REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

# Pravila delovanja izdajatelja SIMoD-CA-Root, javni del

***(Javna pravila SIMoD-CA-Root)***

***Ver 3.0***

***NEURADNO PREČIŠČENO BESEDILO***

***marec 2018***

Zgodovina sprememb in dopolnitev Pravil delovanja izdajatelja SIMoD-CA-Root, javni del:

| Izdaja: | Spremembe glede na prejšnjo izdajo: |
|---|---|
| Neuradno prečiščeno besedilo Pravil delovanja izdajatelja SIMoD-CA-Root, javni del, verzija 3.0, marec 2018 | Združena sta dokumenta Pravila delovanja izdajatelja SIMoD-CA-Root, javni del, verzija 3.0, številka: 382-12/2017-38 in Pravila o dopolnitvah Pravil delovanja izdajatelja SIMoD-CA-Root, javni del, verzija 3.0, številka: 386-12/2018-15. |
| Pravila o dopolnitvah Pravil delovanja izdajatelja SIMoD-CA-Root, javni del, verzija 3.0, številka: 386-12/2018-15, datum: 28.03.2018 | Svetu za upravljanje z infrastrukturo javnih ključev na MO so dodane obveznosti v povezavi z Uredbo eIDAS, predvsem glede okoliščin in načina obveščanja nadzornega organa.<br>Dodana je obveza rednega pregledovanja Pravil delovanja izdajatelja SIMoD-CA-Root in ostalih dokumentov, povezanih z delovanjem izdajatelja SIMoD-CA-Root.<br>Dodane so določbe glede preverjanja skladnosti oziroma nadzora izdajatelja SIMoD-CA-Root kot ponudnika storitev zaupanja v skladu z Uredbo eIDAS. |
| Pravila delovanja izdajatelja SIMoD-CA-Root, javni del, verzija 3.0 | Uskladitev z Uredbo (EU) št. 910/2014 Evropskega parlamenta in sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES.<br>Uskladitev s spremembami ETSI priporočil.<br>Uskladitev izrazov; konsistentna uporaba izrazov »overitelj« in »izdajatelj«.<br>Revidiran postopek za pridobitev digitalnega potrdila podrejenega izdajatelja. |
| Pravila o spremembah in dopolnitvah Pravil delovanja overitelja SIMoD-CA-Root, javni del, verzija 2.0, številka: 386-11/2014-22, datum: 07.02.2014 | Prenehanje uporabe algoritma SHA-1 in začetek uporabe algoritma SHA256. |
| Pravila o spremembah Pravil delovanja overitelja SIMoD-CA-Root, javni del, verzija 2.0, številka: 386-6/2011-337, datum: 21.12.2011 | Podaljšana je veljavnost digitalnega potrdila oziroma javnega ključa in zasebnega ključa korenskega overitelja SIMoD-CA-Root. |
| Pravila delovanja overitelja SIMoD-CA-Root, javni del, verzija 2.0, številka: 382-5/2006-119, datum: 23.11.2010 | Pristojnost sprejemanja pravil delovanja posameznih overiteljev je prenesena na Svet za upravljanje z infrastrukturo javnih ključev na MO,<br>Dokument nima več identifikacijske oznake. |
| Spremembe in dopolnitve Pravil delovanja overitelja SIMoD-CA-Root, javni del, številka: 382-5/2006-43, datum: 27.12.2007 | Spremenjeno je pravilo za določanje identifikacijske oznake dokumenta. |

| | |
|---|---|
| Pravila delovanja overitelja SIMoD-CA-Root, javni del, šifra: 382-5/2006-12, datum: 17.7.2006 | V infrastrukturo javnih ključev na MO je umeščen korenski overitelj SIMoD-CA-Root. |
| Pravila overitelja digitalnih potrdil na Ministrstvu za obrambo Republike Slovenije – javni del notranjih pravil, šifra 471-01-6/2002-47, datum: 29.07.2005. | |

# KAZALO

# PRAVILA DELOVANJA IZDAJATELJA SIMoD-CA-Root
# JAVNI DEL

(JAVNA PRAVILA SIMoD-CA-Root)

Verzija 3.0

## 1. UVOD

### 1.1. Pregled

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

SIMoD-PKI zagotavlja sredstva elektronske identifikacije in je ponudnik storitev zaupanja kot opredeljeno v [3] eIDAS za potrebe obrambe države.

V okviru SIMoD-PKI deluje korenski izdajatelj SIMoD-CA-Root (ang. **S**lovenian **M**inistry **o**f **D**efence **Root C**ertification **A**uthority), podrejeni izdajatelji digitalnih potrdil in izdajatelji časovnih žigov.

Izdajatelj SIMoD-CA-Root deluje v okviru SIMOD-PKI, katere delovanje predpisuje [8] Politika SIMoD-PKI. [8] Politika SIMoD-PKI predpisuje splošne zahteve za digitalna potrdila, minimalne zahteve za tehnične lastnosti in raven varnosti infrastrukture izdajateljev, postopke za upravljanje z digitalnimi potrdili, obveznosti in odgovornosti, ki jih morajo izpolnjevati izdajatelji, imetniki in tretje osebe, ki se zanašajo na digitalna potrdila, ter drugi izdajatelji, ki se želijo povezovati z infrastrukturo javnih ključev na MO.

Pravila delovanja izdajatelja SIMoD-CA-Root, javni del, predstavljajo javni del notranjih pravil izdajatelja SIMoD-CA-Root.

Pravila delovanja izdajatelja SIMoD-CA-Root, javni del, podajajo opis izdajateljeve infrastrukture, postopkov izdajatelja in izpolnjevanje zahtev Politike SIMoD-PKI. Zainteresirane strani, ki potrebujejo informacije za oceno zaupanja v SIMoD-PKI kot celoto, oceno zaupanja v digitalna potrdila imetnikov, ali informacije o podrejenem izdajatelju, morajo poleg pričujočega dokumenta upoštevati še določila Politike SIMoD-PKI ter javnih pravil delovanja podrejenih izdajateljev.

Izdajatelj SIMoD-CA-Root kot korenski izdajatelj predstavlja vrh hierarhične strukture izdajateljev SIMoD-PKI. Izdajatelj SIMoD-CA-Root izdaja digitalna potrdila:

- podrejenim izdajateljev, ki izdajajo digitalna potrdila v skladu s Politiko SIMoD-PKI,
- medsebojno priznanim izdajateljem in
- operativnemu osebju za potrebe upravljanja izdajatelja SIMoD-CA-Root.

Dokument je skladen z [9] RFC 3647 in predstavlja pravila delovanja izdajatelja (ang. Certification Practices Statement, CPS) v odnosu na Politiko SIMoD-PKI, ki predstavlja politiko delovanja (ang. Certificate Policy, CP).

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

### 1.2. Identifikacijske oznake politik delovanja

Digitalna potrdila korenskega izdajatelja SIMoD-CA-Root ne vsebujejo identifikacijskih oznak (ang. Policy Object Identifier; Policy OID).

## 1.3. Udeleženci infrastrukture javnih ključev

### *1.3.1. Korenski izdajatelj SIMoD-CA-Root*

Izdajatelj SIMoD-CA-Root je korenski izdajatelj v okviru SIMoD-PKI.

Izdajatelja SIMoD-CA-Root sestavlja strojna in programska oprema ter operativno osebje. Izdajatelj SIMoD-CA-Root izvaja postopke in ukrepe, ki zagotavljajo varno in zanesljivo delovanje.

#### 1.3.1.1. Svet za upravljanje z infrastrukturo javnih ključev na MO

Svet za upravljanje z infrastrukturo javnih ključev na MO zastopa korenskega izdajatelja SIMoD-CA-Root in ima v zvezi z njim naslednje obveznosti:

- pripravlja spremembe, dopolnitve in nove verzije Pravil delovanja izdajatelja SIMoD-CA-Root, javnega in zaupnega dela,
- ocenjuje in potrjuje skladnost Pravil delovanja izdajatelja SIMoD-CA-Root, javnega in zaupnega dela, s Politiko SIMoD-PKI,
- sprejema Pravila delovanja izdajatelja SIMoD-CA-Root, javni in zaupni del,
- imenuje operativno osebje izdajatelja SIMoD-CA-Root,
- operativnemu osebju daje usmeritve za odpravljanje pomanjkljivosti, ugotovljenih ob inšpekcijskem in drugih oblikah nadzora ter uveljavlja druge ukrepe, kot je npr. preklic izdajateljevega potrdila in
- ocenjuje ustreznost politik drugih overiteljev v postopku medsebojnega priznavanja ter usmerja postopke in ukrepe formalnega medsebojnega priznavanja z drugimi overitelji.

Svet za upravljanje z infrastrukturo javnih ključev na MO je odgovoren, da izdajatelj SIMoD-CA-Root kot ponudnik storitev zaupanja izpolnjuje zahteve [3] Uredbe eIDAS.

Svet za upravljanje z infrastrukturo javnih ključev na MO ima v zvezi z izvajanjem [3] Uredbe eIDAS naslednje naloge obveščanja:

- obvesti nadzorni organ, kot ga določa **Error! Reference source not found. Error! Reference source not found.**, o vseh dejstvih, okoliščinah in spremembah, vezanih na status izdajatelja SIMoD-CA-Root kot ponudnika kvalificiranih storitev zaupanja,
- brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah po ugotovitvi, uradno obvesti nadzorni organ, po potrebi pa tudi druge pristojne organe, kot je pristojni nacionalni organ za varnost informacij ali organ za varstvo podatkov, o kršitvah varnosti ali izgubi celovitosti, ki znatno vpliva na storitev zaupanja ali na osebne podatke, vsebovane v njej.

Način obveščanja določi nadzorni organ oziroma drugi pristojni organ. Če način obveščanja ni določen, se uporabi najbolj učinkovit način sporočanja, v primeru potrebe po hitrem ukrepanju je to uradni elektronski naslov ali uradna telefonska številka organa.

#### 1.3.1.2. Operativno osebje izdajatelja SIMoD-CA-Root

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

### *1.3.2. Prijavna služba*

Izdajatelj SIMoD-CA-Root nima vzpostavljene prijavne službe.

### *1.3.3. Imetniki digitalnih potrdil*

Izdajatelj SIMoD-CA-Root izdaja digitalna potrdila podrejenim izdajateljem in medsebojno priznanim izdajateljem ter operativnemu osebju izključno za potrebe upravljanja z izdajateljevo infrastrukturo.

### *1.3.4. Tretje osebe*

Tretje osebe so osebe, ki zaupajo digitalnim potrdilom oziroma povezavi med imetnikovim imenom in javnim ključem v digitalnem potrdilu. Zaupanje izhaja iz zaupanja v samopodpisano potrdilo izdajatelja SIMoD-CA-Root.

Tretje osebe so:

- imetniki digitalnih potrdil izdajatelja SIMoD-PKI,
- imetniki digitalnih potrdil izdajateljev, ki so medsebojno priznani s SIMoD-PKI,
- podrejeni izdajatelji in
- subjekti, ki nimajo digitalnega potrdila izdajatelja SIMoD-PKI, a se zanašajo na digitalna potrdila, ki so jih je izdali izdajatelji SIMoD-PKI.

### *1.3.5. Posredno odgovorni organi*

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

## 1.4. Namen uporabe digitalnih potrdil

Korenski izdajatelj SIMoD-CA-Root izdaja digitalna potrdila podrejenim izdajateljem in medsebojno priznanim izdajateljem.

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

### *1.4.1. Dovoljena uporaba digitalnih potrdil*

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

### *1.4.2. Nedovoljena uporaba digitalnih potrdil*

Ni relevantno.

## 1.5. Upravljanje s Pravili delovanja SIMoD-CA-Root

### *1.5.1. Organ, ki upravlja s tem dokumentom*

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

Spremembe in dopolnitve oziroma nova Pravila delovanja SIMoD-CA-Root, javni in zaupni del, potrdi vodja Sveta za upravljanje z infrastrukturo javnih ključev na MO.

