprotnega preverjanje statusa digitalnih potrdil

Storitev sprotnega preverjanja statusa digitalnih potrdil (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 postopke določene v Politiki SIMoD-PKI in Pravilih delovanja overitelja SIMoD-CA-Root.

Preklic digitalnega potrdila korenskega overitelja SIMoD-CA-Root ima vedno za posledico preklic digitalnega potrdila overitelja SIMoD-CA-Restricted. Overitelj SIMoD-CA-Restricted bo v tem primeru postopal kot je opisano v poglavju 4.9.3.3 Postopki preklica potrdil podrejenih overiteljev.

4.9.13. Okoliščine za začasno ukinitev veljavnosti

Ni podprto.

4.9.14. Kdo lahko zahteva začasno ukinitev veljavnosti

Ni podprto.

4.9.15. Postopki za začasno ukinitev veljavnosti

Ni podprto.

4.9.16. Omejitve obdobja začasne ukinitve veljavnosti

Ni podprto.

4.10. Storitve objavljanja statusa digitalnih potrdil

4.10.1. Tehnične lastnosti storitve

Status digitalnih potrdil je mogoče preveriti v registrih preklicanih potrdil, ki so dostopni v imeniku in na spletni strani iz poglavja 2.2. Objave informacij o digitalnih potrdilih. Naslov registra preklicanih potrdil je vsebovan v razširitvenem polju *CRLDistributionPoints* vseh digitalnih potrdil, ki jih izda overitelj SIMoD-CA-Restricted.

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

Zaradi navedenih razlogov imetnik ni več upravičen do digitalnega potrdila:

- prenehanje delovnega razmerja imetnika;
- prenehanje delovanja organizacijske enote MO, ukinitev poveljniške dolžnosti oziroma prenehanje delovanja institucije, ki je povezana z obrambo države[16];
- sprememba statusa imetnika, zaposlenega v instituciji, ki je povezana z obrambo države, ki ima za posledico dejstvo, da imetnik ne opravlja več nalog povezanih z obrambo države;

[16] v primeru potrdil za notranje organizacijske enote MO ter poveljniške dolžnosti v SV

- sprememba statusa institucije, ki je povezana z obrambo države, ki ima za posledico dejstvo, da institucija ne opravlja več nalog, povezanih z obrambo države[17];
- prenehanje potrebe po varnostni storitvi strežnika ali druge strojne ali programske opreme[18];
- prenehanje potrebe po storitvi izdajanja časovnih žigov ali podobni storitvi overjanja[19].

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

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

4.12. Postopki dela za varnostno kopiranje in odkrivanje zasebnega ključa

Hranjenje zasebnih ključev pri zunanjih subjektih (ang. key escrow) ni dovoljeno. Dovoljeno je samo varnostno kopiranje zasebnih ključev (ang. key backup) in odkrivanje zasebnih ključev (ang. key recovery) pri overitelju SIMoD-CA-Restricted.

Overitelj SIMoD-CA-Restricted zagotavlja varnostno kopiranje zasebnih ključev (ang. 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

Overitelj SIMoD-CA-Restricted omogoča povrnitev zgodovine ključev za dešifriranje za digitalna potrdila za šifriranje za storitve zagotavljanja tajnosti oziroma zaupnosti, VISOKE stopnje zaupanja, z identifikacijsko oznako 1.3.6.1.4.1.22295.10.1.1.1.1.2.0, izdana po PKIX-CMP protokolu.

Povrnitev zgodovine ključev za dešifriranje se lahko izvede, če imetnik digitalnega potrdila:

- pozabi geslo za dostop do zasebnih ključev;
- izgubi ali poškoduje pametno kartico ali drugačen nosilec zasebnih ključev;
- ni uporabil digitalnega potrdila v predpisanem prehodnem obdobju za avtomatično obnovo ključa (poglavje 4.7. Obnova digitalnih potrdil).

Povrnitev zgodovine ključev za dešifriranje se izvede na osnovi vloge za izdajo digitalnega potrdila z obvezno izbiro *Povrnitev zgodovine ključev za dešifriranje*. Postopki se izvedejo v skladu s poglavji od 4.1. Prošnja za izdajo digitalnega potrdila do 4.4. Prevzem digitalnega potrdila.

4.12.1.2. Odkrivanje kopije ključev za dešifriranje

Overitelj SIMoD-CA-Restricted omogoča odkrivanje kopije ključev za dešifriranje za digitalna potrdila za šifriranje za storitve zagotavljanja tajnosti oziroma zaupnosti, VISOKE stopnje zaupanja, z identifikacijsko oznako 1.3.6.1.4.1.22295.10.1.1.1.1.2.0, izdana po PKIX-CMP protokolu.

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

- imetnikovemu predstojniku na podlagi vloge za odkrivanje kopije ključev za dešifriranje;
- če to odredi pristojno sodišče, sodnik za prekrške ali upravni organ.

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

[17] v primeru potrdil za institucije, ki opravljajo naloge, ki so povezane z obrambo

[18] v primeru potrdil za strežnike in drugo strojno ter programsko opremo

[19] v primeru potrdil za izdajatelje časovnih žigov in podobnih ponudnikov storitev overjanja

Overitelj SIMoD-CA-Restricted pred odkrivanjem kopije ključev za dešifriranje:

- po elektronski pošti obvesti imetnika digitalnega potrdila o datumu ter vlagatelju vloge za odkrivanje kopije njegovih ključev za dešifriranje podatkov in
- prekliče veljavnost digitalnega potrdila in po elektronski pošti o preklicu obvesti imetnika.

Če je v vlogi zahtevano takojšnje odkritje kopije, bo overitelj v roku 24 ur od prejetja vloge izvedel postopek odkrivanja kopije zasebnega ključa za dešifriranje in jo posredovati predstojniku ali subjektu, ki je naveden v odločbi sodišča ali upravnega organa.

4.12.2.Zaščita odkritega zasebnega ključa in postopek prenosa

Postopek prenosa odkritega zasebnega ključa je enak kot postopek prenosa dešifrirnega zasebnega ključa ob kreiranju novega digitalnega potrdila, torej v skladu z drugim odstavkom poglavja 4.3.1.1 Dostava zasebnega ključa imetniku.

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-Restricted se izvajajo v ustrezno varovanih prostorih in na varni lokaciji.

Prostori izpolnjujejo pogoje za namestitev komunikacijske in informacijske opreme ter arhivskih medijev skladno s predpisi, ki urejajo področje tajnih podatkov. Komunikacijska in informacijska oprema overitelja SIMoD-CA-Restricted je nameščena v prostorih varnostnega območja I. stopnje.

