REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije

(Politika SIMoD-PKI)

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) izdajam

PRAVILA DELOVANJA INFRASTRUKTURE JAVNIH KLJUČEV NA MINISTRSTVU ZA OBRAMBO REPUBLIKE SLOVENIJE

(POLITIKA SIMoD-PKI)

1. UVOD

1.1. Pregled

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

V okviru SIMoD-PKI deluje korenski overitelj SIMoD-CA-Root (angl. **S**loveni**i**an **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.

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

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

Politika SIMoD-PKI predpisuje izdajanje in upravljanje digitalnih potrdil za zagotavljanje 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. Politika SIMoD-PKI določa pet osnovnih politik za digitalna potrdila v okviru SIMoD-PKI infrastrukture, ki se med seboj ločijo glede na stopnjo zaupanja v digitalno potrdilo in namen uporabe oziroma storitev, kot je navedeno v 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.
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.

Poleg digitalnih potrdil izdanih v skladu z eno od petih politik za digitalna potrdila, določenih v tej politiki, lahko podrejeni overitelji izdajajo tudi druga digitalna potrdila, kar morajo jasno označiti v svojih pravilih delovanja in digitalnih potrdilih.

[1] Javni ključ iz digitalnega potrdila za šifriranje se uporablja za izmenjavo simetričnih šifrirnih ključev pri zagotavljanju zaupnosti podatkov v elektronski obliki.
[2] Brez omejitve uporabe v smislu varnostnih storitev in aplikacij.

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

Storitve overiteljev SIMoD-PKI, njihovo delovanje in infrastruktura, v povezavi z digitalnimi potrdili izdanimi po tej politiki, so v skladu z določili Politike SIMoD-PKI.

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

SIMoD-PKI deluje po priporočilih zveze NATO in v skladu s predpisi, ki urejajo področje elektronskega podpisa v Republiki Sloveniji. Identifikacijske oznake digitalnih potrdil, ki so izdana kot kvalificirana digitalna potrdila v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 – uradno prečiščeno besedilo), so navedene v poglavju 1.2.1 Identifikacijske oznake kvalificiranih digitalnih potrdil.

1.2. Naziv dokumenta in identifikacijske oznake

Identifikacijske oznake (angl. Object Identifiers - OIDs) SIMoD-PKI na MO se delijo po naslednjem pravilu: »1.3.6.1.4.1.22295[3].10.<overitelj>«.

Del identifikacijske oznake	Vrednost	
1.3.6.1.4.1.22295.10	enolična identifikacijska oznaka SIMoD-PKI na MO	
overitelj	1	infrastruktura SIMoD-PKI
	2	SIMoD-CA-Root
	…	rezervirano za overitelje SIMoD-PKI

Identifikacijske oznake Politik infrastrukture SIMoD-PKI (angl. Policy Object Identifiers; Policy OIDs) so določene po naslednjem pravilu: »1.3.6.1.4.1.22295[4].10.1.1.<klasifikacija KIS>.<stopnja zaupanja>.<PKI varnostna storitev>.<verzija>«.

Del identifikacijske oznake	Vrednost	
1.3.6.1.4.1.22295.10.1.1	oznake politik digitalnih potrdil	
klasifikacija KIS	1	brez stopnje tajnosti, javna omrežja + INTERNO
	2	TAJNO
stopnja zaupanja	1	VISOKA
	2	SREDNJA
PKI varnostna storitev	1	podpisovanje oziroma preverjanje digitalnega podpisa za storitve prepoznavanja in preverjanja istovetnosti, celovitosti in nezanikanja
	2	šifriranje oziroma zagotavljanje zaupnosti
	3	brez omejitve namena v smislu zagotavljanja varnostnih storitev
	4	izdajanje varnih časovnih žigov
	...	druge PKI storitve v MO (rezervirano za bodočo uporabo)
verzija	zaporedna številka izdaje politike	

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

V omrežju INTERNO so predvidene naslednje vrste digitalnih potrdil, ki jih označujejo navedene identifikacijske oznake politik (angl. Policy OIDs):

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

V omrežju TAJNO so predvidene naslednje vrste digitalnih potrdil, ki jih označujejo navedene identifikacijske oznake politik (angl. Policy OIDs):

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	1.3.6.1.4.1.22295.10.1.1.2.1.1.0
VISOKA	Digitalna potrdila za šifriranje za storitve zagotavljanja tajnosti, oziroma zaupnosti	1.3.6.1.4.1.22295.10.1.1.2.1.2.0
VISOKA	Digitalna potrdila za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe	1.3.6.1.4.1.22295.10.1.1.2.1.3.0
SREDNJA	Digitalna potrdila za preverjanje digitalnega podpisa in šifriranje brez omejitev uporabe	1.3.6.1.4.1.22295.10.1.1.2.2.3.0
VISOKA	Digitalna potrdila za izdajatelje časovnih žigov	1.3.6.1.4.1.22295.10.1.1.2.1.4.0

Overitelji SIMoD-PKI lahko izdajajo eno ali več vrst naštetih digitalnih potrdil, kar morajo jasno označiti v svojih pravilih delovanja in digitalnih potrdilih z navedbo identifikacijske oznake politike v razširitvenem polju *certificatePolicies*, kot je določeno v poglavju 7.1.2 Razširitvena polja. Overitelji lahko digitalnim potrdilom, ki jih izdajajo po eni od SIMoD-PKI politik, dodelijo svojo identifikacijsko oznako. V tem primeru mora biti v razširitvenem polju poleg overiteljeve identifikacijske oznake obvezno navedena tudi SIMoD-PKI identifikacijska oznaka.

Overitelji SIMoD-PKI lahko poleg digitalnih potrdil določenih v tej politiki izdajajo tudi druga digitalna potrdila, kar morajo jasno označiti v svojih pravilih delovanja in digitalnih potrdilih z navedbo identifikacijske oznake politike v razširitvenem polju *certificatePolicies*, kot je določeno v poglavju 7.1.2 Razširitvena polja. Digitalna potrdila, ki niso izdana v skladu z eno od identifikacijskih oznak oziroma politik digitalnih potrdil določenih v Politiki SIMoD-PKI, ne smejo vsebovati SIMoD-PKI identifikacijske oznake.

1.2.1. Identifikacijske oznake kvalificiranih digitalnih potrdil

Digitalna potrdila z identifikacijskimi oznakami določenimi v poglavju 1.2. Naziv dokumenta in identifikacijske oznake, navedena v spodnji tabeli, se izdajajo kot kvalificirana digitalna potrdila v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu:

Stopnja zaupanja	Namen uporabe oziroma storitev	Identifikacijske oznaka politike
VISOKA	Digitalna potrdila za preverjanje digitalnega podpis za storitve prepoznavanja in preverjanja istovetnosti, celovitosti in nezanikanja.	1.3.6.1.4.1.22295.10.1.1.1.1.1.0 1.3.6.1.4.1.22295.10.1.1.2.1.1.0

1.3. Udeleženci infrastrukture javnih ključev

1.3.1. Overitelji

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

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

1.3.1.1. Svet za upravljanje z infrastrukturo javnih ključev na MO

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

- 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 sestavlja 7 članov:

- vodja organizacijske enote MO pristojne za informatiko in telekomunikacije, ki je vodja Sveta;
- vodja organizacijske enote MO pristojne za obveščevalno varnostne zadeve;
- vodja organizacijske enote MO pristojne za pravne zadeve;
- prvi varnostni inženir iz skupine za upravljanje z digitalnimi potrdili overitelja SIMoD-CA-Root;
- prvi administrator overitelja iz skupine za upravljanje z informacijskim sistemom overitelja SIMoD-CA-Root;
- dva člana Sveta sta strokovna sodelavca iz organizacijske enote MO pristojne za informatiko in telekomunikacije, ki ju v Svet imenuje minister na predlog vodja organizacijske enote MO pristojne za informatiko in telekomunikacije.

