REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Pravila delovanja overitelja SIMoD-CA-Root, javni del

(Javna pravila SIMoD-CA-Root)

Ver 2.0

NEURADNO PREČIŠČENO BESEDILO

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

Izdaja:	Spremembe glede na prejšnjo izdajo:
Neuradno prečiščeno besedilo Pravil delovanja overitelja SIMoD-CA-Root, javni del, verzija 2.0.	Združena sta dokumenta Pravila delovanja overitelja SIMoD-CA-Root, javni del, verzija 2.0, številka: 382-5/2006-119 in Pravila o spremembah Pravil delovanja overitelja SIMoD-CA-Root, javni del, verzija 2.0, številka: 386-6/2011-337.
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, • 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

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

PRAVILA DELOVANJA OVERITELJA SIMoD-CA-Root, JAVNI DEL

(JAVNA PRAVILA SIMoD-CA-Root)

Verzija 2.0

1. UVOD

1.1. Pregled

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

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

Overitelj SIMoD-CA-Root deluje v okviru SIMOD-PKI, katere delovanje predpisuje [3] Politika SIMoD-PKI. [3] Politika SIMoD-PKI predpisuje splošne zahteve za digitalna potrdila, minimalne zahteve za tehnične lastnosti in raven varnosti infrastrukture overiteljev, postopke za upravljanje z digitalnimi potrdili, obveznosti in odgovornosti, ki jih morajo izpolnjevati overitelji, imetniki in tretje osebe, ki se zanašajo na digitalna potrdila, ter drugi overitelji, ki se želijo povezovati z infrastrukturo javnih ključev na MO.

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

Pravila delovanja overitelja SIMoD-CA-Root, javni del, podajajo opis overiteljeve infrastrukture, postopkov overitelja 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 overitelju, morajo poleg pričujočega dokumenta upoštevati še določila Politike SIMoD-PKI ter javnih pravil delovanja podrejenih overiteljev.

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

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

Dokument je skladen z [4] RFC 3647 in predstavlja pravila delovanja overitelja (ang. Certification Practices Statement, CPS) v odnosu na Politiko SIMoD-PKI, ki predstavlja politiko delovanja (ang. Certificate Policy, CP).

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

1.2. Identifikacijske oznake politik delovanja

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

1.3. Udeleženci infrastrukture javnih ključev

1.3.1. Overitelj SIMoD-CA-Root

Overitelj SIMoD-CA-Root je korenski overitelj SIMoD-PKI.

Overitelj SIMoD-CA-Root sestavlja strojna in programska oprema ter operativno osebje. Overitelj 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 overitelja SIMoD-CA-Root in ima v zvezi z njim naslednje obveznosti:

- nadzira izdelavo, vodi postopek potrditve, ocenjuje predlagane spremembe, predlaga uveljavitve sprememb in načrtuje postopek uveljavitve sprememb Pravil delovanja overitelja SIMoD-CA-Root, javnega in zaupnega dela,
- ocenjuje in potrjuje skladnost Pravil delovanja overitelja SIMoD-CA-Root, javnega in zaupnega dela, s Politiko SIMoD-PKI,
- sprejema Pravila delovanja overitelja SIMoD-CA-Root, javni in zaupni del,
- imenuje operativno osebje overitelja 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 overiteljevega potrdila in
- ocenjuje ustreznost politik drugih overiteljev v postopku medsebojnega priznavanja ter usmerja postopke in ukrepe formalnega medsebojnega priznavanja z drugimi overitelji.

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

1.3.1.2. Operativno osebje overitelja SIMoD-CA-Root

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

1.3.2. Prijavna služba

Overitelj SIMoD-CA-Root nima vzpostavljene prijavne službe.

1.3.3. Imetniki digitalnih potrdil

Overitelj SIMoD-CA-Root izdaja digitalna potrdila podrejenim overiteljem in medsebojno priznanim overiteljem ter operativnemu osebju, izključno za potrebe upravljanja z overiteljevo 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 overitelja SIMoD-CA-Root.