5.1.2. Fizični dostop

Nadzor fizičnega dostopa izvaja pristojna služba MO.

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

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

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

5.1.3. Napajanje in klimatske naprave

Prostor s komunikacijsko in informacijsko opremo overitelja SIMoD-CA-Restricted je opremljen s:

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

5.1.4. Zaščita pred poplavo

Prostori s komunikacijsko in informacijsko opremo overitelja SIMoD-CA-Restricted 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-Restricted 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 overitelja SIMoD-CA-Restricted.

5.1.7. Odstranjevanje odpadkov

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

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

5.1.8. Hranjenje na oddaljeni lokaciji

Overitelj SIMoD-CA-Restricted uporablja oddaljeno lokacijo za varno hranjenje varnostnih kopij in arhivskih podatkov. Podatki, mediji ali naprave so na oddaljeni lokaciji shranjene v varovanih prostorih, ki zagotavljajo enako raven varnosti kot je v prostorih overitelja SIMoD-CA-Restricted.

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

5.2. Organizacijski varnostni ukrepi

5.2.1. Organizacija overitelja SIMoD-CA-Restricted

5.2.1.1. Operativno osebje

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

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

Posamezni operativni osebi je dovoljeno opravljanje nalog samo znotraj ene zaključene organizacijske skupine. Posamezna oseba, ki izvaja naloge v okviru operativnega osebja overitelja SIMoD-CA- Restricted, lahko opravlja naloge tudi za druge overitelje SIMoD-PKI.

V organizacijski skupini za upravljanje z digitalnimi potrdili so:

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

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

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

V organizacijski skupini za varovanje in nadzor komunikacijskega sistema 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-Restricted.

5.2.1.2. Prijavna služba

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

- sprejemanje vlog za izdajo in preklic digitalnega potrdila;

- preverjanje istovetnosti naročnikov oziroma imetnikov in točnosti podatkov v vlogah za izdajo in preklic digitalnega potrdila;
- hranjenje dokazila o postopkih preverjanja istovetnosti;
- posredovanje vlog operativnemu osebju, ki upravlja z digitalnimi potrdili;
- obveščanje operativnega osebje overitelja SIMoD-CA-Restricted, ki upravlja z digitalnimi potrdili, o spremembi podatkov imetnika digitalnega potrdila (npr. prekinitev delovnega razmerja, premestitev v drugo organizacijsko enoto).

5.2.1.3. Druge funkcije

Pristojne organizacijske enote v MO skrbijo za:

- fizično varovanje in nadzor prostorov overitelja SIMoD-CA-Restricted;
- pravne zadeve.

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

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

5.2.2. Število oseb, potrebnih za izvedbo postopkov

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

- generiranje kriptografskih ključev overitelja SIMoD-CA-Restricted;
- preklic overiteljevega potrdila;
- spreminjanje gesel aplikacije za delo z overiteljem SIMoD-CA-Restricted;
- ponovno šifriranje overiteljeve baze podatkov;
- nastavitev števila potrebnih prisotnih varnostnih inženirjev za izvedbo kritičnih operacij pri upravljanju s potrdili;
- restavriranje prijavnih imen varnostnih inženirjev;
- spreminjanje nastavitve zgoščevalnih algoritmov;
- spreminjanje nastavitev kriptografskih algoritmov;
- aktiviranje avtomatskega zagona overiteljevih servisov;
- 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 oseb iz skupine za upravljanje z digitalnimi potrdili s funkcijo prvega ali drugega varnostnega inženirja:

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

5.2.3. Preverjanje istovetnosti operativnega osebja

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

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

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

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

5.3. Zahteve za osebje overitelja

5.3.1. Kvalifikacije, izkušnje in varnostno preverjanje

Operativno osebje overitelja SIMoD-CA-Restricted:

- mora biti ustrezno usposobljeno in o tem imeti dokazila;
- mora imeti za opravljanje nalog pri overitelju SIMoD-CA-Restricted imenovanje Svet za upravljanje z infrastrukturo javnih ključev na MO a SIMoD-PKI;
- ne sme opravljati drugih nalog, ki bi bile v nasprotju z opravljanjem nalog v okviru infrastrukture javnih ključev na MO;
- ne sme biti na prejšnjih podobnih dolžnostih (npr. skrbnik kriptografskih naprav, varnostni inženir v informacijskem sistemu) razrešeno nalog zaradi malomarnosti ali neizpolnjevanja obveznosti;
- 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 (Uradni list RS, št. 50/06).

5.3.3. Usposabljanje osebja overitelja

5.3.3.1. Usposabljanje osebja overitelja

Operativno osebje overitelja SIMoD-CA-Restricted 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.

Osebje prijavne službe je usposobljeno za:

- identifikacijo naročnikov in preverjanje pravilnosti podatkov v vlogah;
- delo s programsko opremo prijavne službe.

5.3.3.2. Usposabljanje osebja za pomoč uporabnikom

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

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

5.3.4. Pogostost dodatnih usposabljanj

Osebje mora pridobiti potrebna znanja pred vsako nadgradnjo.

5.3.5. Kroženje med delovnimi mesti

Ni predpisano.

5.3.6. Ukrepi ob kršitvah pooblastil

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

5.3.7. Zunanji izvajalci

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

5.3.8. Dokumentacija za osebje overitelja

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

5.4. Postopki varnostnih pregledov sistema

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

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

5.4.1. Vrste beleženih dogodkov

Overitelj SIMoD-CA-Restricted beleži naslednje vrste dogodkov:

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

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

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

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

5.4.2. Pogostost pregleda dnevnikov beleženih dogodkov

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

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

Operativno osebje overitelja SIMoD-CA-Restricted 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-Restricted.

Dostop do dnevnikov beleženih dogodkov je dovoljen samo pooblaščenim osebam:

- Svetu za upravljanje z infrastrukturo javnih ključev na MO,
- operativnemu osebju overitelja SIMoD-CA-Restricted v okviru svojih delovnih nalog,
- 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 dnevno v okviru rednega varnostnega kopiranja sistemov. Enkrat mesečno 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 SIMoD-CA-Restricted z namenom odkrivanja in odprave ranljivosti. Ugotovljeno ranljivost se oceni s stališča verjetnosti povzročitve škode in predvidi ukrepe za zmanjšanje grožnje.