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

1.3.1.2. Operativno osebje overiteljev SIMoD-PKI

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

1.3.2. Prijavna služba

Prijavna služba sprejema 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 povezane z obrambo;
c) notranje organizacijske enote in organi v sestavi MO[5] (v nadaljevanju organizacijske enote MO) ter poveljniki enot na ravni poveljniških dolžnosti v SV;
d) institucije[6], ki opravljajo naloge povezane z obrambo;
e) strežniki[7] in druga strojna ter programska oprema;
f) izdajatelji[8] časovnih žigov in podobni ponudniki storitev overjanja, ki delujejo v okviru SIMoD-PKI;

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

Izdajo digitalnih potrdil subjektom iz točk c) in d), ter digitalnih potrdil medsebojno priznanim drugim overiteljem, mora odobriti Svet za upravljanje z infrastrukturo javnih ključev na 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 overitelja.

Tretje osebe so:

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

[5] Odgovorna oseba za digitalno potrdilo je vodja organizacijske enote MO. Odgovorna oseba ima za digitalno potrdilo za notranje organizacijske enote enake obveznosti kot imetnik digitalnega potrdila za zaposlene v MO.
[6] 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.
[7] Odgovorna oseba za digitalno potrdilo je vodja notranje organizacijske enote MO oziroma predstojnik institucije, 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.
[8] 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.

1.3.5. Posredno odgovorni organi

Overitelji SIMoD-PKI delujejo kot del KIS MO in SV in obratujejo v skladu s predpisi MO za področje KIS MO in SV. Posredno odgovorni organi so tudi 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 izdajajo overitelji SIMoD-PKI, se morajo uporabljati v skladu s Politiko SIMoD-PKI in Pravili delovanja overiteljev SIMoD-PKI. Digitalna potrdila overiteljev SIMoD-PKI so namenjena izključno službeni uporabi v MO. V drugih institucijah pa je namen omejen na opravljanje nalog povezanih z obrambo države.

Infrastruktura javnih ključev na MO omogoča pet osnovnih varnostnih storitev:

- **zaupnost**, kot lastnost podatkov v elektronski obliki, da so nerazumljivi ali nerazpoložljivi neavtoriziranim osebam;
- **celovitost** (tudi pristnost), kot lastnost podatkov v elektronski obliki, da se niso spremenili na način, ki ga ne bi bilo moč ugotoviti;
- **nezanikanje**, kot lastnost oz. mehanizem, ki onemogoča zanikanje izvršenega dejanja (npr. elektronske transakcije) oz. lastništva e-podatkov;
- **preverjanje istovetnosti**, kot mehanizem za preverjanje identitete v elektronski obliki;
- **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. Ta storitev mora biti predpisana 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. Ti ukrepi so v okviru infrastrukture javnih ključev na MO enaki za vse vrste digitalnih potrdil ne glede na klasifikacijo omrežja, v katerem se nahajajo. Razlika v stopnji zaupanja izhaja samo iz načina varovanja zasebnih ključev imetnikov.

V okviru infrastrukture javnih ključev na MO se izdajajo 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.

Politika SIMoD-PKI predvideva spodaj navedeno razvrstitev podatkov:

<table>
<tr><th colspan="3">Vrste podatkov</th><th rowspan="2">Pomembnost</th><th rowspan="2">Stopnja tajnosti</th></tr>
<tr><th>Finančne transakcije</th><th colspan="2">Obrambne zadeve, konkretne bojne naloge</th></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
tajno
strogo tajno</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></tr>
<tr><td></td><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.

Politika SIMoD-PKI predvideva uporabo digitalnih potrdil 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 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[9] do stopnje tajnosti TAJNO (angl. Community 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, avtentikacijo, 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.

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

1.4.2. Nedovoljena uporaba digitalnih potrdil

Ni relevantno.

1.5. Upravljanje s Politiko SIMoD-PKI

1.5.1. Organ, ki upravlja s tem dokumentom

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 Politika SIMoD-PKI obveznost nadzirati izdelavo, voditi postopek potrditve, ocenjevati predlagane spremembe, predlagati uveljavitve sprememb in načrtovati postopek uveljavitve sprememb Politike SIMoD-PKI.

1.5.1.2. Operativno osebje overiteljev

Operativno osebje overiteljev SIMoD-PKI 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.

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

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

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

1.5.4. Postopek odobritve Pravil delovanja overitelja

Overitelj mora Svetu za upravljanje z infrastrukturo javnih ključev na MO predložiti javni in zaupni del svojih pravil delovanja. Svet za upravljanje z infrastrukturo javnih ključev na MO preveri:

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

Izdaja digitalnega potrdila podrejenemu overitelju 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 mora biti stalno dostopen. V primeru odpovedi dostopa mora operativno osebje pristopiti k odpravljanju napake v najkrajšem možnem času, ne glede na to, da rezervna kopija normalno deluje.

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 mora biti tak, da je zagotovljen dostop do imeniških storitev vsem uporabnikom ne glede na njihov položaj v segmentiranem omrežju. Zagotovljeno mora biti medsebojno usklajevanje imenikov z namenom, da imajo vsi uporabniki dostopen vsaj en ažuren imenik.

Razen v izjemnih primerih, ko je določeni omrežni segment zaradi trenutne napake ali nezmožnosti povezave izoliran, morajo biti digitalna potrdila in 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, ter pravila delovanja podrejenih overiteljev, so objavljena na spletni strani: http://www.simod-pki.mors.si. Vsebina spletnih strani je zaščitena pred nepooblaščenim spreminjanjem.

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

Overitelji v imenikih objavljajo naslednje podatke:

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

Imeniki so dostopni po protokolu LDAP.

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

Overitelji SIMoD-PKI morajo poleg javnih dokumentov objaviti tudi dokumente, kot so navodila uporabnikom, ter vloge za pridobitev in preklic digitalnih potrdil, ter v svojih pravilih delovanja navesti elektronski naslov na katerem so dokumenti dostopni.

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

2.3. Čas in pogostost objav

Overitelj objavi digitalno potrdilo takoj, ko ga izda. Overitelj uvrsti preklicano digitalno potrdilo v register preklicanih potrdil takoj po opravljenem preklicu. Objava registrov preklicanih potrdil

je v skladu s poglavji 4.9.5 Čas od vloge za preklic do preklica in 4.9.7 Pogostost objav registrov preklicanih potrdil.