Tretje osebe so:

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

1.3.5. Posredno odgovorni organi

Overitelj 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

Overitelj SIMoD-CA-Root kot korenski overitelj SIMoD-PKI izdaja digitalna potrdila podrejenim overiteljem in medsebojno priznanim overiteljem.

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

1.4.1. Dovoljena uporaba digitalnih potrdil

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

1.4.2. Nedovoljena uporaba digitalnih potrdil

Ni relevantno.

1.5. Upravljanje s Pravili delovanja SIMoD-CA-Root

1.5.1. Organ, ki upravlja s tem dokumentom

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

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

1.5.2. Kontaktna oseba

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

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

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

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

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

- skladnost Pravil delovanja overitelja SIMoD-CA-Root, javnega in zaupnega dela, z zahtevami Politike SIMoD-PKI ter
- skladnost infrastrukture in postopkov overitelja SIMoD-CA-Root glede na določila Politike SIMoD-PKI ter javni in zaupni del Pravil delovanja overitelja SIMoD-CA-Root.

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.
Digitalno potrdilo za preverjanje podpisa	Digitalno potrdilo, ki se uporablja za verifikacijo digitalnega podpisa, preverjanje istovetnosti uporabnikov in preverjanje celovitosti podatkov v elektronski obliki.
Digitalno potrdilo za šifriranje	Digitalno potrdilo, ki se uporablja za izmenjavo simetričnih šifrirnih ključev pri zagotavljanju tajnosti podatkov v elektronski obliki.
Elektronski podpis	Niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika.
Elektronsko sporočilo	Niz podatkov, ki so poslani ali prejeti na elektronski način, kar vključuje predvsem elektronsko izmenjavo podatkov in elektronsko pošto.
Imenik	Podatkovna struktura, ki vsebuje objekte z določenimi lastnosti in pripadajočimi vrednostmi. Imenik, ki vsebuje digitalna potrdila je običajno v skladu s standardom X.500 oziroma razširjenim standardom X.509 ver.3.
Imetnik potrdila	Fizična oseba, navedena v digitalnem potrdilu v polju »Subject« kot lastnik zasebnega ključa, ki ustreza javnemu ključu, vsebovanem v digitalnem potrdilu oziroma odgovorna oseba za uporabo digitalnega potrdila.
Informacijski sistem	Skupek naprav in postopkov, ki omogočajo obdelavo informacij oziroma nudijo informacijske storitve. Združuje računalniško strojno in programsko opremo, računalniške nosilce podatkov, podatkovne zbirke in druge naprave ter identifikacijske, avtorizacijske, upravljavske in nadzorne postopke v funkcionalno celoto.
Javni ključ	Ključ iz para ključev, ki je lahko javno objavljen.
Javni komunikacijsko informacijski sistem	Je komunikacijsko informacijski sistem, katerega storitve so namenjene javni uporabi.
Komunikacijski sistem	Skupek naprav in postopkov, ki omogočajo prenos informacij. Primeri takih sistemov so telekomunikacijski sistemi in računalniška omrežja.
Komunikacijsko informacijski sistem	Skupen izraz za komunikacijski in informacijski sistem.
Kvalificirano digitalno potrdilo	Digitalno potrdilo, ki izpolnjuje zahteve iz 28. člena ZEPEP. Izda ga overitelj, ki deluje v skladu z zahtevami iz 28. do 36. člena ZEPEP.
Naročnik potrdila	Fizična ali pravna oseba, ki z zahtevkom zaprosi za izdajo digitalnega potrdila.
Oprema za elektronsko podpisovanje	Strojna ali programska oprema ali njune specifične sestavine, ki jo overitelj uporablja za storitve v zvezi z elektronskim podpisovanjem ali ki se uporabljajo za oblikovanje ali preverjanje elektronskih podpisov.
Overitelj digitalnih potrdil	Fizična ali pravna oseba, ki izdaja digitalna potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi.
Par ključev	Par asimetričnih kriptografskih ključev, ki ga sestavljata zasebni in javni ključ.
Podatki v elektronski obliki	Podatki, ki so oblikovani, shranjeni, poslani, prejeti ali izmenljivi na elektronski način.
Podatki za elektronsko podpisovanje	Edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa.
Podatki za preverjanje elektronskega podpisa	Edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa.