5.5. Arhiviranje podatkov

5.5.1. Vrste arhiviranih podatkov

Overitelj SIMoD-CA-Restricted hrani naslednje podatke:

- dnevnike beleženih dogodkov iz poglavja 5.4.1 Vrste beleženih dogodkov;
- vloge imetnikov digitalnih potrdil;
- dokumentacijo o izvedbi postopka izdaje digitalnih potrdil;
- korespondenco in pogodbe imetnikov digitalnih potrdil z overiteljem SIMoD-CA-Restricted;
- digitalna potrdila in liste preklicanih potrdil;
- verzije pravil delovanja overitelja SIMoD-CA-Restricted, tako javnih kot 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-Restricted hrani dnevnike beleženih dogodkov najmanj pet (5) let od posameznega dogodka ali dejanja.

Overitelj SIMoD-CA-Restricted hrani vloge imetnikov, korespondenco in pogodbe imetnikov z overiteljem SIMoD-CA-Restricted najmanj pet (5) let od zaključka zadeve, ki je vezana na vlogo, korespondenco ali pogodbo oziroma od zadnjega dne veljavnosti digitalnega potrdila, ki je povezano s hranjeno vlogo, korespondenco ali pogodbo.

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

5.5.3. Zaščita arhiva

Podatki, ki sodijo v dokumentarno gradivo (vloge imetnikov, dokumentacija o izvedbi identifikacije, korespondenca in pogodbe imetnikov digitalnih potrdil z overiteljem SIMoD-CA-Restricted, pravila delovanja overitelja SIMoD-CA-Restricted in dnevniki beleženih dogodkov v pisni obliki), se hranijo in arhivirajo v skladu s postopki dela z dokumentarnim gradivom v MO.

Arhivirani podatki, ki se beležijo v okviru informacijskega sistema (avtomatsko generirani dnevniki beleženih dogodkov, digitalna potrdila in liste preklicanih potrdil ter zasebni dešifrirni ključi), se nahajaja v dveh kopijah na ločenih lokacijah. 1x letno se preverja integriteta medijev z arhiviranimi podatki. Arhiv, ki se hrani na drugi lokaciji, je zaščiten z ekvivalentnimi varnostnimi mehanizmi, kot so implementirani v prostorih overitelja SIMoD-CA-Restricted.

5.5.4. Varnostna kopija arhiva

Podatkom, ki sodijo v dokumentarno gradivo (vloge imetnikov, dokumentacija o izvedbi identifikacije, korespondenca in pogodbe imetnikov digitalnih potrdil z overiteljem SIMoD-CA-Restricted, pravila delovanja overitelja SIMoD-CA-Restricted in dnevniki beleženih dogodkov v pisni obliki), se zagotavlja razpoložljivost arhiva v skladu s postopki dela z dokumentarnim gradivom v MO.

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

5.5.5. Časovno žigosanje zapisov

Ni predpisano.

5.5.6. Način arhiviranja

Ni predpisano.

5.5.7. Postopek vpogleda v in verifikacije arhiva

Ob kreiranju arhiva se preveri integriteta medija. 1x letno se preverja integriteta medijev z arhiviranimi podatki in možnost branja podatkov iz arhiva. Dostop do arhiva je možen samo

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

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

5.6. Obnova digitalnih potrdil overiteljev

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

V skladu s poglavjem 5.6.1. Obnova samopodpisanega potrdila korenskega overitelja SIMoD-CA-Root Pravil delovanja overitelja SIMoD-CA-Root, javni del.

5.6.2. Obnova potrdila overitelj SIMoD-CA-Restricted

Za overitelja SIMoD-CA-Restricted kot podrejenega overitelja korenskega overitelja SIMoD-CA-Root veljajo določbe poglavja 5.6.2. Obnova potrdil podrejenih overiteljev v SIMoD-PKI Pravil delovanja overitelja SIMoD-CA-Root, javni del.

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 SIMoD-CA-Restricted.

5.7.2. Uničenje programske, strojne opreme ali podatkov overitelja

V primeru okvare strojne ali programske opreme oziroma podatkov, pri kateri zasebni ključ overitelja SIMoD-CA-Restricted ni bil uničen, bodo storitve overitelja SIMoD-CA-Restricted vzpostavljene nazaj v najkrajšem možnem času. Overitelj SIMoD-CA-Restricted bo v najkrajšem možnem času vzpostavil vsaj funkcionalnost 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 SIMoD-CA-Restricted objavil preklic svojega potrdila in ukrepal v skladu s poglavjem 4.9.3.3 Postopki preklica potrdil podrejenih overiteljev oziroma 4.9.12 Posebne zahteve glede zlorabe ključa.

V primeru okvare, kjer pride do uničenja overiteljevega zasebnega ključa in vseh njegovih kopij, se postopa, kot da je prišlo do zlorabe ključa v skladu s poglavjem 4.9.3.3 Postopki preklica potrdil podrejenih overiteljev oziroma 4.9.12 Posebne zahteve glede zlorabe ključa. 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 SIMoD-CA-Restricted 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 SIMoD-CA-Restricted oziroma uničenje in poškodovanje varovanih prostorov overitelja SIMoD-CA-Restricted, so predpisani v zaupnem delu notranjih pravil delovanja overitelja.

5.8. Prenehanje delovanja overitelja

Odločitev za prenehanje delovanja overitelja SIMoD-CA-Restricted so vzroki podani v poglavju 4.9.1.3 Okoliščine preklica potrdil podrejenih overiteljev oziroma 4.9.12 Posebne zahteve glede zlorabe ključa ali prenehanje potrebe po storitvah overitelja SIMoD-CA-Restricted. Odločitev o prenehanju delovanja izda Svet za upravljanje z infrastrukturo javnih ključev na MO.

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

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

- celotno operativno osebje overitelja SIMoD-CA-Restricted;
- vse imetnike oziroma odgovorne osebe;
- 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.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev para ključev

6.1.1. Generiranje para ključev

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

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

Ključi imetnikov upravljanih (tip A) digitalnih potrdil se generirajo:

Ključ	Stopnja zaupanja	Se generira	Se hrani	Kopija ključa
zasebni ključ za dešifriranje	VISOKA	pri overitelju	na uporabnikovi pametni kartici	šifrirana v bazi overitelja
javni ključ za šifriranje	VISOKA	pri overitelju	na uporabnikovi pametni kartici	v vsaki kopiji digitalnega potrdila za šifriranje
zasebni ključ za digitalni podpis	VISOKA	na uporabnikovi pametni kartici	na uporabnikovi pametni kartici	ne obstaja
zasebni ključ za preverjanje digitalnega podpisa	VISOKA	na uporabnikovi pametni kartici	na uporabnikovi pametni kartici	v vsaki kopiji digitalnega potrdila za preverjanje digitalnega podpisa
zasebni ključ za digitalni podpis in dešifriranje	VISOKA	na uporabnikovi pametni kartici	na uporabnikovi pametni kartici	ne obstaja
javni ključ za preverjanje digitalnega podpisa in šifriranje	VISOKA	na uporabnikovi pametni kartici	na uporabnikovi pametni kartici	v vsaki kopiji digitalnega potrdila za preverjanje digitalnega podpisa in šifriranje
zasebni ključ za digitalni podpis in dešifriranje	SREDNA	na uporabnikovi pametni kartici, ali v programski opremi pri uporabniku	na uporabnikovi pametni kartici, ali v programski opremi pri uporabniku	šifrirana v bazi overitelja, če se generira v programski opremi pri uporabniku
javni ključ za preverjanje digitalnega podpisa in šifriranje	SREDNA	na uporabnikovi pametni kartici, ali v programski opremi pri uporabniku	na uporabnikovi pametni kartici, ali v programski opremi pri uporabniku	v vsaki kopiji digitalnega potrdila za preverjanje digitalnega podpisa in šifriranje

Ključi imetnikov neupravljanih (tip B) digitalnih potrdil se generirajo:

Ključ	Stopnja zaupanja	Se generira	Se hrani	Kopija ključa
zasebni ključ za digitalni podpis in dešifriranje	VISOKA	na uporabnikovi pametni kartici	na uporabnikovi pametni kartici	ne obstaja
javni ključ za preverjanje digitalnega podpisa in šifriranje	VISOKA	na uporabnikovi pametni kartici	na uporabnikovi pametni kartici	v vsaki kopiji digitalnega potrdila za preverjanje digitalnega podpisa in šifriranje
zasebni ključ za digitalni podpis in dešifriranje	SREDNA	na uporabnikovi pametni kartici, ali v programski opremi pri uporabniku	na uporabnikovi pametni kartici, ali v programski opremi pri uporabniku	ne obstaja
javni ključ za preverjanje digitalnega podpisa in šifriranje	SREDNA	na uporabnikovi pametni kartici, ali v programski opremi pri uporabniku	na uporabnikovi pametni kartici, ali v programski opremi pri uporabniku	v vsaki kopiji digitalnega potrdila za preverjanje digitalnega podpisa in šifriranje

6.1.2. Dostava zasebnega ključa imetniku

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

Par ključev za podpisovanje se vedno ustvari na strani bodočega imetnika. Zasebni ključ za podpisovanje se nikdar ne generira, ne prenaša in ne hrani na strojni ali programski opremi overitelja.

6.1.3. Dostava imetnikovega javnega ključa overitelju

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

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.

Uporabniki 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 SIMoD-CA-Restricted overitelja je 2048 bitov.

Imetniki digitalnih potrdil imajo 2048 bitov dolg RSA zasebni ključ za podpisovanje in 2048 bitov dolg RSA zasebni ključ za dešifriranje.

Izdajatelji varnega časovnega žiga imajo 2048 bitov dolg RSA zasebni ključ za podpisovanje.

6.1.6. Parametri za generiranje javnih ključev in preverjanje parametrov

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

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 v3 oziroma RFC 3280.

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

V primeru potrdil za izdajatelje časovnih žigov se par ključev v povezavi s šifrirnim potrdilom v praksi ne uporablja, par ključev v povezavi s potrdilom za verifikacijo podpisa pa se uporablja za digitalno podpisovanje za podpisovanje časovnih žigov. Razširjena uporaba ključa (*extKeyUsage*) za verifikacijo podpisa je časovno žigosanje.

Tabela prikazuje dovoljene vrednosti razširitvenega polja za posamezno vrsto digitalnega potrdila:

Stopnja zaupanja	Namen uporabe oziroma storitev	keyCertSign	CRLSign	DigitalSignature	KeyEncipherment
VISOKA	Digitalna potrdila za preverjanje digitalnega podpisa za storitve prepoznavanja in preverjanja istovetnosti, celovitosti in nezanikanja.			X	
VISOKA	Digitalna potrdila za šifriranje za storitve zagotavljanja tajnosti, oziroma zaupnosti.				X
VISOKA	Digitalna potrdila za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe.			X	X
SREDNJA	Digitalna potrdila za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe.			X	X
VISOKA	Digitalna potrdila za izdajatelje časovnih žigov.			X	

Razširitveno polje *NonRepudiation* se ne uporablja.

Potrdilo za izdajatelja časovnih žigov ima dodatno X.509 razširitveno polje *extKeyUsage* z vrednostjo *id-kp-timeStamping*.

6.2. Zaščita zasebnih ključev in tehnične kontrole kriptografskih modulov

6.2.1. Standardi za kriptografski modul

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

6.2.1.1. Kriptografski moduli izdajateljev časovnega žiga

Generiranje zasebnega kluča za časovno žigosanje se mora izvajati v strojnem varnostnem kriptografskem modulu, ki ima potrdilo o skladnosti z enem 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.

6.2.1.2. Pametne kartice za uporabniška digitalna potrdila

Operativno osebje overiteljev in prijavne službe uporablja pametne kartice ali podobne nosilce ključev stopnje varnosti FIPS 140-2 level 2.

Imetniki digitalnih potrdil VISOKE stopnje zaupanja z obvezno uporabo pametne kartice uporabljajo pametne kartice ali podobne nosilce ključev stopnje varnosti FIPS 140-2 level 2. Kriptografski modul se uporablja na način, da zasebni ključ pametne kartice nikoli ne zapusti.

Par ključev za podpisovanje se vedno generira na strojni opremi, to je na pametni kartici, ki ustreza FIPS 140-2 level 2.

Par ključev za šifriranje, za katera overitelj zagotavlja povrnitev zgodovine ključev se generira pri overitelju in varno prenese na pametno kartico imetnika. Modul ustreza vsaj FIPS 140-2 level 2.

6.2.1.3. Programsko hranjenje zasebnih ključev

Imetniki digitalnih potrdil SREDNJE stopnje zaupanja uporabljajo programske kriptografske module vsaj stopnje varnosti FIPS 140-2 level 1, ali na pametni kartici vsaj stopnje varnosti FIPS 140-2 level 1.

6.2.2. Nadzor zasebnega ključa overitelja z več pooblaščenimi osebami

Za operacije, kjer se upravlja z zasebnim ključem overitelja 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-Restrited overitelja ni možno. Tehnična izvedba varnostnega kriptografskega modula ne omogoča prikaza zasebnega ključa overitelja v nešifrirani obliki.

Odkrivanje zasebnega ključa izdajateljev časovnih žigov ni dovoljeno.