2.4. Dostop do podatkov v repozitoriju

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

Politiko SIMoD-PKI 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

Vsakemu imetniku potrdila se v polju *Subject* v X.509v3 digitalnem potrdilu dodeli edinstveno razločevalno ime - 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 mora biti v obliki X.501 UTF8String in ne sme biti prazno.

3.1.2. Potreba po smiselnosti imen

Kratko razločevalno ime (angl. Relative Distinguished Name, RDN) mora enolično določati imetnika potrdila. Edinstvenost kratkega razločevalnega imena se po potrebi doseže z uporabo oznake (na primer številke) dodane splošnemu imenu, ali uporabo *dnQualifier* X.500 atributa 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 overiteljev SIMoD-PKI 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 SIMoD-PKI 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. Izdaja digitalnih potrdil z zakrito identiteto imetnika oziroma mehanizmi zagotavljanja anonimnosti niso predvideni.

3.1.4. Pravila za interpretacijo različnih oblik imen

Imena se interpretirajo v skladu z definicijami v poglavju 3.1.1 Vrste imen, 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 *dnQualifier* X.500 atributa v relativnem razločevalnem imenu. V primeru uporabe *dnQualifier* X.500 atributa 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. Overitelji SIMoD-PKI ne smejo zavestno izdati digitalnega potrdila z imenom, ki vsebuje zaščiteno znamko naročniku, ki ni nosilec zaščitene znamke. Prijavna služba niti operativno osebje overiteljev SIMoD-PKI niso dolžni preverjati pravic do uporabe zaščitenih znamk, niti razčiščevati sporov glede zaščitenih znamk. Bodočim imetnikom ni dovoljeno zahtevati imen, ki bi kršila intelektualne ali avtorske pravice drugih, čeprav se v okviru infrastrukture javnih ključev na MO tega ne preverja niti ne bo Svet za upravljanje z infrastrukturo javnih ključev na MO posredoval v takšnih sporih. Prijavna služba in operativno osebje overiteljev SIMoD-PKI si pridržuje pravico zavrniti izdajo digitalnega potrdila ali preklicati izdana digitalna potrdila udeležencev spora.

3.2. Prva registracija

3.2.1. Metode dokazovanja lastništva zasebnega ključa

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

3.2.2. Preverjanje istovetnosti 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 iz 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 notranje organizacijske enote 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

Vlogo za digitalna potrdila za strežnike, drugo strojno ali programsko opremo, oziroma izdajatelje časovnega žiga izpolnita in podpišeta skrbnik za napravo oziroma programsko opremo ter vodja ustrezne organizacijske enote MO ali institucije. Preveri se istovetnost fizične osebe, ki je skrbnik naprave ali programske opreme. Prijavna služba preveri pristnost podatkov skrbnika v kadrovski evidenci MO in izvede osebno identifikacijo na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list, ali vozniško dovoljenje); v primeru institucije pa se preveri pristnost 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 vzpostavlja 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 vzpostavlja 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[10] 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 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.

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

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 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 ustreznega overitelja SIMoD-PKI .

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

Operativno osebje overitelja SIMoD-PKI 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. Postopke 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.

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

4.2.2. Odobritev ali zavrnitev izdaje digitalnega potrdila

Vloga za izdajo digitalnega potrdila overiteljev v okviru infrastrukture javnih ključev na MO ne obvezuje 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 ustreznega overitelja SIMoD-PKI. Naročnik je o odobritvi digitalnega potrdila obveščen hkrati s prejemom dela aktivacijskih podatkov.

4.2.3. Čas za obdelavo vloge za izdajo digitalnega potrdila

Največji dopusten čas med oddajo vloge za izdajo digitalnega potrdila prijavni službi in izdajo aktivacijskih podatkov, ki jih bodoči imetnik potrebuje za generiranje ključev, ne sme biti daljši od 21 dni. Bodoči imetnik ima za prevzem digitalnega potrdila na voljo 30 dni od izdaje aktivacijskih podatkov.

4.3. Izdaja digitalnega potrdila

4.3.1. Postopki overiteljev SIMoD-PKI ob izdaji potrdil

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

4.3.1.1. Dostava zasebnega ključa imetniku

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

V primeru, ko overitelj generira zasebne ključe, kot je to v primeru dešifrirnih ključev digitalnih potrdil s podporo za povrnitev zgodovine ključev, poteka prenos zasebnega ključa z uporabo protokola PKIX-CMP in je integralni del postopka za prevzem digitalnega potrdila. Overitelji SIMoD-PKI morajo v svojih pravilih delovanja jasno navesti, za katera digitalna potrdila se ključi generirajo pri overitelju in za katera potrdila se hranijo imetniški dešifrirni za potrebe povrnitve zgodovine ključev.

4.3.1.2. Dostava overiteljevega javnega ključa imetniku

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

Javni ključ overitelja oziroma overiteljevo digitalno potrdilo, ki vsebuje overiteljev javni ključ, se pošlje bodočim imetnikom digitalnih potrdil, ki se izdajajo na osnovi PKCS#10 zahtevka, po protokolu PKCS#7 kot integralni del postopka za prevzem 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 objavi v imeniku iz poglavja 2.2. Objave informacij o digitalnih potrdilih.

4.4. Prevzem digitalnega potrdila

V okviru infrastrukture javnih ključev na MO je izdaja digitalnega potrdila 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 programske opreme na strani uporabnika in posameznega overitelja. Overitelji SIMoD-PKI morajo v svojih pravilih delovanja opisati postopke prevzema oziroma objaviti uporabniška navodila za prevzem potrdil.

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 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 je po izdaji objavljeno v imenikih iz poglavja 2.2. Objave informacij o digitalnih potrdilih. Overitelji lahko v imenikih objavijo tudi digitalna potrdila 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. Uporaba s strani imetnikov

4.5.1.1. Zasebni ključi in digitalna potrdila overiteljev

Overitelj SIMoD-CA-Root lahko uporablja svoj zasebni ključ samo za podpisovanje digitalnih potrdil podrejenim overiteljem, izdajateljem časovnih žigov, za podpisovanje digitalnih potrdil

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

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

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

4.5.1.2. Zasebni ključi in digitalna potrdila prijavne službe

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

4.5.1.3. 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 overitelja, ki je izdal digitalno potrdilo.

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 hranijo 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 overitelja, ki je izdal digitalno potrdilo.

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[11] digitalnih potrdil

4.7.1. Okoliščine obnove digitalnih potrdil

Po preklicu digitalnega potrdila 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.

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

Samodejna obnova digitalnih potrdil izdanih na osnovi PKCS#10 protokola 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 imetniki, oziroma isti subjekti, kot za prvo izdajo, skladno s poglavjem 4.1.1 Kdo lahko zaprosi za izdajo digitalnega potrdila.

4.7.3. Obdelava zahtevkov za 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 infrastrukture javnih ključev na MO v obdobju stotih (100) dni pred zadnjim dnem veljavnosti zasebnega ključa. Generiranje novih parov ključev je možno samo v primeru, da je digitalno potrdilo, ki ga trenutno poseduje imetnik, veljavno. Imetniki, ki nimajo veljavnega digitalnega potrdila, morajo pridobiti novo digitalno potrdilo[12] oziroma ponoviti postopke od 4.1. Prošnja za izdajo digitalnega potrdila do 4.4. Prevzem digitalnega potrdila. 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 protokola 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 mora biti pod kontrolo operativnega osebja SIMoD-PKI.