Podpisnik	Oseba, ki ustvari ali je v njenem imenu in v skladu z njeno voljo ustvarjen elektronski podpis.
Pošiljatelj elektronskega sporočila	Oseba, ki je sama poslala elektronsko sporočilo ali pa je bilo sporočilo poslano v njenem imenu in v skladu z njeno voljo; posrednik elektronskega sporočila se ne šteje za pošiljatelja tega elektronskega sporočila.
Prejemnik elektronskega sporočila	Oseba, ki je prejela elektronsko sporočilo; posrednik elektronskega sporočila se ne šteje za prejemnika tega elektronskega sporočila.
Prijavna služba	Služba oziroma organizacija, ki po pooblastilu overitelja sprejema zahtevke in preverja istovetnosti bodočih imetnikov.
Sredstvo za elektronsko podpisovanje	Nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa.
Sredstvo za varno elektronsko podpisovanje	Sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve iz 37. člena ZEPEP.
Šifrirni (kriptografski) ključ	Niz znakov uporabljen za kriptografsko preoblikovanje (npr. šifriranje, dešifriranje, podpisovanje, ali preverjanje podpisa).
Tajni podatek	Dejstvo ali sredstvo iz delovnega področja organa, ki se nanaša na javno varnost, obrambne zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov določenih v ZTP zaščititi pred nepoklicanimi osebami, in ki je v skladu s ZTP določeno in označeno kot tajno.
Tretja oseba	Subjekt, ki ni aktivno udeležen v storitev, vendar zaupa izvajalcu in rezultatu storitve.
Uporabnik	Naročnik ali imetnik digitalnega potrdila.
Varen elektronski podpis	Je elektronski podpis, ki izpolnjuje naslednje zahteve: • povezan je izključno s podpisnikom, • iz njega je mogoče zanesljivo ugotoviti podpisnika, • ustvarjen je s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom, • povezan je s podatki, na katere se nanaša, tako, da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi.
Zasebni komunikacijsko informacijski sistem	Je komunikacijsko informacijski sistem, ki ni javen in je v lasti, upravljanju in pod nadzorom neke privatne, vladne ali nevladne organizacije.
Zasebni ključ	Ključ iz para ključev, ki mora ostati skriven, da se zagotovi zaupnost in celovitost podatkov v elektronski obliki.
Zloraba	Je razkritje tajnega podatka, izguba celovitosti ali razpoložljivosti podatka.

Kratica	Opis
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).
ARL	Register preklicanih overiteljev (ang. Authority Revocation List).
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).
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).
PKCS	Priporočila podjetja RSA Security za uporabo asimetričnih kriptografskih algoritmov (ang. Public Key Cryptographic Standards).
PKCS#1	Osnovna pravila za formatiranje podatkov ob implementaciji RSA funkcij. Predpisuje, kako se izračuna digitalni podpis, kako se formatirajo podatki, ki se podpisujejo in format podpisa. Predpisuje tudi sintakso javnega in zasebnega RSA ključa.
PKCS#10	Sintaksa zahtevka za digitalno potrdilo. Zahtevek za digitalno potrdilo vsebuje razločevalno ime, javni ključ in nabor drugih atributov, ki jih podpiše subjekt, ki zahteva potrditev. Daljše ime: PKCS#10 Certification Request Syntax Standard.
PKCS#7	Sintaksa za kriptografsko obdelane podatke, kot digitalni podpisi in digitalne ovojnice.
PKI	Infrastruktura javnih ključev; strojna in programska oprema ter varnostni mehanizmi za zaupanja vredno implementacijo varnostnih storitev, ki temeljijo na nesimetrični kriptografiji (ang. Public Key Infrastructure).
PKIX	Delovna skupina za področje infrastrukture javnih ključev v okviru IETF(ang. Internet Engineering Task Force). Izdala serijo priporočil za digitalna potrdila in registre preklicanih potrdil (ang. Public Key Infrastrukture X.509).
PKIX-CMP	Postopek izmenjave podatkov, ki se nanašajo na digitalna potrdila med subjekti infrastrukture overitelja (ang. PKIX Certificate Management Protocol). Vključuje PKCS#7 in PKCS#10.
RFC	Priporočila, ki jih izdaja IETF.
RFC 4210	Priporočilo, ki določa postopke za izmenjavo podatkov, ki se nanašajo na digitalna potrdila. Vsebuje PKIX-CMP.
RFC 3647	Priporočilo, ki določa elemente, ki naj bodo zajeti v politiki overitelja (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework). veljavno od novembra 2003 (je nadomestil RFC 2527).
RFC 3280	Priporočilo, ki določa elemente potrdil in registra preklicanih potrdil.
RSA	Eden prvih nesimetričnih kriptografskih sistemov, patentiran leta 1983, imenovan po odkriteljih: Rivest, Shamir in Adelman.
SIMoD-PKI	Infrastruktura javnih ključev Ministrstva za obrambo Republike Slovenije (ang. **S**loveni**i**an **M**inistry **o**f **D**efence **P**ublic **K**ey **I**nfrastructure - SIMoD-PKI)
X.501	Standard organizacij ITU-T in ISO, ki definira poimenovanje objektov v imeniku. Tudi del serije PKIX Part1.
X.509	Standard organizacij ITU-T in ISO, ki definira strukturo digitalnih potrdil. Eden izmed serije standardov ITU-ISO s področja imenikov. Tudi del RFC 3280.