Povrnitev zgodovine in odkrivanje kopije imetniških zasebnih ključev za dešifriranje je možno ob pogojih določenih v Politiki SIMo-PKI, poglavja 4.12.1.1 Povrnitev zgodovine ključev za dešifriranje oziroma 4.12.1.2 Odkrivanje kopije ključev za dešifriranje.

6.2.4. Varnostno kopiranje zasebnih ključev

Varnostna kopija zasebnega ključa overitelja 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[20] od M[21] administratorskih pametnih karticah varnostnega kriptografskega modula.

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

6.2.5. Arhiviranje zasebnega ključa

Overiteljev zasebni ključ se ne arhivira.

Arhivira se samo zasebne dešifrirne ključe imetniških digitalnih potrdil za katera overitelj zagotavlja storitev povrnitve zgodovine ključev.

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

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

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.

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

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

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

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

6.2.7. Hranjenje zasebnega ključev v kriptografskem modulu

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

Zasebni ključi izdajateljev časovnih žigov se morajo hraniti na varnostnem kriptografskem modulu, ali v varnostni kopiji v šifririani obliki in se nikdar ne smejo pojaviti izven modula v nešifrirani obliki.

6.2.8. Postopek za aktiviranje zasebnega ključa

Overiteljev zasebni ključ se aktivira ob zagonu overiteljeve aplikativne programske opreme. Za aktiviranje je potrebno predložiti operatersko pametno kartico varnostnega kriptografskega modula ter geslo administratorja overitelja.

Zasebni ključ izdajateljev časovnega žiga se aktivirajo ob zagonu aplikativne programske opreme. Za aktiviranje je potrebno predložiti operatersko pametno kartico za aktiviranje varnostnega kriptografskega modula.

Imetniki digitalnih potrdil morajo uporabljati ustrezno uporabniško programsko opremo, ki preveri istovetnost uporabnika z geslom in po uspešnem preverjanju istovetnosti aktivira zasebni ključ.

6.2.9. Postopek za deaktiviranje zasebnega ključa

Zasebni ključ overitelja se deaktivira z zaustavitvijo aplikativne programske opreme overitelja.

Zasebni ključ izdajateljev časovnega žiga se deaktivira z zaustavitvijo aplikativne programske opreme izdajatelja časovnega žiga.

Imetniki digitalnih potrdil morajo uporabljati uporabniško programsko opremo, ki deaktivira zasebni ključ, ko se imetniki odjavijo oziroma ko poteče določen čas neaktivnosti (10 minut).

Ob zaustavitvi aplikativne programske opreme overitelja oziroma izdajatelja časovnega žiga se uničijo vsi ključi, ki se nahajajo v delovnem pomnilniku varnostnega kriptografskega modula. Zasebni ključi overitelja in izdajateljev časovnega žiga se nikoli ne nahajajo v sistemskem pomnilniku, temveč samo v strojni opremi varnostnega kriptografskega modula.

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

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

6.2.10.Postopek za uničenje zasebnega ključa

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

Zasebne ključe izdajateljev časovnih žigov je potrebno uničiti, ko jim poteče obdobje uporabe, oziroma se ne uporabljajo več iz drugih razlogov. Ob uničenju ključev je potrebno uničiti aktivno kopijo 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 arhivira svoj javni ključ za verifikacijo podpisa in imetniške javne ključe v povezavi z potrdili za verifikacijo podpisa kot del arhiviranja digitalnih potrdil (glej poglavje 5.5. Arhiviranje podatkov). Javni ključi v povezavi s šifrirnimi digitalnimi potrdili se ne arhivirajo.

6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil

Veljavnost javnih in zasebnih ključev overiteljev:

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

Veljavnost javnih in zasebnih ključev imetnikov:

Stopnja zaupanja	Namen uporabe oziroma storitev	Ključ	Veljavnost
VISOKA	Digitalna potrdila za preverjanje digitalnega podpisa za storitve prepoznavanja in preverjanja istovetnosti, celovitosti in nezanikanja.	zasebni	dve (2) leti
		javni	tri (3) leta
VISOKA	Digitalna potrdila za šifriranje za storitve zagotavljanja tajnosti, oziroma zaupnosti.	zasebni	neomejeno
		javni	dve (2) leti
VISOKA	Digitalna potrdila za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe[22].	Zasebni	dve (2) leti
		javni	dve (2) leti
SREDNJA	Digitalna potrdila za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe.	zasebni	dve (2) leti
		javni	dve (2) leti
VISOKA	Digitalna potrdila za izdajatelje časovnih žigov.	zasebni	tri (3) leta
		javni	šest (6) let

[22] Brez omejitve uporabe v smislu varnostnih storitev in aplikacij.

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

Aktivacijski podatki za prevzem imetniških digitalnih potrdil se ustvarijo v aplikativni programski opremi overitelja. Aktivacijski podatki so ustvarjeni z generatorjem naključnih kod in so edinstveni.

6.4.1.1. Aktivacija pametnih kartic

Za aktiviranje pametne kartice je potrebno geslo, oziroma PIN koda. Gesla za dostop do pametnih kartic določijo imetniki. Pri temu morajo upoštevati zahteve navedene v poglavju 6.4.3 Drugi vidiki aktivacijskih podatkov.

6.4.1.2. Začetna aktivacija pametnih kartic

Za začetno aktiviranje pametne kartice niso potrebni nobeni aktivacijski podatki.

6.4.2. Zaščita aktivacijskih podatkov

Aktivacijski podatki, ki so ustvarjeni pri overitelju, se hranijo na način, ki zagotavlja njihovo zaupnost. Aktivacijski podatki se pod nadzorom overiteljevega osebja za upravljanje z digitalnimi potrdili tiskajo na kuverte, ki onemogočajo vpogled v vsebino (slepe kuverte). Aktivacijski podatki se dostavijo imetniku v skladu s poglavjem 174.1.2 Postopek obdelave vloge in odgovornosti.

6.4.3. Drugi vidiki aktivacijskih podatkov

Bodoči imetnik ne sme izdelovati kopij aktivacijskih podatkov, jih prepisovati ali kako drugače razkriti. Po prevzemu digitalnega potrdila jih mora uničiti.

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

6.5. Varnostne zahteve za računalnike

6.5.1. Specifične tehnične varnostne zahteve za računalnike

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

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

6.5.2. Raven varnostne zaščite računalnikov

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

6.6. Tehnični nadzor življenjskega cikla overitelja

6.6.1. Nadzor razvoja sistema

Strojna oprema, operacijski sistemi, ter programska oprema overitelja so komercialni proizvodi.

6.6.2. Upravljanje varnosti

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

Operativno osebje overitelja 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 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, oziroma upravljanje varnosti skozi celoten življenski je v skladu z 6.6.2 Upravljanje varnosti.