Za obnovljena digitalna potrdila velja Politika SIMoD-PKI, 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

Overitelji morajo v pravilih delovanja opredeliti okoliščine, v katerih je dovoljena sprememba digitalnega potrdila zaradi spremenjenih podatkov, ob upoštevanju zahtev iz poglavja 4.6. Obnova digitalnih potrdil brez spremembe javnega ključa.

[12] V primeru, da uporabnik želi dešifrirati podatke, zaščitene z neveljavnim potrdilom, mora na vlogi za izdajo novega potrdila obvezno izbrati še “Povrnitev zgodovine ključev za dešifriranje”, glej poglavje 4.12.1 Povrnitev zgodovine ključev za dešifriranje.

4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila

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

4.9.1. Okoliščine preklica

4.9.1.1. Okoliščine preklica imetniških digitalnih potrdil

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 po tej politiki.

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

4.9.1.2. Okoliščine preklica potrdila o priznavanju drugega overitelja

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

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

4.9.1.3. Okoliščine preklica potrdil podrejenih overiteljev

Vzroki za preklic digitalnih potrdil podrejenih overiteljev so:

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

4.9.2. Kdo lahko zahteva preklic

4.9.2.1. Kdo lahko zahteva preklic imetniškega digitalnega potrdila

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 overiteljev SIMoD-PKI, 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

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

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

4.9.2.3. Kdo lahko zahteva preklic potrdil podrejenih overiteljev

Preklic overiteljevega potrdila lahko zahteva:

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

4.9.3. Postopki za preklic

Ob preklicu digitalnega potrdila imetnika mora overitelj, ki je digitalno potrdilo izdal, objaviti preklicano digitalno potrdilo v registru preklicanih potrdil. V primeru preklica digitalnega potrdila o priznavanju drugega overitelja, mora biti preklicano digitalno potrdilo objavljeno v registru preklicanih potrdil in na spletni strani v okviru repozitorija overitelja.

Operativno osebje overitelja o preklicu digitalnega potrdila po elektronski pošti ali s priporočeno pošiljko obvesti imetnika potrdila ali odgovorno osebo, v primeru medsebojnega priznavanja pa odgovorno osebo drugega overitelja.

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

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

4.9.3.1. Postopki preklica digitalnih potrdil imetnikov

Načini posredovanja vloge za preklic:

- poslati z veljavnim digitalnim potrdilom elektronsko podpisano vlogo po elektronski pošti na kontaktni naslov overitelja SIMoD-PKI (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 overiteljev.

V primeru telefonsko posredovane vloge dežurna oseba posreduje vlogo za preklic operativnemu osebju overiteljev.

Preklic izvrši operativno osebje overiteljev .

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 opravi prvi varnostni inženir na zahtevo Sveta za upravljanje z infrastrukturo javnih ključev na MO.

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

4.9.3.3. Postopki preklica potrdil podrejenih overiteljev

Overitelj bo izvedel naslednje postopke:

- preklical vsa digitalna potrdila;
- zagotavljal razpoložljivost registrov preklicanih potrdil vsaj še devetdeset (90) dni od preklica svojega digitalnega potrdila;
- javno objavil preklic digitalnega potrdila;
- ustvaril nove ključe overitelja;
- izdal imetnikom nova digitalna potrdila.

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

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

4.9.4. Čas za posredovanje vloge za preklic

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

4.9.5. Čas od vloge za preklic do preklica

4.9.5.1. Čas za preklic imetniškega digitalnega potrdila

Operativno osebje izvede preklic v 8 urah po prejemu vloge za preklic v primeru:

- dejanske ali domnevne zlorabe zasebnih ključev;
- neizpolnjevanja obveznosti po tej politiki.

Operativno osebje 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

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

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

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

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

4.9.5.3. Čas za preklic potrdila podrejenega overitelja

Overitelj SIMoD-CA-Root prekliče digitalna potrdila podrejenih overiteljev takoj, ko prejme zahtevek, ali v roku, ki ga določi Svet za upravljanje z infrastrukturo javnih ključev na MO.

4.9.6. Obveza preverjanja registra preklicanih potrdil

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

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

Overitelji SIMoD-PKI so dolžni objaviti nov register preklicanih potrdil vsaj na 25 ur.

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

4.9.8. Dovoljene zakasnitve pri objavi registrov preklicanih potrdil

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

Overitelji SIMoD-PKI morajo izdati nov register preklicanih potrdil toliko časa pred iztekom veljavnosti starega registra, da je zagotovljen prenos registra do vseh komponent repozitorija še pred iztekom veljavnosti starega registra.

4.9.9. Storitev sprotnega preverjanje statusa digitalnih potrdil

Storitev 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 naslednje postopke:

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

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

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

4.9.13. Okoliščine za začasno ukinitev veljavnosti

Ni podprto.

4.9.14. Kdo lahko zahteva začasno ukinitev veljavnosti

Ni podprto.

4.9.15. Postopki za začasno ukinitev veljavnosti

Ni podprto.

4.9.16. Omejitve obdobja začasne ukinitve veljavnosti

Ni 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 mora biti vključen v vsa digitalna potrdila, ki jih izdajo overitelji SIMoD-PKI.

4.10.2. Razpoložljivost storitve

Overitelji SIMoD-PKI morajo zagotoviti razpoložljivost storitve v skladu z zahtevami za dostopnost repozitorija v poglavju 2.1. Repozitoriji.

4.10.3. Dodatne možnosti

Niso na voljo.

4.11. Predčasna prekinitev 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[13];
- 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[14];
- prenehanje potrebe po varnostni storitvi strežnika ali druge strojne ali programske opreme[15];
- prenehanje potrebe po storitvi izdajanja časovnih žigov ali podobni storitvi overjanja[16].

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

Dovoljeno je samo varnostno kopiranje (angl. Key Backup) in odkrivanje zasebnih ključev (angl. Key Recovery) v okviru infrastrukture javnih ključev na MO in sicer samo v primerih in ob pogojih navedenih v poglavjih 4.12.1 Povrnitev zgodovine ključev za dešifriranje 4.12.2 Odkrivanje kopije ključev za dešifriranje in 4.12.3 Zaščita odkritega zasebnega ključa in postopek prenosa ter 6.2.4 Varnostno kopiranje zasebnih ključev in 6.2.5 Arhiviranje zasebnega ključa.

4.12.1. Povrnitev zgodovine ključev za dešifriranje

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

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

- pozabi geslo za dostop do zasebnih ključev;
- izgubi ali poškoduje pametno kartico ali drugačen nosilec zasebnih ključev;

[13] v primeru potrdil za notranje organizacijske enote MO ter poveljniške dolžnosti v SV
[14] v primeru potrdil za institucije, ki opravljajo naloge, ki so povezane z obrambo
[15] v primeru potrdil za strežnike in drugo strojno ter programsko opremo
[16] v primeru potrdil za izdajatelje časovnih žigov in podobnih ponudnikov storitev overjanja

- 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 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.

4.12.2. Odkrivanje kopije ključev za dešifriranje

Overitelji SIMoD-PKI morajo v svojih pravilih delovanja navesti, za katera digitalna potrdila je omogočena storitev odkrivanja zgodovine ključev za dešifriranje.