2. ODGOVORNOST ZA OBJAVE IN IMENIK

2.1. Objave dokumentov in imenik

Informacije o overitelju SIMoD-CA-Root in njegovih digitalnih potrdilih se objavljajo v imenikih in na spletni strani.

Lokalni imenik overitelja SIMoD-CA-Root vsebuje:

- digitalna potrdila podrejenih overiteljev,
- register preklicanih potrdil (ang. Certificate Revocation List, CRL) in
- register preklicanih overiteljev (ang. Authority Revocation List, ARL).

Primarni in zrcalni imenik infrastrukture javnih ključev na MO vsebujeta kopije podatkov iz lokalnega imenika LDAP-Root. Zrcalni imenik ima tudi dodatni naslov (ang. alias) imenik.simod-pki.mors.si.

Digitalna potrdila in register preklicanih potrdil se kopirajo tudi v druge imenike v KIS MO in SV.

Na primarnem spletnem strežniku v internem KIS MO in SV na spletni strani http://www.simod-pki.mors.si se poleg drugih informacij o delovanju SIMoD-PKI objavlja:

- digitalno potrdilo overitelja SIMoD-CA-Root,
- register preklicanih potrdil overitelja SIMoD-CA-Root in
- Javna pravila SIMoD-CA-Root.

Zrcalni spletni strežnik v javnem internet omrežju vsebuje kopijo podatkov iz primarnega spletnega strežnika.

2.2. Objave informacij o digitalnih potrdilih

Digitalna potrdila podrejenih overiteljev so objavljena v imenikih v vozliščih cn=*Overitelj*,ou=simod-pki,o=mors,c=si, kjer je *Overitelj* oznaka overitelja (simod-ca-root, simod-ca-restricted, simod-ca-secret), in sicer v atributu cACertificate.

Digitalna potrdila podrejenih overiteljev so na primarnem in zrcalnem spletnem strežniku objavljena na naslovih http://www.simod-pki.mors.si/certs/*overitelj*.cacert, kjer je *overitelj* oznaka overitelja (simod-ca-root, simod-ca-restricted, simod-ca-secret).

Register preklicanih potrdil overitelja SIMoD-CA-Root je v imenikih 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.

Register preklicanih potrdil overitelja SIMoD-CA-Root je na primarnem in zrcalnem spletnem strežniku objavljen na naslovu http://www.simod-pki.mors.si/crl/simod-ca-root.crl.

Register preklicanih overiteljev (ARL) je v imenikih objavljen v vozlišču cn=CRL1,cn=simod-ca-root,ou=simod-pki, o=mors,c=si v atributu authorityRevocationList.