Svet za upravljanje z infrastrukturo javnih ključev na MO pregleda ustreznost Pravil delovanja izdajatelja SIMoD-CA-Root, javnega in zaupnega dela, ter ostalih dokumentov, povezanih z delovanjem izdajatelja SIMoD-CA-Root, vsaj enkrat (1 x) letno. Na osnovi pregleda potrdi ustreznost ali predlaga spremembe oziroma dopolnitve dokumentov.

### *1.5.2. Kontaktna oseba*

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

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

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

### *1.5.4. Postopek odobritve pravil delovanja izdajatelja SIMoD-CA-Root*

V okviru postopka odobritve Pravil delovanja izdajatelja SIMOD-CA-Root, javnega in zasebnega dela:

- Svet za upravljanje z infrastrukturo javnih ključev na MO preveri skladnost Pravil delovanja izdajatelja SIMoD-CA-Root, javnega in zaupnega dela, z zahtevami Politike SIMoD-PKI,
- vodja Sveta za upravljanje z infrastrukturo javnih ključev na MO potrdi spremembe in dopolnitve oziroma nova Pravila delovanja SIMoD-CA-Root, javni in zaupni del.

## 1.6. Pojmi in kratice

| Pojem | Definicija |
|---|---|
| Digitalni podpis | Dodan podatek ali kriptografsko preoblikovanje, ki omogoča, da prejemnik podatkov preveri njihov izvor in integriteto, ter s tem prepreči poneverbo. |
| Digitalno potrdilo | Potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto. V tem dokumentu uporabljen kot ekvivalenten izraz za »potrdilo za elektronski podpis« po [3] eIDAS. |
| Digitalno potrdilo za preverjanje podpisa | Digitalno potrdilo, ki se uporablja za verifikacijo digitalnega podpisa, preverjanje istovetnosti uporabnikov in preverjanje celovitosti podatkov v elektronski obliki. |
| Digitalno potrdilo za šifriranje | Digitalno potrdilo, ki se uporablja za izmenjavo simetričnih šifrirnih ključev pri zagotavljanju tajnosti podatkov v elektronski obliki. |
| Elektronski podpis | Niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika. |
| Elektronsko sporočilo | Niz podatkov, ki so poslani ali prejeti na elektronski način, kar vključuje predvsem elektronsko izmenjavo podatkov in elektronsko pošto. |
| Imenik | Podatkovna struktura, ki vsebuje objekte z določenimi lastnosti in pripadajočimi vrednostmi. Imenik, ki vsebuje digitalna potrdila, je običajno v skladu s standardom X.500 oziroma razširjenim standardom X.509 ver.3. |

| | |
|---|---|
| Imetnik potrdila | Fizična oseba, navedena v digitalnem potrdilu v polju »Subject«.Lastnik zasebnega ključa, ki ustreza javnemu ključu, vsebovanem v digitalnem potrdilu oziroma odgovorna oseba za uporabo digitalnega potrdila. |
| Informacijski sistem | Skupek naprav in postopkov, ki omogočajo obdelavo informacij oziroma nudijo informacijske storitve. Združuje računalniško strojno in programsko opremo, računalniške nosilce podatkov, podatkovne zbirke in druge naprave ter identifikacijske, avtorizacijske, upravljavske in nadzorne postopke v funkcionalno celoto. |
| Javni ključ | Ključ iz para ključev, ki je lahko javno objavljen. |
| Javni komunikacijsko informacijski sistem | Je komunikacijsko informacijski sistem, katerega storitve so namenjene javni uporabi. |
| Komunikacijski sistem | Skupek naprav in postopkov, ki omogočajo prenos informacij. Primeri takih sistemov so telekomunikacijski sistemi in računalniška omrežja. |
| Komunikacijsko informacijski sistem | Skupen izraz za komunikacijski in informacijski sistem. |
| Kvalificirano digitalno potrdilo | Digitalno potrdilo, ki izpolnjuje zahteve iz 28. člena ZEPEP. Izda ga overitelj, ki deluje v skladu z zahtevami iz 28. do 36. člena ZEPEP. |
| Naročnik potrdila | Fizična ali pravna oseba, ki z zahtevkom zaprosi za izdajo digitalnega potrdila. |
| Oprema za elektronsko podpisovanje | Strojna ali programska oprema ali njune specifične sestavine, ki jo izdajatelj uporablja za storitve v zvezi z elektronskim podpisovanjem ali ki se uporabljajo za oblikovanje ali preverjanje elektronskih podpisov. |
| Overitelj | Fizična ali pravna oseba, ki izdaja digitalna potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi. |
| Par ključev | Par asimetričnih kriptografskih ključev, ki ga sestavljata zasebni in javni ključ. |
| Podatki v elektronski obliki | Podatki, ki so oblikovani, shranjeni, poslani, prejeti ali izmenljivi na elektronski način. |
| Podatki za elektronsko podpisovanje | Edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa. |
| Podatki za preverjanje elektronskega podpisa | Edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa. |
| Podpisnik | Oseba, ki ustvari ali je v njenem imenu in v skladu z njeno voljo ustvarjen elektronski podpis. |
| Politika digitalnih potrdil | Nabor pravil, ki posledično definira uporabnost digitalnih potrdil v določeni skupini uporabnikov in/ali za določen nabor aplikacij s skupnimi varnostnimi zahtevami. |
| Ponudnik storitev zaupanja | Po definiciji 19. odstavka 3. člena [3] eIDAS: fizična ali pravna oseba, ki zagotavlja eno ali več storitev zaupanja. |
| Pošiljatelj elektronskega sporočila | Oseba, ki je sama poslala elektronsko sporočilo ali pa je bilo sporočilo poslano v njenem imenu in v skladu z njeno voljo; posrednik elektronskega sporočila se ne šteje za pošiljatelja tega elektronskega sporočila. |
| Potrdilo za elektronski podpis | Po definiciji 14. odstavka 3. člena [3] eIDAS: elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega podpisa s fizično osebo in potrjuje vsaj ime ali psevdonim te osebe. V tem dokumentu se namesto izraza »potrdilo za elektronski podpis« uporablja izraz »digitalno potrdilo«. |
| Prejemnik elektronskega sporočila | Oseba, ki je prejela elektronsko sporočilo; posrednik elektronskega sporočila se ne šteje za prejemnika tega elektronskega sporočila. |
| Prijavna služba | Služba oziroma organizacija, ki po pooblastilu izdajatelja sprejema zahtevke in preverja istovetnosti bodočih imetnikov. |
| Sredstvo za elektronsko podpisovanje | Nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa. |

| | |
|---|---|
| Sredstvo za varno elektronsko podpisovanje | Sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve iz 37. člena ZEPEP. |
| Storitev zaupanja | Elektronska storitev po definiciji 16. odstavka 3. člena [3] eIDAS:<br>a) ustvarjanje, preverjanje in potrjevanje veljavnosti elektronskih podpisov, elektronskih žigov ali elektronskih časovnih žigov, storitev elektronske priporočene dostave in potrdil, povezanih s temi storitvami, ali<br>b) ustvarjanje, preverjanje in potrjevanje veljavnosti potrdil za avtentikacijo spletišč ali<br>c) hrambo elektronskih podpisov, žigov ali potrdil, povezanih s temi storitvami. |
| Šifrirni (kriptografski) ključ | Niz znakov uporabljen za kriptografsko preoblikovanje (npr. šifriranje, dešifriranje, podpisovanje, ali preverjanje podpisa). |
| Tajni podatek | Dejstvo ali sredstvo iz delovnega področja organa, ki se nanaša na javno varnost, obrambne zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov določenih v [13] ZTP določiti in označiti kot tajno ter zaščititi pred nepooblaščenimi osebami. |
| Tretja oseba | Subjekt, ki ni aktivno udeležen v storitev, vendar zaupa izvajalcu in rezultatu storitve. |
| Uporabnik | Naročnik ali imetnik digitalnega potrdila. |
| Varen elektronski podpis | Elektronski podpis, ki izpolnjuje naslednje zahteve:<br>• povezan je izključno s podpisnikom,<br>• iz njega je mogoče zanesljivo ugotoviti podpisnika,<br>• ustvarjen je s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom,<br>• povezan je s podatki, na katere se nanaša, tako, da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi. |
| Zasebni komunikacijsko informacijski sistem | Komunikacijsko informacijski sistem, ki ni javen in je v lasti, upravljanju in pod nadzorom neke privatne, vladne ali nevladne organizacije. |
| Zasebni ključ | Ključ iz para ključev, ki mora ostati skriven, da se zagotovi zaupnost in celovitost podatkov v elektronski obliki. |
| Zloraba | Razkritje tajnega podatka, izguba celovitosti ali razpoložljivosti podatka. |

| Kratica | Opis |
|---|---|
| ASN.1 | Standard organizacij ISO/IEC in ITU-T, ki opisuje zapis, predstavitev, kodiranje, prenos in dekodiranje podatkovnih struktur oziroma objektov (ang. Abstract Syntax Notation One). |
| CN | Splošno ime objekta v imeniku (ang. Common Name). |
| CRL | Register preklicanih potrdil (ang. Certificate Revocation List). |
| DN | Razločevalno ime objekta v imeniku, tudi polno ime objekta v imeniku (ang. Distinguished Name). |
| eIDAS | Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (eIDAS; Uradni list EU, št. L 257/73). |
| ETSI | Evropski inštitut za standardizacijo na področju telekomunikacij; izdaja serijo standardov s področja elektronskega podpisa in delovanja overiteljev (ang. European Telecommunications Standards Institute). |
| FIPS | Standardi za informacijske tehnologije, ki so v uporabi v ameriških zveznih institucijah. Izdaja jih ameriški nacionalni inštitut za standarde in tehnologijo (ang. Federal Information Processing Standards). |
| FIPS 140-2 | Serija standardov FIPS za kriptografske module. |
| HTTP | Protokol za prenos podatkov v spletnem okolju (ang. Hypertext Transfer Protocol). |

| | |
|---|---|
| IETF | Združenje strokovnjakov s področja Internetnih tehnologij. Izdelujejo serije priporočil (ang. Internet Engineering Task Force). |
| ISO | Mednarodna organizacija za standardizacijo (ang. International Standardization Organization). |
| ITU-T | Mednarodna organizacija za standardizacijo na področju telekomunikacij (ang. International Telecommunications Union - Telecommunication Standardization Sector). |
| KIS MO in SV | Komunikacijsko informacijski sistem MO in SV. |
| LDAP | Protokol, ki določa dostop do imenika in je specificiran po IETF (ang. Internet Engineering Task Force) priporočilu RFC 1777 (LDAP, ang. Leightweight Directory Access Protocol). |
| MO | Ministrstvo za obrambo |
| OCSP | Sprotno preverjanje statusa potrdil (ang. Online Certificate Status Protocol) |
| PKCS | Priporočila podjetja RSA Security za uporabo asimetričnih kriptografskih algoritmov (ang. Public Key Cryptographic Standards). |
| PKCS#1 | Osnovna pravila za formatiranje podatkov ob implementaciji RSA funkcij. Predpisuje, kako se izračuna digitalni podpis, kako se formatirajo podatki, ki se podpisujejo in format podpisa. Predpisuje tudi sintakso javnega in zasebnega RSA ključa. |
| PKCS#10 | Sintaksa zahtevka za digitalno potrdilo. Zahtevek za digitalno potrdilo vsebuje razločevalno ime, javni ključ in nabor drugih atributov, ki jih podpiše subjekt, ki zahteva potrditev. Daljše ime: PKCS#10 Certification Request Syntax Standard. |
| PKCS#7 | Sintaksa za kriptografsko obdelane podatke, kot digitalni podpisi in digitalne ovojnice. |
| PKI | Infrastruktura javnih ključev; strojna in programska oprema ter varnostni mehanizmi za zaupanja vredno implementacijo varnostnih storitev, ki temeljijo na nesimetrični kriptografiji (ang. Public Key Infrastructure). |
| PKIX | Delovna skupina za področje infrastrukture javnih ključev v okviru IETF (ang. Internet Engineering Task Force). Izdala serijo priporočil za digitalna potrdila in registre preklicanih potrdil (ang. Public Key Infrastrukture X.509). |
| PKIX-CMP | Postopek izmenjave podatkov, ki se nanašajo na digitalna potrdila med subjekti infrastrukture overitelja (ang. PKIX Certificate Management Protocol). Vključuje PKCS#7 in PKCS#10. |
| RFC | Priporočila, ki jih izdaja IETF. |
| RFC 5280 | Priporočilo, ki določa elemente potrdil in registra preklicanih potrdil. |
| RFC 3647 | Priporočilo, ki določa elemente, ki naj bodo zajeti v politiki overitelja (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework). |
| RFC 4210 | Priporočilo, ki določa postopke za izmenjavo podatkov, ki se nanašajo na digitalna potrdila. Vsebuje PKIX-CMP. |
| RSA | Eden prvih nesimetričnih kriptografskih sistemov, patentiran leta 1983, imenovan po odkriteljih: Rivest, Shamir in Adelman. |
| SIMoD-PKI | Infrastruktura javnih ključev Ministrstva za obrambo Republike Slovenije (ang. **S**loven**i**an **M**inistry **o**f **D**efence **P**ublic **K**ey **I**nfrastructure - SIMoD-PKI) |
| SV | Slovenska vojska |
| X.501 | Standard organizacij ITU-T in ISO, ki definira poimenovanje objektov v imeniku. Tudi del serije PKIX Part1. |
| X.509 | Standard organizacij ITU-T in ISO, ki definira strukturo digitalnih potrdil. Eden izmed serije standardov ITU-ISO s področja imenikov. Tudi del RFC 5280. |

# 2. ODGOVORNOST ZA OBJAVE IN IMENIK

## 2.1. Repozitoriji

Podatki o izdajatelju SIMoD-CA-Root in njegovih digitalnih potrdilih se objavljajo v naslednjih repozitorijih:

- v imeniku LDAP in
- na spletni strani http://www.simod-pki.mors.si.