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

Overitelj 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 o preklicu obvesti imetnika v skladu s poglavjem 4.9.3 Postopki za preklic.

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

4.12.3. Zaščita odkritega zasebnega ključa in postopek prenosa

Postopek prenosa odkritega zasebnega ključa je enak kot postopek prenosa dešifrirnega zasebnega ključa ob 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 overiteljev v infrastrukturi javnih ključev na MO 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 overiteljev SIMoD-PKI mora biti nameščena v prostorih varnostnega območja I. ali II. stopnje.

5.1.2. Fizični dostop

Nadzor fizičnega dostopa izvaja pristojna služba MO.

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

Preden operativno osebje overitelja zapusti prostore overitelja, mora preveriti:

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

5.1.3. Napajanje in klimatske naprave

Prostor s komunikacijsko in informacijsko opremo overiteljev je opremljen s:

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

5.1.4. Zaščita pred poplavo

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

5.1.5. Zaščita pred ognjem

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

5.1.6. Shranjevanje medijev

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

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

5.1.7. Odstranjevanje odpadkov

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

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

5.1.8. Hranjenje na oddaljeni lokaciji

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

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

5.2. Organizacijski varnostni ukrepi

5.2.1. Organizacija overitelja

5.2.1.1. Operativno osebje overiteljev SIMoD-PKI

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

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

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

V organizacijski skupini za upravljanje z digitalnimi potrdili so:

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

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

- prvi administrator overitelja;
- administratorji overitelja.

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 posameznega overitelja SIMoD-PKI.

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 osebja, ki upravlja z digitalnimi potrdili, o spremembah podatkov imetnikov digitalnih potrdil (npr. prekinitev delovnega razmerja, premestitev v drugo organizacijsko enoto).

5.2.1.3. Druge funkcije

Pristojne organizacijske enote v MO skrbijo za:

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

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

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

5.2.2. Število oseb, potrebnih za izvedbo postopkov

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

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

Izvršitev katerekoli zgoraj navedene naloge mora odobriti prvi varnostni inženir.

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

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

5.2.3. Preverjanje istovetnosti operativnega osebja

Operativno osebje overiteljev izkaže svojo istovetnost:

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

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

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

5.3. Zahteve za osebje overiteljev SIMoD-PKI

5.3.1. Kvalifikacije, izkušnje in varnostno preverjanje

Operativno osebje overiteljev:

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

5.3.3.1. Usposabljanje osebja overiteljev SIMoD-PKI

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

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

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

5.3.7. Zunanji izvajalci

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

5.3.8. Dokumentacija za osebje overiteljev SIMoD-PKI

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

5.4. Postopki varnostnih pregledov sistema

Overitelji imajo 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 ali poskusa vdora nepooblaščenih oseb do overiteljeve opreme in podatkov.

5.4.1. Vrste beleženih dogodkov

Overitelji so dolžni beležiti naslednje vrste dogodkov:

- dogodki na operacijskem sistemu, programski in strojni opremi overitelja;
- dogodki na operacijskih sistemih, programski in strojni opremi elementov komunikacijskega sistema;
- dogodki v zvezi s ključi overitelja;
- 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;
- 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.

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

- dogodke v zvezi s fizičnim dostopom do sistemov overitelja ter fizično lokacijo;
- kadrovske spremembe operativnega osebja overiteljev SIMoD-PKI;

- dogodke, povezane z uničevanjem občutljivega materiala (na primer kriptografskega materiala oziroma ključev in nosilcev ključev, aktivacijskih podatkov, osebnih podatkov o imetnikih).

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

5.4.2. Pogostost pregleda dnevnikov beleženih dogodkov

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

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

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

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

5.4.3. Obdobje hranjenja dnevnikov beleženih dogodkov

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

5.4.4. Zaščita dnevnikov beleženih dogodkov

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

Dostop do dnevnikov beleženih dogodkov je dovoljen samo pooblaščenim osebam:

- Svetu za upravljanje z infrastrukturo javnih ključev na MO,
- operativnemu osebju overitelja SIMoD-PKI v okviru svojih delovnih nalog,
- 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-PKI z namenom odkrivanja in odprave ranljivosti. Ugotovljeno ranljivost se oceni s stališča verjetnosti povzročitve škode in predvidi ukrepe za zmanjšanje grožnje.

5.5. Arhiviranje podatkov

5.5.1. Vrste arhiviranih podatkov

Overitelji morajo hraniti naslednje podatke:

- dnevnike beleženih dogodkov iz poglavja 5.4.1 Vrste beleženih dogodkov;
- vloge imetnikov digitalnih potrdil;
- dokumentacijo o izvedbi identifikacije uporabnikov;
- korespondenco in pogodbe imetnikov digitalnih potrdil z overitelji SIMoD-PKI;
- digitalna potrdila in liste preklicanih potrdil;
- verzije Politik SIMoD-PKI in svojih pravil delovanja;
- zasebne dešifrirne ključe v skladu s poglavjem 6.2.4 Varnostno kopiranje zasebnih ključev.

5.5.2. Obdobje hranjenja arhiva

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

Overitelji SIMoD-PKI hranijo vloge imetnikov, korespondenco in pogodbe imetnikov z overiteljem 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 overitelji SIMoD-PKI, verzije Politik SIMoD-PKI, verzije pravil delovanja overiteljev in dnevniki beleženih dogodkov v pisni obliki), se hranijo in arhivirajo v skladu s postopki dela z dokumentarnim gradivom v MO.

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

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 overitelji SIMoD-PKI, verzije Politik SIMoD-PKI, verzije pravil delovanja overiteljev in dnevniki beleženih dogodkov v pisni obliki), se zagotavlja razpoložljivost arhiva v skladu s postopki dela z dokumentarnim gradivom v MO.

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

5.5.5. Časovno žigosanje zapisov

Ni predpisano.

5.5.6. Način arhiviranja

Ni predpisano.

5.5.7. Postopek vpogleda v in verifikacije arhiva

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

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

Postopek priprave arhivskih podatkov je del zaupnega dela pravil delovanja overitelja.

5.6. Obnova digitalnih potrdil overiteljev

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

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

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

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

Če ob zamenjavi overiteljevega para ključev ne bo objavljeno drugače, ostane v veljavi ta Politika SIMoD-PKI.

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

5.6.2. Obnova potrdil podrejenih overiteljev v SIMoD-PKI

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

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

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

Če ob zamenjavi overiteljevega para ključev ne bo objavljeno drugače, ostane v veljavi ta Politika SIMoD-PKI.

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

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

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

5.7.1. Postopki v primeru okvar in zlorab

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

5.7.2. Uničenje programske, strojne opreme ali podatkov overitelja

V primeru okvare strojne ali programske opreme oziroma podatkov, pri kateri zasebni ključ overitelja ni bil uničen, bodo storitve overitelja ponovno vzpostavljene v najkrajšem možnem času. Overitelj mora najkrajšem možnem času vzpostaviti vsaj funkcionalnost preklicevanja digitalnih potrdil in objavljanja registra preklicanih potrdil. Skrajni rok za vzpostavitev storitve preklicevanja digitalnih potrdil in objavljanja registra preklicanih potrdil je sedem (7) dni. Po tem roku mora overitelj objaviti preklic svojega potrdila in ukrepati v skladu s poglavjem 4.9.3.3 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 so predpisani v poglavju 4.9.3.3 Postopki preklica potrdil podrejenih overiteljev.