2.3. Čas in pogostost objav

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

2.4. Dostop do podatkov v imeniku in na spletni strani

Dostop do podatkov v lokalnem imeniku LDAP-Root in primarnem imeniku infrastrukture javnih ključev na MO je dovoljen samo ustreznemu overitelju in upravljavcem imenika.

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

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

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

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

Overitelj SIMoD-CA-Root zagotovi dokument Pravila delovanja overitelja SIMoD-CA-Root, zaupni del, in dopolnjujoča navodila in postopkovnike, če je to potrebno zaradi nadzora, akreditacije ali medsebojnega povezovanja, ob pogojih, ki jih določa [7] ZTP.

3. PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI

3.1. Določanje imen

3.1.1. Vrste imen

Vsako izdano X.509v3 digitalno potrdilo vsebuje polje *Subject* z edinstvenim razločevalnim imenom - X.501 DN (ang. Distinguished Name, DN) v skladu z RFC 3280. Razločevalno ime je v digitalno potrdilo zapisano v obliki X.501 UTF8String in ni nikdar prazno. Digitalna potrdila podrejenih overiteljev, imajo lahko tudi alternativno ime overitelja, ki je zapisano v razširitvenem polju *subjectAltName*, v skladu z RFC 3280.

3.1.2. Potreba po smiselnosti imen

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

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

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

3.1.3. Anonimnost imetnikov in uporaba psevdonimov

Uporaba psevdonimov ni dovoljena. Overitelj 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 overitelja.

3.1.6. Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk

Uporaba zaščitenih znamk v imenih je dovoljena samo nosilcem zaščitenih znamk. SIMoD-CA-Root ne sme zavestno izdati digitalnega potrdila z imenom, ki vsebuje zaščiteno znamko naročniku, ki ni nosilec zaščitene znamke. Operativno osebje overitelja SIMoD-CA-Root ni dolžno preverjati pravic do uporabe zaščitenih znamk, niti razčiščevati sporov glede zaščitenih znamk.

Prosilcem ni dovoljeno zahtevati imen, ki bi kršila intelektualne ali avtorske pravice drugih, čeprav se v okviru SIMoD-PKI tega ne preverja niti ne bo Svet za upravljanje z infrastrukturo javnih ključev na MO ali SIMoD-CA-Root posredoval v takšnih sporih. Svet za upravljanje z infrastrukturo javnih ključev na MO in operativno osebje SIMoD-CA-Root overitelja si pridržujejo pravico zavrniti izdajo digitalnega potrdila ali preklicati izdana digitalna potrdila udeležencev spora.

3.2. Preverjanje istovetnosti imetnikov ob prvi registraciji

3.2.1. Metode dokazovanja lastništva zasebnega ključa

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

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

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

3.2.2. Preverjanje istovetnosti za imetnike, ki niso fizične osebe

Za pravilnost podatkov o bodočem podrejenem overitelju jamči odgovorna oseba bodočega podrejenega overitelja, ki je praviloma vodja organizacijske enote MO, ki bo upravljala s podrejenim overiteljem, s podpisom na zahtevku za pridobitev digitalnega potrdila. Istovetnost podrejenega overitelja oziroma pristnost podatkov v zahtevku preverja Svet za upravljanje z infrastrukturo javnih ključev na MO v okviru obravnavanja zahtevka za izdajo digitalnega potrdila.

3.2.3. Preverjanje istovetnosti za fizične osebe

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

Zahtevek za pridobitev digitalnega potrdila za operativno osebje overitelja SIMoD-CA-Root izpolnita in podpišeta bodoča operativna oseba overitelja in vodja Sveta za upravljanje z infrastrukturo javnih ključev na MO.

Prijavna služba preveri pristnost podatkov bodoče operativne osebe v kadrovski evidenci in izvede osebno identifikacijo na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list ali vozniško dovoljenje).

3.2.4. Podatki o naročniku, ki se ne preverjajo

Ni relevantno.

3.2.5. Preverjanje pooblastil

Vodja organizacijske enote MO s podpisom na zahtevku za pridobitev digitalnega potrdila za podrejenega overitelja jamči, da želi digitalno potrdilo za podrejenega overitelja, ki bo deloval v okviru njegove organizacijske enote.