Obstaja več instanc imenika, in sicer primarni imenik ter več zrcalnih imenikov. Vsi imeniki so dostopni po protokolu LDAP.

Zrcalni imeniki vsebujejo kopijo podatkov iz primarnega imenika. Zrcalni imeniki so nameščeni v računalniških omrežjih, ki med seboj niso povezana. Vsi imajo naslov imenik.simod-pki.mors.si.

Obstaja več instanc spletne strani, in sicer primarna instanca ter več zrcalnih instanc.

Zrcalne spletne strani so kopija primarne spletne strani. Nameščene so v računalniških omrežjih, ki med seboj niso povezana. Vse instance spletne strani imajo naslov http://www.simod-pki.mors.si.

Na javno dostopni zrcalni spletni strani nekateri podatki niso objavljeni (na primer licenčna programska oprema).

## 2.2. Objave informacij o digitalnih potrdilih

Izdajatelj SIMoD-CA-Root v imeniku objavlja naslednje podatke:

- digitalno potrdilo izdajatelja SIMoD-CA-Root ter podrejenih izdajateljev,
- register preklicanih potrdil (ang. Certificate Revocation List, CRL).

Digitalna potrdila izdajateljev so v imenikih objavljena v vozliščih cn=*Izdajatelj*,ou=simod-pki,o=mors,c=si, kjer je *Izdajatelj* oznaka izdajatelja (simod-ca-root, simod-ca-restricted, itd.), in sicer v atributu cACertificate.

Register preklicanih potrdil izdajatelja SIMoD-CA-Root je objavljen v vozliščih cn=simod-ca-root,ou=simod-pki, o=mors,c=si ter cn=CRL1,cn=simod-ca-root,ou=simod-pki, o=mors,c=si v atributu certificateRevocationList.

Na spletni strani http://www.simod-pki.mors.si so objavljeni naslednji podatki o izdajatelju SIMoD-CA-Root:

- digitalno potrdilo izdajatelja SIMoD-CA-Root ter podrejenih izdajateljev,
- register preklicanih potrdil izdajatelja SIMoD-CA-Root,
- Javna pravila SIMoD-CA-Root in
- druge javne objave.

Digitalna potrdila izdajateljev so na spletnih strežnikih objavljena na naslovih http://www.simod-pki.mors.si/certs/*izdajatelj*.cacert, kjer je *izdajatelj* oznaka izdajatelja (simod-ca-root, simod-ca-restricted, itd.).

Register preklicanih potrdil izdajatelja SIMoD-CA-Root je objavljen na naslovu http://www.simod-pki.mors.si/crl/simod-ca-root.crl

## 2.3. Čas in pogostost objav

Pogostost objav registrov preklicanih izdajateljev in registrov preklicanih digitalnih potrdil je v skladu s 4.9.7 Pogostost objav registrov preklicanih potrdil.

## 2.4. Dostop do podatkov v repozitorijih

Dostop do primarnega imenika je dovoljen samo izdajatelju in upravljavcem imenika.

Dostop do digitalnih potrdil in registrov preklicanih potrdil v zrcalnih imenikih je omogočen vsem uporabnikom in tretjim osebam.

Dostop do podatkov na primarni in zrcalnih spletnih straneh je omogočen vsem uporabnikom in tretjim osebam.

Dokument Pravila delovanja izdajatelja SIMoD-CA-Root, zaupni del, ni javno objavljen.

Izdajatelj SIMoD-CA-Root zagotovi dokument Pravila delovanja izdajatelja SIMoD-CA-Root, zaupni del, in dopolnjujoča navodila ter postopkovnike, če je to potrebno zaradi nadzora, akreditacije ali medsebojnega povezovanja.

# 3. PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI

## 3.1. Določanje imen

### *3.1.1. Vrste imen*

Podrejeni izdajatelji podrobnosti o imenovanju subjektov, ki jim izdajajo digitalna potrdila, določijo v svojih pravilih delovanja.

Podatki o imetniku digitalnega potrdila v svojem digitalnem potrdilu in digitalnih potrdilih podrejenih izdajateljev so v skladu s priporočilom [10] RFC 5280.

### *3.1.2. Potreba po smiselnosti imen*

Splošno ime (ang. Common Name, CN) mora enolično identificirati podrejenega izdajatelja.

### *3.1.3. Anonimnost imetnikov in uporaba psevdonimov*

Uporaba psevdonimov ni dovoljena. Izdajatelj SIMoD-CA-Root ne izdaja digitalnih potrdil z zakrito identiteto oziroma mehanizmi zagotavljanja anonimnosti.

### *3.1.4. Pravila za interpretacijo različnih oblik imen*

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

### *3.1.5. Edinstvenost imen*

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

### *3.1.6. Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk*

Uporaba zaščitenih znamk v imenih je dovoljena samo nosilcem zaščitenih znamk. Izdajatelj SIMoD-CA-Root ne sme zavestno izdati digitalnega potrdila z imenom, ki vsebuje zaščiteno znamko naročniku, ki ni nosilec zaščitene znamke.

Operativno osebje izdajatelja SIMoD-CA-Root ni dolžno preverjati pravic do uporabe zaščitenih znamk. Svet za upravljanje z infrastrukturo javnih ključev na MO ni dolžan razčiščevati sporov glede uporabe zaščitenih znamk.

Svet za upravljanje z infrastrukturo javnih ključev na MO in operativno osebje izdajatelja SIMoD-CA-Root si pridržujejo pravico zavrniti izdajo digitalnega potrdila ali preklicati izdana digitalna potrdila udeležencev spora.

## 3.2. Preverjanje istovetnosti imetnikov ob prvi registraciji

### *3.2.1. Metode dokazovanja lastništva zasebnega ključa*

Izdajatelj SIMoD-CA-Root preverja lastništvo zasebnega ključa, ki pripada javnemu ključu v digitalnemu potrdilu, v okviru varnega postopka pred in ob prevzemu digitalnega potrdila.

Zahtevek za izdajo digitalnega potrdila podrejenemu izdajatelju mora biti v obliki RSA PKCS#10.

Dokazovanje lastništva zasebnega ključa ob izdaji digitalnih potrdil operativnemu osebju izdajatelja SIMoD-CA-Root se zagotavlja z uporabo protokola RFC 4210 PKIX-CMP ali RSA PKCS#10.

### *3.2.2. Preverjanje istovetnosti za imetnike, ki niso fizične osebe*

Za pravilnost podatkov o bodočem podrejenem izdajatelju jamči Svet za upravljanje z infrastrukturo javnih ključev na MO.

#### *3.2.3. Preverjanje istovetnosti za fizične osebe*

Izdajatelj SIMoD-CA-Root izdaja digitalna potrdila le zaposlenim v MO, ki izvajajo naloge operativnega osebja izdajatelja SIMoD-CA-Root.

Vodja Sveta za infrastrukturo javnih ključev na MO z imenovanjem operativnega osebja izdajatelja SIMoD-CA-Root jamči za njihovo istovetnost.

#### *3.2.4. Podatki o naročniku, ki se ne preverjajo*

Ni relevantno.

#### *3.2.5. Preverjanje pooblastil*

Vodja Sveta za upravljanje z infrastrukturo javnih ključev na MO z imenovanjem operativne osebe izdajatelja SIMoD-CA-Root jamči, da je to oseba, ki opravlja naloge operativne osebe.

#### *3.2.6. Merila za medsebojno povezovanje*

Medsebojno povezovanje je mogoče samo na nivoju korenskega izdajatelja SIMoD-CA-Root. Način in pogoji medsebojnega povezovanja bodo določeni s pogodbo o medsebojnem priznavanju.

Minimalni pogoji za medsebojno priznavanje:

- zadostno ujemanje politik digitalnih potrdil, za katere velja medsebojno priznavanje, 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 priznavanje.

### 3.3. Preverjanje istovetnosti za ponovno izdajo digitalnega potrdila

#### *3.3.1. Preverjanje istovetnosti pri rutinski ponovni izdaji digitalnih potrdil*

Ob rutinski ponovni izdaji digitalnega potrdila, ki je bilo izdano operativni osebi izdajatelja SIMoD-CA-Root po protokolu PKIX-CMP, imetnik izkaže svojo istovetnost s posedovanjem še veljavnega zasebnega ključa.

Rutinska ponovna izdaja digitalnega potrdila podrejenemu izdajatelju ni možna.

#### *3.3.2. Preverjanje istovetnosti za ponovno izdajo digitalnega potrdila po preklicu*

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

### 3.4. Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila

Ni relevantno.

# 4. UPRAVLJANJE Z DIGITALNIMI POTRDILI

## 4.1. Pridobitev digitalnega potrdila

### *4.1.1. Kdo lahko zaprosi za izdajo digitalnega potrdila*

Svet za upravljanje za infrastrukturo na MO na podlagi potreb po elektronskih storitvah zaupanja v KIS MO in SV odloči o uvedi podrejenega izdajatelja digitalnih potrdil SIMoD-PKI oziroma izdaji digitalnega potrdila podrejenega izdajatelja.

Na osnovi imenovanja Sveta za upravljanje z infrastrukturo javnih ključev na MO operativnega oseba izdajatelja SIMoD-CA-Root pridobi digitalno potrdilo za opravljanje svojih nalog.

### *4.1.2. Postopek bodočega imetnika za pridobitev digitalnega potrdila in odgovornosti*

V imenu bodočega podrejenega izdajatelja vodi postopek pridobitve digitalnega potrdila Svet za upravljanje z infrastrukturo javnih ključev na MO.

Odločitev Sveta za upravljanje infrastrukture javnih ključev na MO o izdaji digitalnega potrdila podrejenega izdajatelja vsebuje:

- obrazložitev odločitve,
- predlog za razločevalno ime podrejenega izdajatelja, če ni razvidno iz pravil delovanja podrejenega izdajatelja,
- predlog alternativnega imena digitalnega potrdila (po potrebi),
- dokazila o izpolnjevanju pogojev npr. oceno skladnosti pravil delovanja bodočega podrejenega izdajatelja s Politiko SIMoD-PKI.

## 4.2. Obdelava zahtevka za izdajo digitalnega potrdila

### *4.2.1. Preverjanje istovetnosti bodočega imetnika*

Za pravilnost podatkov o bodočem podrejenem izdajatelju jamči Svet za upravljanje z infrastrukturo javnih ključev na MO.

### *4.2.2. Odobritev ali zavrnitev izdaje digitalnega potrdila*

Svet za upravljanje z infrastrukturo javnih ključev na MO pred odločitvijo o izdaji digitalnega potrdila podrejenemu izdajatelju:

- oceni skladnost pravil delovanja podrejenega izdajatelja s Politiko SIMoD-PKI,
- lahko zahteva poročilo o varnostnem pregledu infrastrukture.