5.7.3.2. Postopki ob zlorabi zasebnega ključa korenskega overitelja

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

5.7.4. Naravne in druge nesreče

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

5.8. Prenehanje delovanja overitelja

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

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

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

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

Overitelj bo izvedel naslednje postopke:

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

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev para ključev

6.1.1. Generiranje para ključev

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

Imetniški par ključev za podpisovanje se vedno generira pri bodočem imetniku in pod njegovo izključno kontrolo. Ko se za hranjenje ključev uporablja varnostni kriptografski modul, kot je to v primeru overitelja in izdajateljev časovnega žiga, oziroma pametne kartice pri imetnikih, je generiranje para ključev izvedeno znotraj teh modulov.

Imetniški par ključev, za katerega overitelji zagotavljajo storitev povrnitve zgodovine ključev, se generira pri overitelju in varno prenese bodočemu imetniku.

6.1.2. Dostava zasebnega ključa imetniku

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

Par ključev za podpisovanje se vedno ustvari na strani bodočega imetnika. 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 protokolih PKIX-CMP ali PKCS#10.

6.1.4. Dostava overiteljevega javnega ključa tretjim osebam

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

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

6.1.5. Dolžina ključev

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

Dolžina RSA zasebnega ključa podrejenih overiteljev v SIMoD-PKI 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 in 2048 bitov dolg RSA zasebni ključ za dešifriranje, ki pa se ne uporablja.

6.1.6. Parametri za generiranje javnih ključev in preverjanje parametrov

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

6.1.7. Namen uporabe ključev

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

Za podpisovanje digitalnih potrdil in registrov preklicanih potrdil se uporabljajo samo zasebni ključi 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. Razširjena uporaba ključa 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
	Overiteljevo potrdilo	X	X		
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	

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

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

6.2. Zaščita zasebnih ključev in tehnične kontrole kriptografskih modulov

6.2.1. Standardi za kriptografski modul

6.2.1.1. Overiteljevi kriptografski moduli

Generiranje overiteljevih parov ključev ter digitalno podpisovanje z overiteljevim zasebnim ključem se izvaja 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. Kriptografski moduli izdajateljev časovnega žiga

Generiranje zasebnega ključa za časovno žigosanje se izvaja 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.

6.2.1.3. 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 v primeru digitalnih potrdil visoke stopnje zaupanja 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.

6.2.1.4. Programsko hranjenje zasebnih ključev

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

6.2.2. Nadzor zasebnega ključa overitelja z več pooblaščenimi osebami

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

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

6.2.4. Varnostno kopiranje zasebnih ključev

Varnostna kopija zasebnega ključa overitelja se zagotavlja z varnostnimi mehanizmi varnostnega kriptografskega modula. Varnostna kopija je zaščitena s šifriranjem pred izvozom iz varnostnega kriptografskega modula. Dešifrirni ključ je porazdeljen na N[17] od M[18] administratorskih pametnih karticah varnostnega kriptografskega modula.

Kopije zasebnih ključev za dešifriranje digitalnih potrdil, za katera overitelj zagotavlja storitev povrnitve zgodovine ključev, se morajo hraniti 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 posamezni overitelj SIMoD-PKI zagotavlja storitev povrnitve zgodovine ključev.

6.2.6. Zapis zasebnega ključa v kriptografski modul in iz njega

Overiteljev zasebni ključ je generiran v varnostnem kriptografskem modulu.

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

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

Zasebni ključi za dešifriranje se v primeru digitalnih potrdil, za katera overitelj zagotavlja storitev povrnitve zgodovine 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-PKI overiteljev so shranjeni v varnostnem kriptografskem modulu v šifrirani obliki in se nikdar ne pojavijo 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 izdajatelja časovnega žiga se aktivira 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.

[17] N mora biti večji ali enak 2
[18] M mora biti večji ali enak 3

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.

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

Zasebne ključe overiteljev digitalnih potrdil in overiteljev 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

Overitelji arhivira svoj javni ključ za verifikacijo podpisa in imetniške javne ključe v povezavi z digitalnimi 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
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.	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

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 overiteljev. 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 overiteljih SIMoD-PKI, se morajo hraniti na način, ki zagotavlja njihovo zaupnost. Aktivacijski podatki se morajo pod nadzorom osebja za upravljanje z digitalnimi potrdili tiskati na kuverte, ki onemogočajo vpogled v vsebino (slepe kuverte). Aktivacijski podatki se dostavijo imetniku v skladu s poglavjem 4.1.2 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

Ni predpisano.

6.6. Tehnični nadzor življenjskega cikla overitelja

6.6.1. Nadzor razvoja sistema

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

6.6.2. Upravljanje varnosti

SIMoD-PKI evidentira postopke inštalacije, sprememb konfiguracije in nadgradnje za vse komponente infrastrukture javnih ključev na MO.

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

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

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

Programska 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 overiteljev, oziroma upravljanje varnosti skozi celoten življenjski cikel, morajo biti v skladu z 6.6.2 Upravljanje varnosti.

6.7. Varnostne kontrole na ravni računalniškega omrežja

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

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

6.8. Časovno žigosanje

Ni predpisano.

7. PROFIL DIGITALNIH POTRDIL IN REGISTROV PREKLICANIH POTRDIL

7.1. Profil digitalnih potrdil

7.1.1. Verzija digitalnih potrdil

Overitelji v okviru infrastrukture javnih ključev na MO izdajajo digitalna potrdila X.509 v3 v skladu s priporočili PKIX Certificate and 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 overitelja>
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.509 v3 digitalnih potrdilih.

Standardna razširitvena polja so definirana v skladu s priporočilom RFC 3280, ki dovoljuje tudi definiranje in dodajanje lastnih razširitvenih polj za potrebe overiteljev potrdil.

Tabela prikazuje standardna razširitvena polja, ki so uporabljena po Politiki SIMoD-PKI.

Standardno razširitveno polje - angleški naziv	Standardno razširitveno polje - slovenski opis	Vrednost
authorityKeyIdentifier	odtis javnega ključa overitelja	<SHA-1 odtis javnega ključa overitelja>
subjectKeyIdentifier	odtis imetnikovega javnega ključa	<SHA-1 odtis javnega ključa imetnika>
keyUsage	namen uporabe	Kot določeno v 6.1.7 Namen uporabe ključev oziroma v pravilih delovanja overitelja
extendedKeyUsage	razširjen namen uporabe	Kot določeno v 6.1.7 Namen uporabe ključev oziroma v pravilih delovanja overitelja
privateKeyUsagePeriod	veljavnost zasebnega ključa	Not Before: <začetek veljavnosti po GMT> Not After: <konec veljavnosti po GMT>
certificatePolicies:	oznaka politike potrdila	Določeno v pravilih delovanja overitelja; za imetniška potrdila je *UserNotice* predpisan v 7.1.8 Specifični podatki o politiki
CertPolicyID	enolična oznaka politike	

UserNotice	obvestilo uporabnikom	
CRLDistributionPoints	naslovi, na katerih je objavljen register preklicanih potrdil	Določeno v pravilih delovanja overitelja
subjectAlternativeName	elektronski poštni naslov	se ne uporablja
issuerAlternativeName	alternativno ime izdajatelja	se ne uporablja
subjectDirectoryAttributes	atributi imenika	se ne uporablja
basicConstraints	osnovne omejitve	Določeno v pravilih delovanja overitelja

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

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

7.1.3. Identifikacijske oznake algoritmov

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

Algoritem	Identifikacijska oznaka
rsaEncryption	1.2.840.113549.1.1.1
sha1WithRSAEncryption	1.2.840.113549.1.1.5

7.1.4. Oblike imen

Kot v poglavju 3.1.1 Vrste imen.