Vodja Sveta za upravljanje z infrastrukturo javnih ključev na MO s podpisom na zahtevku za pridobitev digitalnega potrdila za operativno osebo overitelja SIMoD-CA-Root jamči, da želi za to osebo, da le-ta pridobi digitalno potrdilo za opravljanje nalog operativne osebe.

3.2.6. Merila za medsebojno povezovanje

Medsebojno povezovanje je mogoče samo na nivoju korenskega overitelja SIMoD-CA-Root. Način in pogoji medsebojnega povezovanja bodo določeni s pogodbo o medsebojnem zaupanju overiteljev. Pogodba o medsebojnem zaupanju overiteljev je obvezna za vse možne načine medsebojnega povezovanja.

Minimalni pogoji za medsebojno povezovanje:

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

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 SIMoD-CA-Root po protokolu PKIX-CMP, imetnik izkaže svojo istovetnost s posedovanjem še veljavnega zasebnega ključa.

Rutinska ponovna izdaja digitalnega potrdila podrejenemu overitelju 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

Operativna oseba overitelja SIMoD-CA-Root, ki želi preklicati digitalno potrdilo, se lahko identificira:

- z digitalno podpisanim zahtevkom za preklic digitalnega potrdila,
- z oddajo pisnega zahtevka za preklic digitalnega potrdila, pri čemer je postopek preverjanja istovetnosti enak kot pri prvi registraciji v skladu s poglavjem 3.2.3 Preverjanje istovetnosti za fizične osebe ali
- s skrivnim geslom, ki ga je izbral ob oddaji zahtevka za izdajo digitalnega potrdila.

Oseba, ki želi preklicati digitalno potrdilo podrejenega overitelja ali medsebojno priznanega overitelja, se mora identificirati po enakem postopku kot pri prvi registraciji v skladu s poglavjem 3.2.2 Preverjanje istovetnosti za imetnike, ki niso fizične osebe.

4. UPRAVLJANJE Z DIGITALNIMI POTRDILI

4.1. Pridobitev digitalnega potrdila

4.1.1. Kdo lahko zaprosi za izdajo digitalnega potrdila

Zahtevek za pridobitev digitalnega potrdila podrejenega overitelja odda predvideni prvi administrator ali prvi varnostni inženir podrejenega overitelja.

Zahtevek za pridobitev digitalnega potrdila operativnega osebja overitelja SIMoD-CA-Root oddajo operativna oseba po tem, ko jo je za opravljanje funkcije pooblastil Svet za upravljanje z infrastrukturo javnih ključev na MO.

4.1.2. Postopek bodočega imetnika za pridobitev digitalnega potrdila in odgovornosti

Zahtevek za pridobitev digitalnega potrdila podrejenega overitelja mora vsebovati:

- naziv organizacijske enote MO, ki bo upravljala s podrejenim overiteljem,
- ime odgovorne osebe, ki je praviloma vodja organizacijske enote MO, ki bo upravljala s podrejenim overiteljem,
- ime prvega administratorja ali prvega varnostnega inženirja podrejenega overitelja ali druge osebe, ki bo v postopku izdaje digitalnega potrdila predala overitelju SIMoD-CA-Root zahtevek z javnim ključem, za katerega se izdaja digitalno potrdilo,
- predlog za razločevalno ime podrejenega overitelja, če ni razvidno iz javnega dela pravil delovanja overitelja,
- predlog alternativnega imena digitalnega potrdila (po potrebi),
- obrazložitev oziroma utemeljitev prošnje in
- javni del pravil delovanja podrejenega overitelja.

Zahtevek se pošlje Svetu za upravljanje z infrastrukturo javnih ključev na MO.

4.2. Obdelava zahtevka za izdajo digitalnega potrdila

4.2.1. Preverjanje istovetnosti bodočega podrejenega overitelja

Istovetnost bodočega podrejenega overitelja se preverja skladno s poglavjem 3.2.2 Preverjanje istovetnosti za imetnike, ki niso fizične osebe.