Svet za upravljanje z infrastrukturo javnih ključev na MO po odločitvi izda operativnemu osebju SIMoD-CA-Root nalog za izdajo digitalnega potrdila podrejenemu izdajatelju.

### *4.2.3. Čas za obdelavo zahtevka za izdajo digitalnega potrdila*

Za izdajo digitalnega potrdila podrejenega izdajatelja zahtevek ni predviden. Postopek izdaje digitalnega potrdila vodi Svet za upravljanje z infrastrukturo javnih ključev na MO. Časovni rok za izdajo digitalnega potrdila ni predpisano.

## 4.3. Izdaja digitalnega potrdila

### *4.3.1. Postopki izdajatelja SIMoD-CA-Root ob izdaji digitalnih potrdil*

Operativno osebje izdajatelja SIMoD-CA-Root v postopku izdaje digitalnega potrdila podrejenemu izdajatelju izvede naslednje:

- preveri istovetnost operativne osebe podrejenega izdajatelja, ki v postopku izdaje digitalnega potrdila preda izdajatelju SIMoD-CA-Root zahtevek z javnim ključem, za katerega se izdaja digitalno potrdilo in preveri ujemanje s podatki, vsebovanimi v nalogu za izdajo digitalnega potrdila. Istovetnost se preveri na osnovi uradnega osebnega dokumenta s sliko in službene izkaznice MO,
- preveri integriteto PKCS#10 zahtevka za izdajo digitalnega potrdila,
- preveri podatke o podrejenem izdajatelju, tako da jih primerja s podatki v nalogu,
- če so izpolnjeni zgoraj navedeni pogoji, izda digitalno potrdilo,
- zapiše digitalno potrdilo in vsebino ASN.1 strukture potrdila v berljivi obliki na trajni medij in ga preda osebi, ki je predala PKCS#10 zahtevek in
- postopek dokumentira.

#### 4.3.1.1. Dostava zasebnega ključa imetniku

Ni relevantno. Podrejeni izdajatelji sami generirajo zasebne ključe.

#### 4.3.1.2. Dostava izdajateljevega javnega ključa imetniku

Javni ključ izdajatelja SIMoD-CA-Root oziroma izdajateljevo digitalno potrdilo, ki vsebuje izdajateljev javni ključ, se izroči na trajnem mediju pooblaščeni osebi podrejenega izdajatelja hkrati z izdanim digitalnim potrdilom. Medij vsebuje poleg izdajateljevega digitalnega potrdila tudi odtis (ang. hash) in izpis vsebine ASN.1 strukture v berljivi obliki.

Digitalno potrdilo izdajatelja SIMoD-CA-Root lahko uporabniki pridobijo tudi kadarkoli iz imenika, vendar morajo preveriti istovetnost izdajatelja SIMoD-CA-Root in celovitost digitalnega potrdila.

### *4.3.2. Obvestilo naročnikom o izdaji digitalnega potrdila*

Prevzem digitalnega potrdila podrejenega izdajatelja na trajni medij s strani operativnega osebja podrejenega izdajatelja se šteje kot obvestilo izdajatelja SIMoD-CA-Root o izdaji digitalnega potrdila.

## 4.4. Prevzem digitalnega potrdila

### *4.4.1. Postopek potrditve prevzema digitalnega potrdila*

Podrejeni izdajatelji je dolžni preveriti istovetnost in vsebino izdanega digitalnega potrdila. S prvo uporabo, oziroma če podrejeni izdajatelj (tri) 3 dni od prevzema digitalnega potrdila izdajatelja SIMoD-CA-Root ne obvesti o morebitnih napakah, velja, da je potrdil točnost podatkov v digitalnem potrdilu in da prevzema tudi vse obveznosti in jamstva iz poglavja 9.6.3 Odgovornosti in jamstva imetnikov digitalnih potrdil.

### *4.4.2. Objava digitalnega potrdila*

Podrejeni izdajatelj mora objaviti izdano digitalno potrdilo v imenikih v skladu z zahtevami Politike SIMoD-PKI in svojimi pravili delovanja.

### *4.4.3. Obveščanje drugih udeležencev o izdaji digitalnega potrdila*

Ni predvideno.

## 4.5. Uporaba ključev in digitalnih potrdil

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

### *4.5.1. Uporaba ključev in digitalnih potrdil imetnikov*

#### 4.5.1.1. Zasebni ključi in digitalna potrdila izdajateljev

Izdajatelj SIMoD-CA-Root uporablja svoj zasebni ključ za podpisovanje:

- digitalnih potrdil podrejenih izdajateljev,
- digitalnih potrdil medsebojno priznanih izdajateljev,
- registrov preklicanih izdajateljev in registrov preklicanih potrdil ter
- digitalnih potrdil operativnega osebja izdajatelja SIMoD-CA-Root.

Operativno osebje izdajatelja SIMoD-CA-Root uporablja namenska digitalna potrdila in pripadajoče ključe izključno za izvajanje nalog operativnega osebja izdajatelja SIMoD-CA-Root.

#### 4.5.1.2. Zasebni ključi in digitalna potrdila prijavne službe

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

#### 4.5.1.3. Uporabniški zasebni ključi in digitalna potrdila

Ni relevantno. Izdajatelj SIMoD-CA-Root ne izdaja uporabniških digitalnih potrdil.

### *4.5.2. Uporaba digitalnih potrdil s strani tretjih oseb*

Tretja oseba je dolžna:

- pred uporabo digitalnega potrdila preveriti, ali je ustrezno za predvideno uporabo,
- uporabiti digitalno potrdilo le za namene, določene v Politiki SIMoD PKI, pravilih delovanja izdajatelja oziroma pogodbi o medsebojnem priznavanju,
- za uporabljeno digitalno potrdilo izvesti popoln postopek preverjanja poti zaupanja in
- preveriti status digitalnega potrdila v veljavnem registru preklicanih potrdil oziroma registru preklicanih izdajateljev.

## 4.6. Ponovna izdaja digitalnega potrdila brez spremembe javnega ključa

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

## 4.7. Ponovna izdaja digitalnih potrdil[1]

Ponovna izdaja digitalnega potrdila izdajatelja SIMoD-CA-Root je opisana v poglavju 5.6. Zamenjava ključev korenskega izdajatelja SIMoD-CA-Root.

### *4.7.1. Razlogi za ponovno izdajo digitalnega potrdila*

Ponovna izdaja digitalnega potrdila izdajatelja SIMoD-CA-Root in digitalnih potrdil podrejenih izdajateljev se z namenom neprekinjenega zagotavljanja storitev zaupanja izvede pred pretekom njihove veljavnosti.

### *4.7.2. Kdo lahko zahteva ponovno izdajo digitalnega potrdila*

Digitalno potrdilo se ponovno izda obstoječemu izdajatelju.

[1] Ponovna izdaja digitalnega potrdila za overitelje pomeni generiranje novega para ključev in novega digitalnega potrdila.

#### *4.7.3. Obdelava zahtevkov za ponovno izdajo digitalnega potrdila*

Za ponovno izdajo digitalnega potrdila izdajatelju SIMoD-CA-Root ali podrejenemu izdajatelju pred pretekom veljavnosti v splošnem ni potreben zahtevek ali nalog.

Ponovni izdajo izvede operativno osebje izdajateljev in o tem izdela zapisnik.

#### *4.7.4. Obvestilo imetniku o izdaji novega digitalnega potrdila*

Za obvestilo o ponovni izdaji digitalnega potrdila se šteje ponovno izdano digitalno potrdilo oziroma predaja digitalnega potrdila in vsebine ASN.1 strukture potrdila v berljivi obliki na trajni medij odgovorni osebi podrejenega izdajatelja.

#### *4.7.5. Postopek potrditve prevzema novega digitalnega potrdila*

Enako kot 4.4.1 Postopek potrditve prevzema digitalnega potrdila.

#### *4.7.6. Objava novega digitalnega potrdila*

Enako kot 4.4.2 Objava digitalnega potrdila.

#### *4.7.7. Obveščanje drugih udeležencev o izdaji digitalnega potrdila*

Enako kot 4.4.3 Obveščanje drugih udeležencev o izdaji digitalnega potrdila.

### 4.8. Sprememba digitalnega potrdila

Sprememba digitalnih potrdil zaradi spremembe podatkov v digitalnem potrdilu ni možna.

### 4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila

#### *4.9.1. Okoliščine preklica*

##### 4.9.1.1. Okoliščine preklica imetniških digitalnih potrdil

Ni relevantno.

##### 4.9.1.2. Okoliščine preklica digitalnega potrdila izdajatelja SIMoD-CA-Root

Razlogi za preklic digitalnega potrdila korenskega izdajatelja SIMoD-CA-Root so:

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

##### 4.9.1.3. Okoliščine preklica digitalnega potrdila o priznavanju drugega izdajatelja

Korenski izdajatelj SIMoD-CA-Root prekliče digitalno potrdilo o priznavanju drugega izdajatelja iz naslednjih razlogov:

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

#### 4.9.1.4. Okoliščine preklica digitalnega potrdila podrejenega izdajatelja

Razlogi za preklic digitalnega potrdila podrejenega izdajatelja so:

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

### *4.9.2. Kdo lahko zahteva preklic*

#### 4.9.2.1. Kdo lahko zahteva preklic digitalnega potrdila imetnika

Ni relevantno.

#### 4.9.2.2. Kdo lahko zahteva preklic digitalnega potrdila izdajatelja SIMoD-CA-Root

Preklic digitalnega potrdila korenskega izdajatelja SIMoD-CA-Root lahko zahteva:

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

#### 4.9.2.3. Kdo lahko zahteva preklic digitalnega potrdila o priznavanju drugega izdajatelja

Preklic digitalnega potrdila o priznavanju drugega izdajatelja lahko zahteva:

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

#### 4.9.2.4. Kdo lahko zahteva preklic digitalnega potrdila podrejenega izdajatelja

Preklic digitalnega potrdila izdajatelja lahko zahteva:

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

### *4.9.3. Postopki za preklic*

#### 4.9.3.1. Postopki preklica imetniških digitalnih potrdil

Ni relevantno.

#### 4.9.3.2. Postopki preklica digitalnega potrdila izdajatelja SIMoD-CA-Root

Preklic digitalnega potrdila korenskega izdajatelja SIMoD-CA-Root izvedeta prvi in drugi varnostni inženir na zahtevo Sveta za upravljanje z infrastrukturo javnih ključev na MO.

Korenski izdajatelj SIMoD-CA-Root mora ob preklicu svojega digitalnega potrdila izvesti naslednje postopke:

- preklicati vsa digitalna potrdila,
- zagotavljati razpoložljivost registrov preklicanih izdajateljev vsaj še devetdeset (90) dni od preklica svojega digitalnega potrdila,
- objaviti preklic digitalnega potrdila v registru preklicanih izdajateljev,
- javno objaviti obvestilo o preklicu svojega potrdila na spletni strani http://www.simod-pki.mors.si
- ustvariti nove ključe in generirati novo samopodpisano potrdilo in
- izdati podrejenim izdajateljem nova digitalna potrdila.

#### 4.9.3.3. Postopki preklica digitalnega potrdila o priznavanju drugega izdajatelja

Preklic potrdila o priznavanju drugega izdajatelja izvedeta prvi in drugi varnostni inženir korenskega izdajatelja SIMoD-CA-Root na zahtevo Sveta za upravljanje z infrastrukturo javnih ključev na MO.

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

Preklicano digitalno potrdilo mora biti objavljeno v registru preklicanih izdajateljev.

#### 4.9.3.4. Postopki preklica digitalnega potrdila podrejenega izdajatelja

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

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

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

Korenski izdajatelj SIMoD-CA-Root mora ob preklicu digitalnega potrdila podrejenega izdajatelja izvesti naslednje postopke:

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

### *4.9.4. Čas za posredovanje zahtevka za preklic*

Osebe, ki lahko zahtevajo preklic, morajo posredovati zahtevek za preklic takoj, ko izvejo za okoliščine preklica.