7.1.5. Omejitve imen

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

Upravitelj imenika lahko določi dodatne omejitve glede imen.

7.1.6. Identifikacijska oznaka politik

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

7.1.7. Način uporabe razširitvenega polja za omejitev uporabe politik

Z namenom, da se prepreči nenadzorovano prenašanje zaupanja v verigi medsebojno priznanih overiteljev, je polje "*Policy Constrains*" označeno kot kritično.

7.1.8. Specifični podatki o politiki

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

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

7.1.9. Procesiranje oznake kritičnosti razširitvenih polj

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

7.2. Profil registrov preklicanih potrdil

7.2.1. Verzija registrov preklicanih potrdil

Registri preklicanih potrdil morajo biti v skladu s priporočili RFC 3280: Certificate and 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 overitelja>
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 PKIX Part 1: Certificate and CRL Profile X.509 Version 2 CRL and ARL, 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 overiteljev v okviru infrastrukture javnih ključev na MO z Zakonom o elektronskem poslovanju in elektronskem podpisu in Politiko SIMoD-PKI.

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

8.1. Pogostost inšpekcije

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

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

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

8.2. Pogoji za inšpektorja

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

8.3. Relacija med inšpektorjem in overitelji SIMoD-PKI

Inšpektor mora biti neodvisen od infrastrukture javnih ključev na MO.

8.4. Področja inšpekcije

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

8.5. Postopki po opravljeni inšpekciji

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

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

- opozori na pomanjkljivosti, vendar kljub temu dovoli obratovanje overitelja do naslednje predvidene inšpekcije ali

- pred preklicem overiteljevega potrdila dodeli overitelju 30 dni za odpravo pomanjkljivosti, v tem času dovoli overitelju delovanje ali
- 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.

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

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

9. OSTALE POSLOVNE IN PRAVNE ZADEVE

9.1. Cenik

9.1.1. 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

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, 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 overiteljev, 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 poglavja 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 pred podpisom vloge za izdajo digitalnega potrdila;
- ravna v skladu s Politiko SIMoD-PKI in ostalimi pravnimi akti;
- spremlja obvestila SIMoD-PKI in ravna v skladu z njimi;
- je prijavni službi in operativnemu osebju overitelja, ki upravlja z digitalnimi potrdili, posredoval popolne in točne podatke;
- 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 obvestil 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 tretjih oseb

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 v okviru infrastrukture javnih ključev na MO ni odgovoren za škodo (direktno ali posredno), izgube, stroške ter terjatve, ki izhajajo iz ali so nastale zaradi uporabe digitalnih potrdil overiteljev in z njim povezanih ključev, če:

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

9.8. Omejitve odgovornosti 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

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

9.10.2. Prenehanje veljavnosti

Veljavnost Politike SIMoD-PKI ni časovna omejena in velja do uveljavitve nove verzije, oziroma do prenehanja delovanja overitelja.

9.10.3. Posledice prenehanja veljavnosti

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

Posledice prenehanja veljavnosti Politike SIMoD-PKI 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 te politike.

9.12. Spreminjanje dokumenta

9.12.1. Postopek uveljavitve spremembe

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

9.12.2. Postopek in roki obveščanja

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

Svet za upravljanje z infrastrukturo javnih ključev na MO o spremembah Politike SIMoD-PKI s SIMoD-PKI medsebojno priznane overitelje pisno 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 Politike SIMoD-PKI takšne, da zahtevajo objavo nove Politike SIMoD-PKI 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 Politike SIMoD-PKI so vsi udeleženci infrastrukture javnih ključev na MO dolžni upoštevati tudi določila pravil overitelja, ki je izdal digitalno potrdilo, izjavo uporabnika podpisano ob oddaji vloge za pridobitev digitalnega potrdila, veljavne predpise na območju Republike Slovenije ter določila morebitnih drugih dokumentov, ki jih določi overitelj v svojih pravilih delovanja.

9.16.2. Prenos pravic in obveznosti

Ni predpisano.

9.16.3. Spremembe okoliščin delovanja

Če postane zaradi spremenjenih okoliščin delovanja ali spremembe zakonodaje del Politike SIMoD-PKI nepravilen ali neveljaven, ostanejo ostali deli Politike SIMoD-PKI veljavni vse dokler se ne objavi sprememba. Postopek spremembe Politike SIMoD-PKI 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 politike SIMoD-PKI v izjemnih primerih odloča Svet za upravljanje infrastrukture javnih ključev na MO za vsak primer posebej na podlagi pisnega zahtevka, ki mora vsebovati obrazložitev, previden čas trajanja odstopanja in načrt odprave neskladja.

9.16.5. Višje sile

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

Noben udeleženec ne more uveljavljati zahtevkov, ki mu po Politiki SIMoD-PKI ali po ostalih obvezujočih dokumentih pripadajo, če je do ravnanja v nasprotju s Politiko SIMoD-PKI 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 SIMoD-PKI 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. PREHODNE IN KONČNE DOLOČBE

Svet za upravljanje z infrastrukturo javnih ključev na MO v dosedanji sestavi dela do oblikovanja Sveta za upravljanje z infrastrukturo javnih ključev na MO po teh pravilih.

Z uveljavitvijo teh pravil prenehajo veljati Pravila overitelja digitalnih potrdil na Ministrstvu za obrambo Republike Slovenije – javni del notranjih pravil (MO šifra 471-01-6/2002-47, datum 29. 07. 2005), in Pravila overitelja na Ministrstvu za obrambo Republike Slovenije za izdajo varnih časovnih žigov – javni del notranjih pravil (MO šifra 471-01-6/2002-48, datum 29. 7. 2005).

Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije začnejo veljati naslednji dan po podpisu, uporabljati pa se začnejo trideseti (30) dan po podpisu.