6.7. Varnostne kontrole na ravni računalniškega omrežja

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

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

SIMoD-CA-Restricted 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. Digitalna potrdila vsebujejo naslednja osnovna polja:

Osnovno polje - angleški naziv	Osnovno polje – slovenski naziv in opis	Vrednost
Signature	overiteljev podpis	sha1WithRSAEncryption (1.2.840.113549.1.1.5) <podpis potrdila s strani overitelja >
Issuer	izdajatelj	<razločevalno ime SIMoD-CA-Restricted>
Validity	pričetek in konec veljavnosti potrdila	<pričetek veljavnosti po GMT> <konec veljavnosti po GMT>
Subject	imetnik	< razločevalno ime imetnika>
SubjectPublicKeyInformation	algoritem za javni ključ	rsaEncryption (1.2.840.113549.1.1.1),<modul, eksponent, vrednost javnega ključa>
Version	verzija potrdila X.509	2 (kar pomeni verzijo 3)
SerialNumber	enolična serijska številka	<enolična serijska številka>

7.1.2. Razširitvena polja

Razširitvena polja so namenjena uporabi dodatnih atributov v X.509v3 potrdilih. Overitelj SIMoD-CA-Restricted 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 spodnjih tabelah. Polja definirana v RFC 3280, ki niso navedena v tabelah, se ne uporabljajo.

Zaradi preglednosti je v tabeli podano digitalno potrdilo korenskega overitelja SIMoD-CA-Root.

Digitalno potrdilo korenskega overitelja SIMoD-CA-Root, overitelja SIMoD-CA-Restricted in digitalna potrdila izdajateljev časovnega žiga vsebujejo naslednja razširitvena polja:

Polje (Field)	Potrdilo overitelja SOMoD-CA-Root	Potrdilo overitelja SOMoD-CA-Restricted	Digitalna potrdila za izdajatelje časovnih žigov
odtis javnega ključa overitelja (authority Key Identifier)	Ni uporabljeno	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Root s katerim je podpisano potrdilo	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Restricted s katerim je podpisano potrdilo
odtis imetnikovega javnega ključa (subject Key Identifier)	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Root	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Restricted	SHA-1 odtis imetnikovega javnega ključa
namen uporabe ključa (key Usage)	**Kritično** keyCertSign cRLSign	**Kritično** keyCertSign cRLSign	**Kritično** digitalSignature
razširjen namen uporabe (extended Key Usage)	Ni uporabljeno	Ni uporabljeno	**Kritično** id-kp-timeStamping
obdobje veljavnosti zasebnega ključa (privateKeyUsagePeriod)	V skladu s poglavjem 6.3.2	V skladu s poglavjem 6.3.2	V skladu s poglavjem 6.3.2
OID oznaka tipa potrdila (certificate Policies)	Ni uporabljeno	Ni uporabljeno	CertPolicyId: v skladu s poglavjem 1.2. > UserNotice: kot določeno v poglavju 7.1.8>
naslovi registera preklicanih potrdil (CRL Distribution Points)	Ni uporabljeno	LDAP in http URL naslov SIMoD-CA-Root registra preklicanih potrdil	LDAP in http URL naslov SIMoD-CA-Restricted registra preklicanih potrdil
Alternativno ime imetnika (subject Alternative Name)	Ni uporabljeno	Ni uporabljeno	Ni uporabljeno
Osnovne omejitve (basicConstraint)	**Kritično** CA =: True pathLenConstraint = 1	**Kritično** CA =: True pathLenConstraint = 0	**Kritično** CA =: False

Imetniška digitalna potrdila[23], ki jih izdaja overitelj SIMoD-CA-Restricted, vsebujejo naslednja razširitvena polja:

Polje (Field)	Potrdilo za preverjanje digitalnega podpisa…[24]	Potrdilo za šifriranje…[25]	Potrdilo za preverjanje digitalnega podpisa in šifriranje[26]…
odtis javnega ključa overitelja (authority Key Identifier)	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Restricted s katerim je podpisano potrdilo	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Restricted s katerim je podpisano potrdilo	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Restricted s katerim je podpisano potrdilo
odtis imetnikovega javnega ključa (subject Key Identifier)	SHA-1 odtis imetnikovega javnega ključa	SHA-1 odtis imetnikovega javnega ključa	SHA-1 odtis imetnikovega javnega ključa
namen uporabe ključa (key Usage)	**Kritično** digitalSignature	**Kritično** keyEncipherment	**Kritično** DigitalSignature keyEncipherment
razširjen namen uporabe (extended Key Usage)	Ni uporabljeno	Ni uporabljeno	Ni uporabljeno
obdobje veljavnosti zasebnega ključa (privateKeyUsagePeriod)	V skladu s poglavjem 6.3.2	V skladu s poglavjem 6.3.2	V skladu s poglavjem 6.3.2
OID oznaka tipa potrdila (certificate Policies)	**Kritično** CertPolicyId: v skladu s poglavjem 1.2. > UserNotice: kot določeno v poglavju 7.1.8>	**Kritično** CertPolicyId: v skladu s poglavjem 1.2. > UserNotice: kot določeno v poglavju 7.1.8>	**Kritično** CertPolicyId: v skladu s poglavjem 1.2. > UserNotice: kot določeno v poglavju 7.1.8>
naslovi registera preklicanih potrdil (CRL Distribution Points)	LDAP in http URL naslov SIMoD-CA-Restricted registra preklicanih potrdil	LDAP in http URL naslov SIMoD-CA-Restricted registra preklicanih potrdil	LDAP in http URL naslov SIMoD-CA-Restricted registra preklicanih potrdil
Alternativno ime imetnika (subject Alternative Name)	<elektronski naslov imetnika>	<elektronski naslov imetnika>	<elektronski naslov imetnika>
Osnovne omejitve (basicConstraint)	**Kritično** CA =: False	**Kritično** CA =: False	**Kritično** CA =: False

[23] Vsebina polj imetniških digitalnih potrdil je podana glede na namen uporabe potrdila. Tip potrdila in stopnja tajnosti ne vplivata na vsebino polj v potrdilu.

[24] Polno ime digitalnega potrdila: Digitalno potrdilo za preverjanje digitalnega podpisa za storitve prepoznavanja in preverjanja istovetnosti, celovitosti in nezanikanja.

[25] Polno ime digitalnega potrdila: Digitalno potrdilo za šifriranje za storitve zagotavljanja tajnosti oziroma zaupnosti.

[26] Popolno ime digitalnega potrdila: Digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe.