### *4.9.5. Čas od prejema zahtevka za preklic do preklica*

#### 4.9.5.1. Čas za preklic digitalnega potrdila imetnika

Ni relevantno.

#### 4.9.5.2. Čas za preklic digitalnega potrdila korenskega izdajatelja SIMoD-CA-Root

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

#### 4.9.5.3. Čas za preklic digitalnega potrdila o priznavanju drugega izdajatelja

Korenski izdajatelj SIMoD-CA-Root prekliče digitalno potrdilo o priznavanju drugega izdajatelja najkasneje v osmih (8) urah, če so okoliščine preklica:

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

Korenski izdajatelj SIMoD-CA-Root prekliče digitalno potrdilo o priznavanju drugega izdajatelja v roku štiriindvajset (24) ur, če je okoliščina preklica sprememba podatkov o drugem izdajatelju, tako da je potrebno izdati novo digitalno potrdilo o priznavanju drugega izdajatelja.

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

#### 4.9.5.4. Čas za preklic digitalnega potrdila podrejenega izdajatelja

Korenski izdajatelj SIMoD-CA-Root prekliče digitalno potrdilo podrejenega izdajatelja 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 [10] RFC 5280.

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

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

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

Overitelj na MO zagotavlja varnostne mehanizme ob predpostavki rednega preverjanja veljavnosti digitalnih potrdil.

### *4.9.7. Pogostost objav registrov preklicanih potrdil*

Korenski izdajatelj SIMoD-CA-Root objavlja nov register preklicanih potrdil in register preklicanih izdajateljev vsaj na dvaindevetdeset (92) dni.

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

### *4.9.8. Dovoljene zakasnitve pri objavi registrov preklicanih potrdil*

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

Korenski izdajatelj SIMoD-CA-Root izda nov register preklicanih potrdil in register preklicanih izdajateljev vsaj toliko časa pred iztekom veljavnosti starega, da je zagotovljen prenos novega registra do vseh lokacij, kjer se le ta objavlja, še pred iztekom veljavnosti starega registra.

### *4.9.9. Storitev sprotnega preverjanje statusa digitalnih potrdil*

Podprt je protokol za sprotno preverjanje statusa digitalnih potrdil (ang. On-line Certificate Status Protocol, OCSP) v skladu s priporočilom [11] RFC 6960.

### *4.9.10. Obveza sprotnega preverjanja statusa preklicanih potrdil*

Tretje osebe morajo ob uporabi digitalnega potrdila vedno preveriti, ali je digitalno potrdilo na katerega se zanašajo, preklicano. Glej tudi poglavje 4.9.6 Obveza preverjanja registra preklicanih potrdil.

### *4.9.11. Ostale oblike objavljanja preklicanih digitalnih potrdil*

Niso podprte.

### *4.9.12. Posebne zahteve glede zlorabe ključa*

Ni predpisano.

### *4.9.13. Okoliščine za začasno ukinitev veljavnosti*

Ni podprto.

### *4.9.14. Kdo lahko zahteva začasno ukinitev veljavnosti*

Ni relevantno.

#### 4.9.15. Postopki za začasno ukinitev veljavnosti

Ni relevantno.

#### 4.9.16. Omejitve obdobja začasne ukinitve veljavnosti

Ni relevantno.

### 4.10. Preverjanje statusa digitalnih potrdil

#### 4.10.1. Tehnične lastnosti storitve

Registri preklicanih potrdil so dostopni, kot je opisano v poglavju 2.2. Objave informacij o digitalnih potrdilih.

Povezava na storitve sprotnega preverjanja statusa digitalnih potrdil (OCSP) je objavljena na spletnem naslovu www.simod-pki.mors.si.

Registri preklicanih potrdil so v skladu z [10] RFC 5280.

Sprotno preverjanje statusa potrdil je v skladu z [11] RFC 6960.

#### 4.10.2. Razpoložljivost storitve

Preverjanje statusa digitalnih potrdil je na razpolago štiriindvajset (24) ur vse dni v letu.

#### 4.10.3. Dodatne možnosti

Niso na voljo.

### 4.11. Predčasna prekinitev veljavnosti digitalnih potrdil

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

### 4.12. Varnostno kopiranje in odkrivanje zasebnega ključa

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

Korenski izdajatelj SIMoD-CA-Root zagotavlja varnostno kopiranje svojega zasebnega ključa (ang. Key Backup) v skladu s poglavjem 6.2.4 Varnostno kopiranje zasebnih ključev.

#### 4.12.1. Povrnitev zgodovine ključev za dešifriranje

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

#### 4.12.2. Odkrivanje kopije ključev za dešifriranje

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

#### 4.12.3. Zaščita odkritega zasebnega ključa in postopek prenosa

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

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

## 5.1. Fizično varovanje

### *5.1.1. Lokacija in konstrukcija prostorov*

Komunikacijska in informacijska oprema korenskega izdajatelja SIMoD-CA-Root je nameščena v posebnih in ločenih prostorih, ki so varovani z več nivojskim sistemom fizičnega in tehničnega varovanja.

Informacijska oprema izdajatelja SIMoD-CA-Root je v prostoru, ki je varnostno območje II. stopnje po [13] ZTP.

### *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 korenskega izdajatelja SIMoD-CA-Root. Druge osebe, ki izkažejo upravičeni interes, smejo vstopiti v prostore samo v spremstvu operativnega osebja. O vstopih in izstopih v prostore se vodi evidenca.

### *5.1.3. Napajanje in klimatske naprave*

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

### *5.1.4. Zaščita pred poplavo*

Prostori z informacijsko opremo korenskega izdajatelja SIMoD-CA-Root se nahajajo na lokaciji, kjer je verjetnost poplave zelo majhna.

### *5.1.5. Zaščita pred ognjem*

Prostori z informacijsko opremo korenskega izdajatelja SIMoD-CA-Root so opremljeni z detektorji temperature in dima.

### *5.1.6. Shranjevanje medijev*

Mediji z varnostnimi kopijami in arhivom podatkov se hranijo v protivlomni omari.

Mediji z varnostnimi kopijami in arhivom podatkov na oddaljeni lokaciji se hranijo v varnostno ekvivalentnih pogojih.

### *5.1.7. Odstranjevanje odpadkov*

Zagotovljeno je uničevanje dokumentov v fizični in elektronski obliki ter elektronskih medijev v skladu s področnimi predpisi.

Če dokumentov in medijev ni mogoče varno izbrisati ali uničiti v prostorih korenskega izdajatelja SIMoD-CA-Root, se jih dostavi v uničevalno mesto in uniči po postopku, predpisanem za stopnjo tajnosti dokumenta oziroma podatkov, ki jih medij hrani.

### *5.1.8. Hranjenje na oddaljeni lokaciji*

Varnostne kopije in arhivski podatki se hranijo tudi na oddaljeni lokaciji, kjer so zagotovljeni varnostno ekvivalentnih pogojih kot na primarni lokaciji.

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

## 5.2. Organizacijski varnostni ukrepi

### *5.2.1. Organizacija korenskega izdajatelja SIMoD-CA-Root*

#### 5.2.1.1. Operativno osebje

Naloge upravljanja s korenskim izdajateljem SIMoD-CA-Root izvaja operativno osebje, ki je glede na vsebinska področja razdeljeno na zaključeni organizacijski skupini:

- upravljanje z digitalnimi potrdili in
- upravljanje s programsko in strojno opremo.

V skupini za upravljanje z digitalnimi potrdili korenskega izdajatelja SIMoD-CA-Root so:

- prvi varnostni inženir in
- drugi varnostni inženirji.

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

- prvi administrator in
- administratorji.

Podrobnejša razdelitev nalog je del zaupnega dela pravil delovanja korenskega izdajatelja SIMoD-CA-Root.

#### 5.2.1.2. Prijavna služba

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

#### 5.2.1.3. Druge funkcije

Pristojne organizacijske enote v MO skrbijo za:

- fizično varovanje in nadzor prostorov korenskega izdajatelja SIMoD-CA-Root ter
- pravne zadeve.

### *5.2.2. Število oseb, potrebnih za izvedbo postopkov*

V skupini za upravljane z digitalnimi potrdili korenskega izdajatelja SIMoD-CA-Root so najmanj tri (3) osebe, v organizacijski skupini za upravljane s programsko in strojno opremo korenskega izdajatelja SIMoD-CA-Root sta najmanj dve (2) osebi.

Zahteve glede števila prisotnih oseb za izvedbo varnostno občutljivih kriptografskih operacij so predpisane v poglavju 6.2.2 Nadzor zasebnega ključa z več pooblaščenimi osebami.

### *5.2.3. Preverjanje istovetnosti operativnega osebja*

Operativno osebje korenskega izdajatelja SIMoD-CA-Root izkaže svojo istovetnost:

- pri vstopu v varovane prostore z informacijsko opremo izdajatelja z identifikacijsko kartico in vstopno kodo,
- za delo na izdajateljevem informacijskem sistemu s prijavnim imenom in geslom ter
- za upravljanje digitalnih potrdil z digitalnim potrdilom.

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

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

## 5.3. Zahteve za osebje izdajatelja SIMoD-CA-Root

### *5.3.1. Kvalifikacije, izkušnje in varnostno preverjanje*

Operativno osebje korenskega izdajatelja SIMoD-CA-Root:

- je ustrezno usposobljeno,
- ima za opravljanje nalog operativne osebe korenskega izdajatelja SIMoD-CA-Root imenovanje Sveta za upravljanje z infrastrukturo javnih ključev na MO,
- ne sme opravljati drugih nalog, ki bi bile v nasprotju z opravljanjem nalog pri korenskem izdajatelju SIMoD-CA-Root,
- ne sme biti na prejšnjih podobnih dolžnostih (npr. skrbnik kriptografskih naprav, varnostni inženir v informacijskem sistemu) razrešeno nalog zaradi malomarnosti ali neizpolnjevanja obveznosti in
- mora imeti dovoljenje za dostop do tajnih podatkov najmanj TAJNO.

### *5.3.2. Dovoljenja za dostop do tajnih podatkov*

V skladu z [13] ZTP.

### *5.3.3. Usposabljanje osebja*

Operativno osebje korenskega izdajatelja SIMoD-CA-Root se usposablja za opravljanje svojih nalog.

### *5.3.4. Pogostost dodatnih usposabljanj*

Osebje se usposablja glede na potrebe oziroma novosti v zvezi z delovanjem korenskega izdajatelja SIMoD-CA-Root.

### *5.3.5. Kroženje med delovnimi mesti*

Ni predpisano.

### *5.3.6. Ukrepi ob kršitvah pooblastil*

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

### *5.3.7. Zunanji izvajalci*

Zunanji izvajalci morajo za izvajanje posegov izpolnjevati vse pogoje, določene v [13] ZTP in vse varnostne zahteve korenskega izdajatelja SIMoD-CA-Root.

### *5.3.8. Dokumentacija za operativno osebje*

Operativnemu osebju korenskega izdajatelja SIMoD-CA-Root so na voljo interni priročniki, originalna dokumentacija programske in strojne opreme ter priročniki šolanj.

## 5.4. Postopki varnostnih pregledov sistema

### *5.4.1. Vrste beleženih dogodkov*

Korenski izdajatelj SIMoD-CA-Root beleži dogodke:

- na svojem operacijskem sistemu, programski in strojni opremi,
- v zvezi s svojimi ključi,
- v zvezi s ključi in digitalnimi potrdili podrejenih izdajateljev - izdaja, prevzem, ponovna izdaja in preklic ter
- v zvezi z varnostno politiko in upravljanjem informacijskega sistema korenskega izdajatelja SIMoD-CA-Root.

V elektronski ali pisni obliki se beležijo tudi dogodki, ki niso vezani direktno na informacijski sistem korenskega izdajatelja SIMoD-CA-Root, a vplivajo na njegovo varnost:

- dogodki v zvezi s fizičnim dostopom ter fizično lokacijo,
- kadrovske spremembe operativnega osebja izdajatelja SIMoD-CA-Root,
- dogodki, povezani z uničevanjem občutljivega materiala, na primer kriptografskega materiala oziroma ključev in nosilcev ključev.