Šifra: 382-5/2006-11
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 kriptografskih algoritmov (angl. Public Key Cryptographic Standards).
PKCS#1	Osnovna pravila za formatiranje podatkov ob implementaciji RSA funkcij. Predpisuje, kako se izračuna digitalni podpis, kako se formatirajo podatki, ki se podpisujejo in format podpisa. Predpisuje tudi sintakso javnega in zasebnega RSA ključa.
PKCS#10	Sintaksa zahtevka za digitalno potrdilo. Zahtevek za digitalno potrdilo vsebuje razločevalno ime, javni ključ in nabor drugih atributov, ki jih podpiše subjekt, ki zahteva potrditev. Daljše ime: PKCS#10 Certification Request Syntax Standard.
PKCS#7	Sintaksa za kriptografsko obdelane podatke, kot digitalni podpisi in digitalne ovojnice.
PKI	Infrastruktura javnih ključev; strojna in programska oprema ter varnostni mehanizmi za zaupanja vredno implementacijo varnostnih storitev, ki temeljijo na nesimetrični kriptografiji (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 registra preklicanih potrdil.
RSA	Eden prvih nesimetričnih kriptografskih sistemov, patentiran leta 1983, imenovan po odkriteljih: Rivest, Shamir in Adelman.
SIMoD-PKI	Infrastruktura javnih ključev Ministrstva za obrambo Republike Slovenije (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 Defence Certification 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

Izraz	Definicija
Časovni žig	Je elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša v navedenem času.
Digitalni podpis	Je dodan podatek ali kriptografsko preoblikovanje, ki omogoča, da prejemnik podatkov preveri njihov izvor in integriteto, ter s tem prepreči poneverbo.
Digitalno potrdilo	Je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto.
Digitalno potrdilo 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 ključ	Polovica para ključev, ki je lahko javno objavljen.
Javni komunikacijsko informacijski sistem	Je komunikacijsko informacijski sistem, katerega storitve so namenjene javni uporabi.
Komunikacijski sistem	Je skupek naprav in postopkov, ki omogočajo prenos informacij. Primeri takih sistemov so telekomunikacijski sistemi in računalniška omrežja.
Komunikacijsko informacijski sistem	Je skupen izraz za komunikacijski in informacijski sistem.
Kvalificirano digitalno potrdilo	Je digitalno potrdilo, ki izpolnjuje zahteve iz 28. člena ZEPEP. Izda ga overitelj, ki deluje v skladu z zahtevami iz 28. do 36. člena ZEPEP.
LDAP	Protokol za dostop do podatkov v imeniku (angl. Lightweight Data Access Protocol).
Naročnik potrdila	Je fizična ali pravna oseba, ki z vlogo zaprosi za izdajo digitalnega potrdila.
Naslovnik elektronskega sporočila	Je oseba, ki ji je pošiljatelj namenil elektronsko sporočilo.
Nevarovani KIS	KIS, ki ni akreditiran za nobeno stopnjo tajnosti glede na tajnost podatkov, ki se v KIS obdelujejo.
Ogrožanje	Je dejanska ali domnevna možnost razkritja tajnih podatkov, izgube celovitosti ali razpoložljivosti podatkov.

Oprema za elektronsko podpisovanje	Je strojna ali programska oprema ali njune specifične sestavine, ki jo overitelj uporablja za storitve v zvezi z elektronskim podpisovanjem ali ki se uporabljajo za oblikovanje ali preverjanje elektronskih podpisov.
Overitelj digitalnih potrdil	Je fizična ali pravna oseba, ki izdaja digitalna potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi.
Par ključev	Je par asimetričnih kriptografskih ključev, ki ga sestavljata zasebni ključ in javni ključ.
Podatki v elektronski obliki	So podatki, ki so oblikovani, shranjeni, poslani, prejeti ali izmenljivi na elektronski način.
Podatki za elektronsko podpisovanje	So edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa.
Podatki za preverjanje elektronskega podpisa	So edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa.
Podpisnik	Je oseba, ki ustvari ali je v njenem imenu in v skladu z njeno voljo ustvarjen elektronski podpis.
Politika digitalnih potrdil	Je nabor pravil, ki posledično definira uporabnost digitalnih potrdil v določeni skupini uporabnikov in/ali za določen nabor aplikacij s skupnimi varnostnimi zahtevami (RFC 3647).
Pošiljatelj elektronskega sporočila	Je oseba, ki je sama poslala elektronsko sporočilo ali pa je bilo sporočilo poslano v njenem imenu in v skladu z njeno voljo; posrednik elektronskega sporočila se ne šteje za pošiljatelja tega elektronskega sporočila.
Prejemnik elektronskega sporočila	Je oseba, ki je prejela elektronsko sporočilo; posrednik elektronskega sporočila se ne šteje za prejemnika tega elektronskega sporočila.
Prijavna služba	Je služba oziroma organizacija, ki po pooblastilu overitelja sprejema vloge in preverja istovetnosti bodočih imetnikov.
Repozitorij	Je skladišče oziroma odlagališče objektov, vključno z digitalnimi potrdili. Repozitorij sestavljata imenik in spletne strani.
Selektivno omejevanje dostopa	Ločevanje dostopa glede na upravičen interes.
Sredstvo za preverjanje elektronskega podpisa	Je nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa.
Sredstvo za elektronsko podpisovanje	Je nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa.
Sredstvo za varno elektronsko podpisovanje	Je sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve iz 37. člena ZEPEP.
Šifrirni (kriptografski) ključ	Je niz znakov uporabljen za kriptografsko preoblikovanje (npr. šifriranje, dešifriranje, podpisovanje, ali preverjanje podpisa).
Tajni podatek	Dejstvo ali sredstvo iz delovnega področja organa, ki se nanaša na javno varnost, obrambne zadeve,ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov določenih v ZTP zaščititi pred nepoklicanimi osebami, in ki je v skladu s ZTP določeno in označeno kot tajno.
Tajnost	Zaupnost v smislu ZTP.

Tretja oseba	Je subjekt, ki ni aktivno udeležen v storitev, vendar zaupa izvajalcu in rezultatu storitve.
Uporabnik	Je naročnik ali imetnik digitalnega potrdila.
Varen 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.
Varen elektronski podpis	Je elektronski podpis, ki izpolnjuje naslednje zahteve: • povezan je izključno s podpisnikom; • iz njega je mogoče zanesljivo ugotoviti podpisnika; • ustvarjen je s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom; • povezan je s podatki, na katere se nanaša, tako, da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi.
Varovani KIS	KIS, akreditiran za ustrezno stopnjo tajnosti glede na tajnost podatkov, ki se v KIS obdelujejo.
Vloge	So obrazci overitelja za pridobitev ali preklic digitalnega potrdila, povrnitev zgodovine dešifrirnih ključev osebnega digitalnega potrdila.
Zasebni komunikacijsko informacijski sistem	Je komunikacijsko informacijski sistem, ki ni javen in je v lasti, upravljanju in pod nadzorom neke privatne, vladne ali nevladne organizacije.
Zasebni ključ	Polovica para ključev, ki mora ostati skriven, da se zagotovi zaupnost, integriteta, istovetnost in nezatajljivost podatkov v elektronski obliki.
Zaupni del notranjih pravil overitelja	Po Uredbi o pogojih za elektronsko poslovanje in elektronsko podpisovanje vsebuje zaupni del notranjih pravil overitelja "določila glede prostorov, osebja, fizičnega, elektronskega in programskega varovanja infrastrukture overitelja, notranjega nadzora, ukrepanja ob nepredvidenih dogodkih in določila glede vodenja zapisov in sestave dnevnikov“.
Zloraba	Je razkritje tajnega podatka, izguba celovitosti ali razpoložljivosti podatka.
Zunanji izvajalec	Je fizična ali pravna oseba, ki za MO opravlja dela po pogodbi in ni zaposlena v MO.