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 SIMoD-CA-Restricted, 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

Overitelj SIMoD-CA-Restricted ne predvideva uporabe razširitvenega polja za specifične podatke (angl.: *Policy Qualifiers extension*) za objavo spletnega naslova, kjer bi bila objavljena politika oziroma druge informacije za uporabnike.

Overitelj SIMoD-CA-Restricted uporablja razširitveno polje za specifične podatke (angl.: *Policy Qualifiers extension*) *"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. Verizija registov 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>
Issuer	izdajatelj	<razločevalno ime SIMoD-CA-Restricted>
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-Restricted 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 SIMoD-CA-Restricted overitelj 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.

Preverjanje skladnosti delovanja overitelja s Politiko SIMoD-PKI se izvede pred pričetkom delovanja overitelja in vsaj enkrat letno.

Preverjanje skladnosti Javnih pravil SIMoD-CA-Restricted s Politko SIMoD-PKI se izvaja skladno z drugim odstavkom tega poglavja.

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 delovanja overitelja 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-Restricted, je potrebno dovoljenje stopnje TAJNO.

8.3. Relacija med inšpektorjem in overitelji infrastrukture javnih ključev na MO

Inšpektor mora biti neodvisen od infrastrukture javnih ključev na MO.

8.4. Področja inšpekcije

Inšpekcijski nadzor preverja skladnost delovanja overitelja SIMoD-CA-Restricted 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 overitelja SIMoD-CA-Restricted 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-Restricted pomanjkljivosti ne odpravi, je Svet za upravljanje z infrastrukturo javnih ključev na MO dolžan ukrepati v okviru naslednjih možnosti:

- opozori na pomanjkljivosti, vendar kljub temu dovoli obratovanje overitelja do naslednje predvidene inšpekcije, ali
- pred preklicem overiteljevega potrdila dodeli overitelju 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.

Overitelj 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

Overitelji pridobijo podatke od bodočih imetnikov v postopku preverjanja vloge za izdajo digitalnega potrdila, ki ga izvede prijavna služba. Pridobljeni podatki se uporabljajo izključno za potrebe izdaje in upravljanja digitalnih potrdil. Osebni podatki imetnikov se hranijo v prijavni službi v skladu s predpisi, ki urejajo varstvo osebnih podatkov v Republiki Sloveniji.

9.4.2. Obseg osebnih podatkov (Osebni podatki, ki se obravnavajo kot zaupni)

Kot osebni podatki se obravnavajo podatki določeni s predpisi, ki urejajo varstvo osebnih podatkov v Republiki Sloveniji.

9.4.3. Osebni podatki ki se ne obravnavajo kot zaupni

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

9.4.4. Odgovornost glede varovanja osebnih podatkov

Za varovanje osebnih podatkov je odgovorna prijavna služba.

9.4.5. Dovoljenje za uporabo osebnih podatkov

Prijavna služba mora od bodočih imetnikov pridobiti dovoljenje za uporabo osebnih podatkov v postopku preverjanja identitete prosilca in postopkih upravljanja digitalnih potrdil, ter dovoljenje za objavo podatkov iz 9.4.3 Osebni podatki ki se ne obravnavajo kot zaupni.

9.4.6. Posredovanje osebnih podatkov v sodnih in upravnih postopkih

Osebne podatke se v sodnih in upravnih postopkih posreduje v skladu s predpisi, ki urejajo varstvo osebnih podatkov v Republiki Sloveniji.

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 jamči, da upravlja z digitalnimi potrdili, upravlja z repozitorijem in izdaja registre preklicanih potrdil v skladu s Politiko SIMoD-PKI. Overitelje v okviru infrastrukture javnih ključev na MO predstavlja, odgovarja in jamči za izpolnjevanje njihovih obveznosti Svet za upravljanje z infrastrukturo javnih ključev na MO.

9.6.2. Odgovornost in jamstva prijavne službe

Prijavna služba je odgovorna za skladnost identifikacijskih postopkov s Politiko SIMoD-PKI in točnost podatkov v vlogah. Za pravilnost delovanja prijavne službe jamči overitelj, oziroma 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

Imetnik digitalnega potrdila jamči, da:

- je bil seznanjen s Politiko SIMoD PKI in Javnimi pravili SIMoD-CA-Restricted pred podpisom vloge za izdajo digitalnega potrdila;
- ravna v skladu s Politiko SIMoD-PKI, Javnimi pravili SIMoD-CA-Restricted in ostalimi pravnimi akti;
- spremlja obvestila SIMoD-PKI in overitelja SIMoD-CA-Restricted, ter ravna v skladu z njimi;
- je prijavni službi in operativnemu osebju overitelja, ki upravlja z digitalnimi potrdili, posredoval popolne in točne podatke;
- se strinja z javno objavo svojega digitalnega potrdila;
- varuje svoje zasebne ključe in pametne kartice ali drugačne nosilce zasebnih ključev in upošteva vse ukrepe, da se prepreči izguba, razkritje, sprememba ali nepooblaščena uporaba;
- uporablja ključe in digitalna potrdila samo za namene, ki so definirani v Politiki SIMoD PKI;
- digitalno podpisuje in/ali šifrira le podatke, katerih veljavnost je krajša od veljavnosti digitalnega potrdila ali da pred potekom veljavnosti digitalnega potrdila ponovno podpiše in/ali šifrira podatke, če to ni rešeno na drug način (z aplikacijo);
- uporablja digitalna potrdila samo v obdobju njihove veljavnosti;
- bo ob sumu zlorabe svojega zasebnega ključa takoj obvestiti prijavno službo ali operativno osebje overitelja, ki upravlja z digitalnimi potrdili po postopku, ki je opisan v poglavju 4.9.3.1 Postopki preklica digitalnih potrdil imetnikov. Tudi če imetnik sumi, da gre za zlorabo ali razkritje zasebnega ključa tretje osebe, mora o tem obvestiti overitelja.

9.6.4. Odgovornost in jamstva tretje osebe

Tretja oseba, ki se zanaša na digitalna potrdila overitelja infrastrukture javnih ključev na MO, jamči, da:

- bo zahtevala preklic digitalnega potrdila druge osebe, če izve, da je bil zasebni ključ ogrožen na način, ki vpliva na zanesljivost uporabe, če obstaja nevarnost zlorabe ali če so spremenjeni podatki, ki so navedeni v digitalnem potrdilu;
- bo pred uporabo digitalnega potrdila preverila, ali je digitalno potrdilo ustrezno za predvideno uporabo in da bo uporabila digitalno potrdilo le za namene, določene v Politiki SIMoD PKI;
- bo pred uporabo digitalnega potrdila preverila status digitalnega potrdila v ustreznem veljavnem registru preklicanih potrdil v skladu z zahtevami iz poglavja 4.9.6 Obveza preverjanja registra preklicanih potrdil.