#### *5.4.2. Pogostost pregleda dnevnikov beleženih dogodkov*

Operativno osebje pregleda dnevnike beleženih dogodkov v primeru napak na strežniku korenskega izdajatelja SIMoD-CA-Root.

#### *5.4.3. Obdobje hranjenja dnevnikov beleženih dogodkov*

Najmanj sedem (7) let v arhivu.

#### *5.4.4. Zaščita dnevnikov beleženih dogodkov*

Dnevniki se hranijo na sistemu, kjer nastanejo. Zaščiteni so z varnostnimi mehanizmi, ki zagotavljajo čim višji nivo varnosti.

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

Dostop do dnevnikov beleženih dogodkov je dovoljen samo pooblaščenim osebam:

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

#### *5.4.5. Varnostne kopije dnevnikov beleženih dogodkov*

Varnostne kopije dnevnikov beleženih dogodkov v elektronski obliki se izdeluje v okviru rednega varnostnega kopiranja sistemov. Varnostne kopije so zaščitene z varnostnimi mehanizmi, ki zagotavljajo čim višji nivo varnosti.

Periodično se en izvod varnostne kopije dnevnikov beleženih dogodkov v elektronski obliki prenese na oddaljeno lokacijo.

#### *5.4.6. Način zbiranja beleženih dogodkov*

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

#### *5.4.7. Obveščanje povzročitelja dogodka*

Povzročitelja dogodka o dogodku ni treba obvestiti.

#### *5.4.8. Ocena in odprava ranljivosti*

Dnevnike beleženih dogodkov pregleduje operativno osebje korenskega izdajatelja SIMoD-CA-Root 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*

Korenski izdajatelj SIMoD-CA-Root hrani naslednje podatke:

- dnevnike beleženih dogodkov iz poglavja 5.4.1 Vrste beleženih dogodkov,
- naloge za izdajo digitalnih potrdil podrejenih izdajateljev in spremljajoče dokumente,
- dokumentacijo o izvedbi postopkov izdaje digitalnih potrdil,
- sklenjene medsebojne dogovore oz. pogodbe,

- korespondenco s subjekti, katerim je korenski izdajatelj SIMoD-CA-Root izdal digitalno potrdilo,
- digitalna potrdila, liste preklicanih potrdil in liste preklicanih izdajateljev,
- verzije svojih pravil delovanja, javnih in zaupnih delov ter
- zasebne dešifrirne ključe v skladu s poglavjem 6.2.4 Varnostno kopiranje zasebnih ključev.

### *5.5.2. Obdobje hranjenja arhiva*

Arhivirani podatki v zvezi z digitalnimi potrdili in ključi se hranijo vsaj sedem (7) let po preteku veljavnosti digitalnega potrdila, na katerega se podatek nanaša.

Ostali arhivirani podatki se hranijo vsaj sedem (7) let po njihovem nastanku.

### *5.5.3. Zaščita arhiva*

Podatki, ki sodijo v dokumentarno gradivo (nalogi za izdajo digitalnih potrdil in spremljajoči dokumenti, dokumentacija o izvedbi postopka izdaje digitalnih potrdil, sklenjeni medsebojni dogovori oz. pogodbe, korespondenca s subjekti, katerim je korenski izdajatelj SIMoD-CA-Root izdal digitalno potrdilo in verzije pravil delovanja) se hranijo in arhivirajo v skladu s predpisi za delo z dokumentarnim gradivom na MO.

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

### *5.5.4. Varnostna kopija arhiva*

Podatkom, ki sodijo v dokumentarno gradivo (glej prvi odstavek poglavja 5.5.3 Zaščita arhiva), se hranijo in arhivirajo v skladu s predpisi za delo z dokumentarnim gradivom na MO.

Ob izdelavi arhiva podatkov, ki se beležijo v okviru komunikacijskega in informacijskega sistema izdajatelja SIMoD-CA-Restricted (glej drugi odstavek poglavja 5.5.3 Zaščita arhiva), se izdela varnostna kopija.

### *5.5.5. Časovno žigosanje zapisov*

Ni predpisano.

### *5.5.6. Način arhiviranja*

Način zbiranja arhivskih podatkov je del zaupnega dela pravil delovanja.

### *5.5.7. Postopek vpogleda v arhiv in njegova verifikacija*

Dostop do arhiva je omogočen samo:

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

Ob kreiranju arhiva se preveri integriteta medija.

## 5.6. Zamenjava ključev korenskega izdajatelja SIMoD-CA-Root

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

Za podpisovanje digitalnih potrdil podrejenih izdajateljev se vedno uporablja najnovejši zasebni ključ korenskega izdajatelja SIMoD-CA-Root. Za preverjanje veljavnosti digitalnih potrdil podrejenih izdajateljev pa se uporablja predhodno potrdilo korenskega izdajatelja SIMoD-CA-Root vse dokler ne poteče veljavnost zadnjega digitalnega potrdila, podpisanega s

pripadajočim zasebnim ključem. Zasebni ključ se vedno uporablja krajše obdobje kot je veljavnost pripadajočega digitalnega potrdila.

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

Ponovna izdaja digitalnega potrdila korenskega izdajatelja SIMoD-CA-Root se izvede po predpisanem in nadzorovanem postopku. Posamezne korake postopka izvaja operativno osebje korenskega izdajatelja SIMoD-CA-Root. Izvedba postopka je dokumentirana v zapisniku.

## 5.7. Okrevalni načrt

### *5.7.1. Postopki v primeru okvar in zlorab*

Postopki v primeru okvar in zlorab so del okrevalnega načrta, ki je predpisan v zaupnem delu pravil delovanja.

### *5.7.2. Uničenje programske, strojne opreme ali podatkov izdajatelja*

V primeru okvare strojne ali programske opreme oziroma podatkov, pri kateri zasebni ključ korenskega izdajatelja SIMoD-CA-Root ni bil uničen, bodo storitve izdajatelja vzpostavljene nazaj v najkrajšem možnem času. Korenski izdajatelj SIMoD-CA-Root bo v najkrajšem možnem času vzpostavil vsaj funkcionalnost preklica digitalnih potrdil in objavljanja registra preklicanih izdajateljev. Skrajni rok za vzpostavitev storitve preklica digitalnih potrdil in objavljanja registra preklicanih izdajateljev je sedem (7) dni. Po tem roku bo korenski izdajatelj SIMoD-CA-Root objavil preklic svojega potrdila in ukrepal v skladu s poglavjem 4.9.3.2 Postopki preklica digitalnega potrdila izdajatelja SIMoD-CA-Root.

V primeru okvare, kjer pride do uničenja zasebnega ključa korenskega izdajatelja SIMoD-CA-Root in vseh njegovih kopij, se postopa, kot da je prišlo do zlorabe ključa v skladu s poglavjem 4.9.3.2 Postopki preklica digitalnega potrdila izdajatelja SIMoD-CA-Root.

### *5.7.3. Zloraba zasebnega ključa izdajatelja SIMoD-CA-Root*

Postopki ob zlorabi zasebnega ključa korenskega izdajatelja SIMoD-CA-Root so predpisani v poglavju 4.9.3.2 Postopki preklica digitalnega potrdila izdajatelja SIMoD-CA-Root.

### *5.7.4. Zagotavljanje kontinuitete delovanja po nesrečah*

Postopki v primeru naravnih in drugih nesreč, ki imajo za posledico fizično uničenje ali varnostno vprašljivo delovanje programske ali strojne opreme ali ogroženo celovitost podatkov korenskega izdajatelja SIMoD-CA-Root oziroma uničenje in poškodovanje varovanih prostorov korenskega izdajatelja SIMoD-CA-Root, so del okrevalnega načrta, ki je predpisan v zaupnem delu pravil delovanja.

## 5.8. Prenehanje delovanja korenskega izdajatelja SIMoD-CA-Root

Vzroki za prenehanje delovanja korenskega izdajatelja SIMoD-CA-Root so podani v poglavju 4.9.1.2 Okoliščine preklica digitalnega potrdila izdajatelja SIMoD-CA-Root in veljavni zakonodaji.

Sklep o prenehanju delovanja izda Svet za upravljanje z infrastrukturo javnih ključev na MO.

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

- operativno osebje in
- medsebojno priznane ali podrejene izdajatelje.

Korenski izdajatelj SIMoD-CA-Root bo po prenehanju delovanja izvedel postopke predpisane v poglavju 4.9.3.2 Postopki preklica digitalnega potrdila izdajatelja SIMoD-CA-Root.

# 6. TEHNIČNE VARNOSTNE ZAHTEVE

## 6.1. Generiranje in namestitev para ključev

### *6.1.1. Generiranje para ključev*

Postopek generiranja ključev korenskega izdajatelja SIMoD-CA-Root izvede operativno osebje. Izvedba postopka je dokumentirana v zapisniku. Generiranje para ključev je vedno izvedeno znotraj varnostnega kriptografskega modula.

Par ključev podrejenih izdajateljev se vedno generira pri podrejenem izdajatelju v njegovem varnostnem kriptografskem modulu in pod njegovo izključno kontrolo.

### *6.1.2. Dostava zasebnega ključa imetniku*

Ni relevantno. Korenski izdajatelj SIMoD-CA-Root ne generira zasebnih ključev podrejenim ali medsebojno priznanim izdajateljem.

### *6.1.3. Dostava imetnikovega javnega ključa izdajatelju SIMoD-CA-Root*

Podrejeni izdajatelj dostavi svoj javni ključ v kot del PKCS#10 zahtevka za izdajo digitalnega potrdila.

### *6.1.4. Dostava izdajateljevega javnega ključa uporabnikom*

Javni ključ korenskega izdajatelja SIMoD-CA-Root oziroma izdajateljevo digitalno potrdilo, ki vsebuje javni ključ, se preda podrejenemu ali medsebojno priznanemu izdajatelju v postopku izdaje digitalnega potrdila podrejenega oziroma medsebojno priznanega izdajatelja.

Tretje osebe lahko pridobijo javni ključ korenskega izdajatelja SIMoD-CA-Root oziroma digitalno potrdilo, ki vsebuje javni ključ, kadarkoli iz imenika ali na spletnih straneh (poglavje 2.2. Objave informacij o digitalnih potrdilih) vendar je njihova obveznost, da preverijo istovetnost korenskega izdajatelja SIMoD-CA-Root in celovitost izdajateljevega digitalnega potrdila.

### *6.1.5. Dolžina ključev*

Dolžina RSA zasebnega ključa podrejenih izdajateljev SIMoD-PKI je najmanj 3072 bitov.

### *6.1.6. Parametri za generiranje javnih ključev in preverjanje parametrov*

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

### *6.1.7. Namen uporabe ključev*

Namen uporabe ključev je določen v razširitvenem polju *keyUsage* in *extKeyUsage* po priporočilu [10] RFC 5280.

Ključi korenskega izdajatelja SIMoD-CA-Root se uporabljajo samo za podpisovanje digitalnih potrdil, registrov preklicanih potrdil in registrov preklicanih izdajateljev.

Dovoljene vrednosti razširitvenega polja za digitalna potrdila korenskega izdajatelje SIMoD-CA-Root in podrejene izdajatelje sta:

- *KeyCertSign* in
- *CRLSign*.

## 6.2. Zaščita zasebnih ključev in zahteve za kriptografske module

### *6.2.1. Standardi za kriptografski modul*

Korenski izdajatelj SIMoD-CA-Root uporablja strojni varnostni kriptografski modul, ki ustreza varnostnemu tehničnemu standardu [6] ETSI EN 319 411-1, poglavje 6.5.2..

### *6.2.2. Nadzor zasebnega ključa z več pooblaščenimi osebami*

Za upravljanje z zasebnim ključem korenskega izdajatelja SIMoD-CA-Root oziroma z varnostnim kriptografskim modulom je potrebna prisotnost vsaj dveh (2) oseb z ustreznimi pooblastili, ki izkažeta svojo istovetnost s pametno kartico s porazdeljenim ključem kriptografskega modula in geslom kartice.

### *6.2.3. Odkrivanje zasebnega ključa*

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

### *6.2.4. Varnostno kopiranje zasebnih ključev*

Varnostna kopija zasebnega ključa korenskega izdajatelja SIMoD-CA-Root se zagotavlja z mehanizmi varnostnega kriptografskega modula. Varnostna kopija se pred izvozom iz varnostnega kriptografskega modula šifrira. Dešifrirni ključ je porazdeljen na N[2] od M[3] administratorskih pametnih karticah.

Korenski izdajatelja SIMoD-CA-Root ne hrani kopij zasebnih ključev podrejenih izdajateljev.

### *6.2.5. Arhiviranje zasebnega ključa*

Zasebni ključ korenskega izdajatelja SIMoD-CA-Root se ne arhivira.

### *6.2.6. Zapis zasebnega ključa v kriptografski modul in iz njega*

Zasebni ključ korenskega izdajatelja SIMoD-CA-Root se generira v varnostnem kriptografskem modulu. Tehnična izvedba varnostnega kriptografskega modula ne omogoča izvoza in prikaza zasebnega ključa v nešifrirani obliki.

### *6.2.7. Hranjenje zasebnega ključev v kriptografskem modulu*

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

### *6.2.8. Postopek za aktiviranje zasebnega ključa*

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

### *6.2.9. Postopek za deaktiviranje zasebnega ključa*

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

### *6.2.10. Postopek za uničenje zasebnega ključa*

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

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

#### *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*

Korenski izdajatelj SIMoD-CA-Root arhivira svoj javni ključ za preverjanje podpisa in izdana digitalna potrdila kot del arhiviranja digitalnih potrdil kot predpisano v poglavju 5.5. Arhiviranje podatkov.

#### *6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil*

Veljavnost digitalnega potrdila korenskega izdajatelja SIMoD-CA-Root je največ štiriindvajset (24) let.

Veljavnost digitalnih potrdil podrejenih izdajateljev je največ dvajset (20) let oziroma do poteka veljavnosti digitalnega potrdila korenskega izdajatelja SIMoD-CA-Restricted.

### 6.4. Gesla za dostop do zasebnih ključev

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

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

#### *6.4.2. Zaščita gesel*

Gesla se morajo hraniti na način, ki zagotavlja njihovo zaupnost.

#### *6.4.3. Druge zahteve za gesla*

Geslo mora biti dolgo najmanj 9 znakov in mora vsebovati velike in male črke, številke ter posebne znake in ne sme biti beseda iz slovarja. Če izvedba varnostnega kriptografskega modula ne omogoča takega kompleksnega gesla, je potrebno izbrati najmočnejše geslo v okviru tehničnih možnosti..

### 6.5. Varnostne zahteve za računalnike

#### *6.5.1. Specifične tehnične varnostne zahteve za računalnike*

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

- kontrolo dostopa do izdajateljevih storitev,
- delitev nalog med operativnim osebjem,
- preverjanje istovetnosti operativnega osebja,
- šifriranje zaupnih podatkov v svoji podatkovni bazi,
- varnostne beležke vseh varnostno relevantnih dogodkov,
- varen arhiv in varno hranjenje varnostnih beležk,
- mehanizme restavriranja sistema, ključev in baze podatkov.

#### *6.5.2. Raven varnostne zaščite računalnikov*

Informacijski sistem korenskega izdajatelja SIMoD-CA-Root za upravljanje z digitalnimi potrdili dosega raven varnostne zaščite vsaj CC EAL4+.

## 6.6. Tehnični nadzor življenjskega cikla izdajatelja

### *6.6.1. Nadzor razvoja sistema*

Strojna oprema, operacijski sistem in programska oprema korenskega izdajatelja SIMoD-CA-Root so komercialni proizvodi.

### *6.6.2. Upravljanje varnosti*

Korenski izdajatelj SIMoD-CA-Root evidentira postopke inštalacije, spremembe konfiguracije in nadgradnje.

Programska oprema korenskega izdajatelja SIMoD-CA-Root je zaščitena na način, da se da preveriti njen izvor in celovitost.

### *6.6.3. Upravljanje varnosti čez življenjski cikel*

Nadgradnje, nove verzije in popravki delov informacijskih sistemov korenskega izdajatelja SIMoD-CA-Root, oziroma upravljanje varnosti skozi celoten življenjski cikel je v skladu s poglavjem 6.6.2 Upravljanje varnosti.

## 6.7. Varnostne kontrole na ravni računalniškega omrežja

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

## 6.8. Časovno žigosanje

Ni predpisano.

# 7. PROFIL DIGITALNIH POTRDIL IN REGISTROV PREKLICANIH POTRDIL

## 7.1. Profil digitalnih potrdil

### *7.1.1. Verzija digitalnih potrdil*

Korenski izdajatelj SIMoD-CA-Root izdaja digitalna potrdila X.509 verzije 3 v skladu s priporočilom [10] RFC 5280, ki vsebujejo naslednja osnovna polja:

| Ime osnovnega polja / prevod ali opis | Vrednost polja v potrdilu korenskega izdajatelja SIMoD-CA-Root | Vrednost polja v potrdilu podrejenega izdajatelja |
|---|---|---|
| *Version*<br>X.509 verzija | *V3* | *v3* |
| *Serial Number*<br>serijska številka | enolična serijska številka na nivoju SIMoD-CA-Root | enolična serijska številka na nivoju SIMoD-CA-Root |
| *Signature Algorithm*<br>Algoritem za podpis | *Sha256WithRSAEncryption* | *Sha256WithRSAEncryption* |
| *Issuer*<br>izdajatelj | razločevalno ime SIMoD-CA-Root | razločevalno ime SIMoD-CA-Root |
| *Validity*<br>veljavnost potrdila | *Not Before:* pričetek veljavnosti po GMT<br>*Not After:* konec veljavnosti po GMT | *Not Before:* pričetek veljavnosti po GMT<br>*Not After:* konec veljavnosti po GMT |
| *Subject*<br>imetnik | razločevalno ime SIMoD-CA-Root | razločevalno ime podrejenega izdajatelja |
| *Public Key*<br>podatki o imetnikovem javnem ključu | *rsaEncryption*, modul, eksponent, vrednost javnega ključa | *rsaEncryption*, modul, eksponent, vrednost javnega ključa |

### *7.1.2. Razširitvena polja*

Standardna razširitvena polja po priporočilu [10] RFC 5280, uporabljena v digitalnih potrdilih korenskega izdajatelja SIMoD-CA-Root in podrejenih izdajateljev:

| Ime standardnega razširitvenega polja / prevod ali opis | Vrednost polja v potrdilu korenskega izdajatelja SIMoD-CA-Root | Vrednost polja v potrdilu podrejenega izdajatelja |
|---|---|---|
| *Authority Key Identifier*<br>odtis javnega ključa izdajatelja | ni uporabljeno | SHA256 odtis javnega ključa izdajatelja SIMoD-CA-Root, s katerim je podpisano potrdilo |
| *Subject Key Identifier*<br>odtis imetnikovega javnega ključa | SHA256 odtis javnega ključa izdajatelja SIMoD-CA-Root | SHA256 odtis javnega ključa podrejenega izdajatelja |
| *Key Usage*<br>namen uporabe ključa | **Kritično**<br>*keyCertSign*<br>*cRLSign* | **Kritično**<br>*keyCertSign*<br>*cRLSign* |
| *Extended Key Usage*<br>razširjen namen uporabe ključa | ni uporabljeno | ni uporabljeno |
| *Certificate Policies*<br>oznaka politike potrdila | ni uporabljeno | ni uporabljeno |

| | | |
|---|---|---|
| *CRL Distribution Points*<br>naslovi registra preklicanih potrdil | ni uporabljeno | LDAP in http URL naslov registra preklicanih potrdil korenskega izdajatelja SIMoD-CA-Root |
| Subject Alternative Name<br>alternativno ime imetnika | ni uporabljeno | ni uporabljeno |
| *Basic Constraints*<br>osnovne omejitve | **Kritično**<br>*CA =: True*<br>*pathLenConstraint = 1* | **Kritično**<br>*CA =: True*<br>*pathLenConstraint = 0* |
| *Authority Info Access /*<br>dostop do informacij o izdajatelju | ni uporabljeno | URL naslov izdajatelja |

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

### *7.1.3. Identifikacijske oznake algoritmov*

Identifikacijski oznaki kriptografskih algoritmov, uporabljenih v digitalnih potrdilih, ki jih izdaja korenski izdajatelj SIMoD-CA-Root, sta:

| Algoritem | Identifikacijska oznaka |
|---|---|
| rsaEncryption | 1.2.840.113549.1.1.1 |
| sha256WithRSAEncryption | 1.2.840.113549.1.1.11 |

### *7.1.4. Oblike imen*

Predpisano 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.

Omejitve glede imen (polje *nameConstraints*) niso predpisane.

### *7.1.6. Identifikacijska oznaka politik*

Digitalna potrdila korenskega izdajatelja SIMoD-CA-Root in podrejenih izdajateljev nimajo identifikacijske oznake politike.

### *7.1.7. Način uporabe razširitvenega polja za omejitev uporabe politik*

Omejitve uporabe politik (polje *Policy Constrains*) niso predpisane.

### *7.1.8. Specifični podatki o politiki*

Razširitveno polje za specifične podatke o politiki *certificatePolicies, policyQualifier* se v digitalnih potrdilih izdajateljev ne uporablja.

### *7.1.9. Procesiranje oznake kritičnosti razširitvenih polj*

Uporabniške aplikacije morajo procesirati razširitvena polja, označena kot kritična, v skladu s priporočili [10] RFC 5280.

## 7.2. Profil registrov preklicanih potrdil

### *7.2.1. Verzija registrov preklicanih potrdil*

Korenski izdajatelj SIMoD-CA-Root izdaja registre preklicanih potrdil verzije 2 v skladu s priporočilom [10] RFC 5280, ki vsebujejo naslednja osnovna polja:

| Ime osnovnega polja | | Prevod ali opis | Vrednost |
|---|---|---|---|
| *version* | | verzija | v2 |
| *signature* | | algoritem za podpis registra | *Sha256WithRSAEncryption* |
| *Issuer* | | izdajatelj | razločevalno ime izdajatelja |
| *thisUpdate* | | čas izdaje registra | čas izdaje po GMT |
| *nextUpdate* | | čas izdaje naslednjega registra | čas naslednje izdaje po GMT |
| *revokedCertificates:* | | preklicana potrdila | |
| | *userCertificate* | preklicano potrdilo | serijska številka preklicanega potrdila |
| | *revocationDate* | datum preklica | čas preklica |
| | *reasonCode* | vzrok za preklic | *Unspecified (0), keyCompromise (1), cACompromise (2), affiliationChanged(3), superseded (4), cessationOfOperation (5), certificateHold (6), removeFromCRL (8), privilegeWithdrawn (9), aACompromise (10)* |

### *7.2.2. Razširitvena polja registrov preklicanih potrdil*

Korenski izdajatelj SIMoD-CA-Root izdaja registre preklicanih potrdil verzije 2 v skladu s priporočilom [10] RFC 5280, ki vsebujejo naslednja standardna razširitvena polja:

| Ime razširitvenega polja | Prevod ali opis | Vrednost |
|---|---|---|
| *CRLNumber* | zaporedna številka registra | zaporedna številka registra |
| *AuthorityKeyIdentifier* | identifikator javnega ključa izdajatelja, ki podpisuje register preklicanih potrdil | SHA256 odtis javnega ključa izdajatelja |

## 7.3. Profil sprotnega preverjanja statusa potrdil

### *7.3.1. Verzija sprotnega preverjanja statusa digitalnih potrdil*

Storitev sprotnega preverjanja statusa digitalnih potrdil (OCSP) je v skladu s priporočilom [11] RFC 6960.

### *7.3.2. Razširitve sprotnega preverjanja statusa digitalnih potrdil*

Sporočila OCSP zahtevek/odgovor podpirajo razširitev Nonce, ki ni označena kot kritična.

# 8. PREVERJANJE SKLADNOSTI IN OSTALE OBLIKE NADZORA

## 8.1. Pogostost inšpekcije

Pogostost inšpekcijskega nadzora je določena z veljavno zakonodajo.

Nadzor izdajatelja SIMoD-CA-Root kot ponudnika storitev zaupanja je v skladu z oddelkom 2 [3] Uredbe eIDAS.