Pravice in obveznosti tretjih oseb, ki so člani infrastrukture javnih ključev MO, so predpisane v Politiki SIMoD-PKI. Pravice in obveznosti tretjih oseb, ki pripadajo drugim infrastrukturam javnih ključev, so navedene v pogodbi o medsebojnem priznavanju med overiteljema.

9.6.5. Odgovornost in jamstva drugih udeležencev

Ni relevantno.

9.7. Zanikanje odgovornosti overitelja

Overitelj ni odgovoren za škodo (direktno ali posredno), izgube, stroške ter terjatve, ki izhajajo iz ali so nastale zaradi uporabe digitalnih potrdil overitelja 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, pravili delovanja overitelja ali morebitni drugi pogodbi;
- je nastala škoda zaradi napake v delovanju strojne ali programske opreme imetnika ali tretje osebe.

9.8. Omejitve odgovornosti overiteljev SIMoD-PKI

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

Javna pravila SIMoD-CA-Restricted overitelja digitalnih potrdil na Ministrstvu za obrambo Republike Slovenije začnejo veljati naslednji dan po podpisu.

9.10.2.Prenehanje veljavnosti

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

9.10.3.Posledice prenehanja veljavnosti

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

Posledice prenehanja veljavnosti politike v primeru prenehanja delovanja overitelja, 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 tega dokumenta.

9.12. Spreminjanje dokumenta

9.12.1.Postopke uveljavitve spremembe

Svet za upravljanje z infrastrukturo javnih ključev na MO odobri teh Javnih pravil SIMoD-CA-Restricted in jih predlaga ministru v sprejem.

9.12.2.Postopek obveščanja in rok za pripombe

Za vsa področja iz teh Javnih pravil SIMoD-CA-Restricted velja obveznost obveščanja o spremembah osem dni (8) dni pred uporabo sprememb Javnih pravil SIMoD-CA-Restricted 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-Restricted.

Svet za upravljanje z infrastrukturo javnih ključev na MO o spremembah Javnih pravil SIMoD-CA-Restricted 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 overitelja tolikšne, da zahtevajo objavo novih Javnih pravil SIMoD-CA- Restricted 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

Overitelji SIMoD-PKI 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 Javnih pravil SIMoD-CA-Restricted so vsi udeleženci infrastrukture javnih ključev na MO dolžni upoštevati tudi določila Politike SIMoD-PKI, Izjavo uporabnika podpisano ob oddaji vloge za pridobitev 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 Javnih pravil SIMoD-CA-Restricted nepravilen ali neveljaven, ostanejo ostali deli Javnih pravil SIMoD-CA-Restricted veljavni vse dokler se ne objavi sprememba. Postopek spremembe Javnih pravil SIMoD-CA-Restricted 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 te politike 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, predviden čas trajanja odstopanja in načrt odprave neskaldja.

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 trajno nemogoče, bo overitelj 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-Restricted, javni del, začnejo veljati naslednji dan po podpisu, uporabljati pa se začnejo trideseti (30) dan po podpisu.

Šifra: 382-5/2006-13
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).
RDN	Kratko razločevalno ime objekta v imeniku, praviloma sestavljeno in splošnega imena (angl. Common Name, CN) in serijske številke (angl., serialNumber)
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.
FQDN	Popolno ime naprave v domenskem sistemu (angl.: Fully Qualified Domain Name).
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.
RFC	Priporočila, ki jih izdaja IETF.
RFC 4210	Priporočilo, ki določa postopke za izmenjavo podatkov, ki se nanašajo na digitalna potrdila. Vsebuje PKIX-CMP.
RFC 3647	Priporočilo, ki določa elemente, ki naj bodo zajeti v politiki overitelja (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework). veljavno od novembra 2003 (je nadomestil RFC 2527).
RFC 3280	Priporočilo, ki določa elemente potrdil in regista preklicanih potrdil.
RSA	Eden prvih nesimetričnih kriptografskih sistemov, patentiran leta 1983, imenovan po odkriteljih: Rivest, Shamir in Adelman.
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)
SIMoD-CA-Root	Overitelj digitalnih potrdil na Ministrstvu za obrambo Republike Slovenije (angl.: Slovenian Ministry of Defense Certification Authority).
SIMoD-CA*n*-Restricted	Overitelj, ki deluje v oviru SIMoD-PKI, kot podrejeni overitelj SIMoD-CA-Root korenskega overitelja
SIMoD-CA*n*-Secret	Overitelj, ki deluje v oviru SIMoD-PKI, kot podrejeni overitelj SIMoD-CA-Root korenskega overitelja
SIMoD-TSAm-Restricted	Izdajatelj varnih časovnih žigov na Ministrstvu za obrambo Republike Slovenije (angl.: Slovenian Ministry of Defense Time Stamping Authority)
SIMoD-TSAm-Secret	Izdajatelj varnih časovnih žigov na Ministrstvu za obrambo Republike Slovenije (angl.: Slovenian Ministry of Defense Time Stamping Authority)
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

A.1 Izraz	A.2 Definicija
Časovni žig	Je elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša v navedenem času.
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 izdajatelja časovnih žigov	Je digitalno potrdilo, s katerim izdajatelj časovnih žigov izdaja časovne žige.
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”. Javni del notranjih pravil overitelja in Politika overitelja digitalnih potrdil sta v konkretnem primeru overitelja na MO isti dokument.
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.

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.
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.
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.
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.

Varen časovni žig	Je elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času (2. člen ZEPEP). Varen časovni žig mora v skladu s 34. členom Uredbe vsebovati nedvoumne in pravilne podatke o datumu, točnem času najmanj na sekundo natančno in overitelju, ki je varni časovni žig ustvaril. Varni časovni žig je lahko dokumentu dodan ali priložen in z njim povezan, vendar morajo biti pri tem vedno izpolnjene enake zahteve kot za varen elektronski podpis s kvalificiranim digitalnim potrdilom.
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.
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.
Selektivno omejevanje dostopa	Ločevanje dostopa glede na upravičen interes.
Tajnost	Zaupnost v smislu ZTP.
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.
Nevarovani KIS	KIS, ki ni akreditirianih za nobeno stopnjo tajnosti glede na tajnost podatkov, ki se v KIS obdeluejo.
Varovani KIS	KIS, akreditiran za ustrezno stopnjo tajnosti glede na tajnost podatkov, ki se v KIS obdeluejo.