Nadzor izdajatelja SIMoD-CA-Root kot ponudnika kvalificiranih storitev zaupanja je v skladu z 20. členom [3] Uredbe eIDAS.

V skladu z prvim odstavkom 20. člena [3] Uredbe eIDAS je pogostost nadzora za ugotavljanje skladnosti ponudnika kvalificiranih storitev zaupanja in kvalificiranih storitev zaupanja vsaj vsakih 24 mesecev.

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

## 8.2. Pogoji za inšpektorja

Inšpekcijski nadzor izvaja pristojna inšpekcijska služba v skladu z veljavno zakonodajo.

Skladnost izdajatelja SIMoD-CA-Root kot ponudnika kvalificiranih storitev zaupanja z zahtevami [3] Uredbe eIDAS ugotavlja organ za ugotavljanje skladnosti, ki je opredeljen v 3. členu [3] Uredbe eIDAS.

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

## 8.3. Relacija med inšpektorjem in izdajateljem SIMoD-CA-Root

Inšpektor mora biti neodvisen od infrastrukture javnih ključev na MO.

Organ za ugotavljanje skladnosti ponudnikov kvalificiranih storitev zaupanja z [3] Uredbo eIDAS je neodvisen od infrastrukture javnih ključev na MO.

## 8.4. Področja inšpekcije

Inšpekcijski nadzor preverja skladnost delovanja korenskega izdajatelja SIMoD-CA-Root z veljavno zakonodajo, Politiko SIMoD-PKI in pravili delovanja korenskega izdajatelja SIMoD-CA-Root.

Organ za ugotavljanje skladnosti ugotavlja skladnost ponudnika kvalificiranih storitev zaupanja in kvalificiranih storitev zaupanja z zahtevami [3] Uredbe eIDAS.

Zunanja inšpekcijska služba ali organizacija po pooblastilu Sveta za upravljanje z infrastrukturo javnih ključev na MO preverja samo skladnost delovanja korenskega izdajatelja s Politiko SIMoD-PKI in pravili delovanja korenskega izdajatelja SIMoD-CA-Root.

## 8.5. Postopki po opravljeni inšpekciji

V primeru ugotovljenih nepravilnosti mora korenski izdajatelj SIMoD-CA-Root 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 korenski izdajatelj SIMoD-CA-Root pomanjkljivosti ne odpravi, je Svet za upravljanje z infrastrukturo javnih ključev na MO dolžan ukrepati v okviru naslednjih možnosti:

- opozori na pomanjkljivosti, vendar kljub temu dovoli obratovanje korenskega izdajatelja SIMoD-CA-Root do naslednje predvidene inšpekcije ali
- pred preklicem izdajateljevega digitalnega potrdila dodeli korenskemu izdajatelju SIMoD-CA-Root rok za odpravo pomanjkljivosti, v tem času dovoli delovanje ali
- odredi preklic izdajateljevega digitalnega potrdila.

Nadaljnji postopki po opravljenem pregledu skladnosti ponudnika kvalificiranih storitev zaupanja so v skladu z drugim in tretjim odstavkom 20. člena [3] Uredbe eIDAS.

## 8.6. Prejemniki ugotovitev o inšpekciji

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

Korenski izdajatelj SIMoD-CA-Root se odloči ali je potrebno o ugotovitvah obvestiti podrejene izdajatelje, imetnike digitalnih potrdil in ostale udeležence. Obvestilo imetnikom in ostalim udeležencem objavi v skladu s poglavjem 9.11. Obvestila in komuniciranje z udeleženci.

V skladu s prvim odstavkom 20. člena [3] Uredbe eIDAS mora ponudnik kvalificiranih storitev zaupanja poročilo o ugotovitvi skladnosti predložiti nadzornemu organu, ki je določen v 3. členu **Error! Reference source not found.** Uredbe o izvajanju eIDAS, v treh (3) dneh po njegovem prejemu.

# 9. OSTALE POSLOVNE IN PRAVNE ZADEVE

## 9.1. Cenik

### *9.1.1. Cena prve in ponovne izdaje digitalnega potrdila*

Ni predpisano.

### *9.1.2. Cena dostopa do digitalnega potrdila*

Ni predpisano.

### *9.1.3. Cena dostopa do podatka o statusu in preklicu potrdila*

Ni predpisano.

### *9.1.4. Cene drugih storitev*

Ni predpisano.

### *9.1.5. Povračilo stroškov*

Ni predpisano.

## 9.2. Finančna odgovornost

### *9.2.1. Višina zavarovanja*

Ministrstvo za obrambo ima glede delovanja izdajateljev SIMoD-PKI ustrezno zavarovano svojo odgovornost skladno z veljavno zakonodajo.

### *9.2.2. Druge oblike zavarovanja*

Ni predpisano.

### *9.2.3. Zavarovanje ali jamstva za končne uporabnike*

Ni predpisano.

## 9.3. Zaupnost poslovnih informacij

Ni predpisano.

### *9.3.1. Obseg zaupnih poslovnih informacij*

Ni predpisano.

### *9.3.2. Informacije izven obsega zaupnih poslovnih informacij*

Ni predpisano.

### *9.3.3. Odgovornost za zagotavljanje zaupnosti poslovnih informacij*

Ni predpisano.

## 9.4. Zaupnost osebnih podatkov

### *9.4.1. Načrt zagotavljanja zaupnosti osebnih podatkov*

Varovanje osebnih podatkov je v skladu z veljavno zakonodajo o varstvu osebnih podatkov.

#### *9.4.2. Obseg osebnih podatkov, ki se obravnavajo kot zaupni*

Osebni podatki so določeni v predpisih o varstvu osebnih podatkov.

#### *9.4.3. Osebni podatki, ki se ne obravnavajo kot zaupni*

Osebni podatki so določeni v predpisih o varstvu osebnih podatkov.

#### *9.4.4. Odgovornost glede varovanja osebnih podatkov*

Overitelj na MO je odgovoren za varovanje osebnih podatkov v skladu s predpisi o varstvu osebnih podatkov.

#### *9.4.5. Dovoljenje za uporabo osebnih podatkov*

V skladu s predpisi o varstvu osebnih podatkov.

#### *9.4.6. Posredovanje osebnih podatkov v sodnih in upravnih postopkih*

Osebne podatke se v sodnih in upravnih postopkih posreduje v skladu s predpisi o varstvu osebnih podatkov.

#### *9.4.7. Druge okoliščine posredovanja osebnih podatkov*

Ni predpisano.

### 9.5. Zaščita intelektualne lastnine

MO je lastnik podatkov v digitalnih potrdilih, imenikih in registrih preklicanih potrdil, ki so bili izdani v okviru infrastrukture javnih ključev na MO.

### 9.6. Odgovornosti in jamstva

#### *9.6.1. Odgovornosti in jamstva izdajatelja SIMoD-CA-Root*

Korenski izdajatelj SIMoD-CA-Root jamči, da deluje v skladu s Politiko SIMoD-PKI in svojimi pravili delovanja. Korenskega izdajatelja SIMoD-CA-Root predstavlja in jamči za izpolnjevanje njegovih obveznosti Svet za upravljanje z infrastrukturo javnih ključev na MO.

Svet za upravljanje z infrastrukturo javnih ključev na MO je odgovoren, da izdajatelj SIMoD-CA-Root kot ponudnik storitev zaupanja izpolnjuje zahteve [3] Uredbe eIDAS.

#### *9.6.2. Odgovornosti in jamstva prijavne službe*

Korenski izdajatelj SIMoD-CA-Root nima vzpostavljene prijavne službe.

Svet za upravljanje z infrastrukturo javnih ključev na MO je odgovoren za ustreznost identifikacijskih postopkov in točnost podatkov v okviru delovanja korenskega izdajatelja SIMoD-CA-Root.

#### *9.6.3. Odgovornosti in jamstva imetnikov digitalnih potrdil*

Svet za upravljanje z infrastrukturo javnih ključev na MO odgovarja in jamči za podrejene izdajatelje SIMoD-PKI.

#### *9.6.4. Odgovornost in jamstva tretjih oseb*

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

#### *9.6.5. Odgovornost in jamstva drugih udeležencev*

Ni relevantno.

## 9.7. Zanikanje odgovornosti

Korenski izdajatelj SIMoD-CA-Root ne izdaja digitalnih potrdil imetnikom. Razlogi za zanikanje odgovornosti overitelja na MO v povezavi z imetniškimi digitalnimi potrdili so podani v pravilih delovanja podrejenega izdajatelja.

Korenski izdajatelj SIMoD-CA-Root ni odgovoren za škodo, ki bi lahko nastala zaradi višje sile oziroma nepredvidljive okoliščine, na katero nima vpliva (naravne nesreče, terorizem,…).

## 9.8. Omejitve odgovornosti

Korenski izdajatelja SIMoD-CA-Root ne prevzema jamstva posamezne pravne posle.

## 9.9. Zavarovanje pred škodo zaradi neizpolnjevanja obveznosti

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

## 9.10. Začetek in prenehanje veljavnosti

### *9.10.1. Začetek veljavnosti*

Javna pravila SIMoD-CA-Root začnejo veljati in se uporabljati naslednji dan po podpisu.

### *9.10.2. Prenehanje veljavnosti*

Veljavnost Javnih pravil SIMoD-CA-Root ni časovna omejena. Javna pravila SIMoD-CA-Root veljajo do uveljavitve nove verzije.

### *9.10.3. Posledice prenehanja veljavnosti*

Po prenehanju veljavnosti Javnih pravil SIMoD-CA-Root zaradi objave nove verzije podrejeni izdajatelji praviloma uporabljajo obstoječa digitalna potrdila v skladu s Javnimi pravili SIMoD-CA-Root, po katerih so bila izdana.

## 9.11. Obvestila in komuniciranje z udeleženci

Korenski izdajatelj SIMoD-CA-Root objavlja obvestila na spletni strani: http://www.simod-pki.mors.si.

## 9.12. Spreminjanje dokumenta

### *9.12.1. Postopek uveljavitve spremembe*

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

### *9.12.2. Postopek in roki obveščanja*

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

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

#### *9.12.3. Spremembe, ki zahtevajo novo identifikacijsko oznako politike*

Ni relevantno.

### 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

Korenski izdajatelj SIMoD-CA-Root deluje v skladu z predpisi in priporočili:

| | | |
|---|---|---|
| [1] | ZEPEP | Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 – UPB1, 61/06) |
| [2] | Uredba o izvajanju eIDAS | Uredba o izvajanju Uredbe (EU) o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 199/93/ES (Uradni list RS, št. 46/16) |
| [3] | eIDAS | Uredba (EU) št. 910/2014 Evropskega parlamenta in sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (Uradni list EU, št. L 257/83 z dne 28.8.2014) |
| [4] | ETSI ES 319 401 | v2.1.1 Electronic Signatures and Infrastructures (ESI); General Policy requirements for Trust Service Providers |
| [5] | ETSI EN 319 411 | Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Provider issuing certificates |
| [6] | ETSI EN 319 411-1 | v1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Provider issuing certificates, Part 1: General requirements |
| [7] | ETSI EN 319 411-2 | v2.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Provider issuing certificates, Part 2: Requirements for trust service providers issuing EU qualified certificates |
| [8] | Politika SIMoD-PKI | Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, Verzija 3.0 |
| [9] | RFC 3647 | Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework |
| [10] | RFC 5280 | Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile |
| [11] | RFC 6960 | X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OSCP |

### 9.15. Ostala relevantna zakonodaja

Korenski izdajatelj SIMoD-CA-Root mora pri svojem delovanju upoštevati tudi:

| | | |
|---|---|---|
| [12] | ZObr | Zakon o obrambi (Uradni list RS, št. 103/04 – UPB1, 95/15) |
| [13] | ZTP | Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – UPB2, 9/10, 60/11) |
| [14] | ZVOP-1 | Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – UPB1) |

## 9.16. Razne določbe

Poleg Javnih pravil SIMoD-CA-Root opredeljujejo delovanje korenskega izdajatelja SIMoD-CA-Root še naslednji dokumenti:

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

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

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

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

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

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

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

A.8. Pravila delovanja izdajatelja SIMoD-CA-Root, zaupni del

## 9.17. Ostale določbe

Ni ostalih določb.