4.2.2. Odobritev ali zavrnitev izdaje digitalnega potrdila

Zahtevek za pridobitev digitalnega potrdila Sveta za upravljanje z infrastrukturo MO ne obvezuje k odobritvi izdaje digitalnega potrdila.

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

- kopijo ali vpogled v zaupni del pravil delovanja overitelja,
- poročilo o varnostnem pregledu infrastrukture.

Obvestilo o zavrnitvi ali odobritvi izdaje digitalnega potrdila pošlje Svet za upravljanje z infrastrukturo javnih ključev na MO prosilcu v pisni obliki.

Svet za upravljanje z infrastrukturo javnih ključev na MO po odobritvi izda operativnemu osebju SIMoD-CA-Root nalog za izdajo digitalnega potrdila podrejenemu overitelju. Nalog vsebuje vse podatke iz zahtevka za pridobitev digitalnega potrdila.

4.2.3. Čas za obdelavo zahtevka za izdajo digitalnega potrdila

Največji dopusten čas od sprejema zahtevka za pridobitev digitalnega potrdila in izdajo obvestila o odobritvi ali zavrnitvi je enaindvajset (21) dni.

4.3. Izdaja digitalnega potrdila

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

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

- preveri istovetnost osebe, ki v postopku izdaje digitalnega potrdila preda overitelju 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 vsaj dveh dokumentov, od katerih je eden uradni osebni dokument s sliko in drugi službena izkaznica MO,
- preveri integriteto PKCS#10 zahtevka za izdajo digitalnega potrdila,
- preveri podatke o podrejenem overitelju, 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 overitelji sami generirajo zasebne ključe.

4.3.1.2. Dostava overiteljevega javnega ključa imetniku

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

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

4.3.2. Obvestilo naročnikom o izdaji digitalnega potrdila

Overitelj SIMoD-CA-Root o odobritvi izdaje obvesti kontaktno osebo, navedeno v javnih pravilih delovanja overitelja, ali odgovorno osebo iz prošnje za izdajo digitalnega potrdila.

4.4. Prevzem digitalnega potrdila

4.4.1. Postopek potrditve prevzema digitalnega potrdila

Podrejeni overitelj je dolžan preveriti istovetnost izdanega digitalnega potrdila na osnovi digitalnega potrdila overitelja SIMoD-CA-Root kot tudi vsebino digitalnega potrdila. S prvo uporabo, oziroma če podrejeni overitelj (tri) 3 dni od prevzema digitalnega potrdila overitelja 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 overitelj 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 overiteljev

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

- digitalnih potrdil podrejenim overiteljem,
- digitalnih potrdil medsebojno priznanih overiteljev,
- registrov preklicanih overiteljev in registrov preklicanih potrdil ter
- digitalnih potrdil operativnega osebja overitelja SIMoD-CA-Root.

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

4.5.1.2. Zasebni ključi in digitalna potrdila prijavne službe

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

4.5.1.3. Uporabniški zasebni ključi in digitalna potrdila

Ni relevantno. Overitelj 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 overitelja 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 overiteljev.

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[1] digitalnih potrdil

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

4.7.1. Razlogi za ponovno izdajo digitalnega potrdila

Ponovna izdaja digitalnih potrdil overitelja SIMoD-CA-Root oziroma podrejenih overiteljev se praviloma izvede pred pretekom njihove veljavnosti.

4.7.2. Kdo lahko zahteva ponovno izdajo digitalnega potrdila

Digitalno potrdilo se ponovno izda obstoječemu overitelju.

[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 overitelju SIMoD-CA-Root ali podrejenemu overitelju pred pretekom veljavnosti v splošnem ni potreben zahtevek. O potrebi po ponovni izdaji digitalnega potrdila operativno osebje ustreznega overitelja pravočasno obvesti Svet za upravljane z infrastrukturo javnih ključev na MO.

Postopek na osnovi naloga Sveta za upravljanja z infrastrukturo javnih ključev na MO izvede operativno osebje overiteljev 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 overitelja.

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 overitelja SIMoD-CA-Root

Razlogi za preklic digitalnega potrdila korenskega overitelja 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 overitelja SIMoD-CA-Root.

4.9.1.3. Okoliščine preklica digitalnega potrdila o priznavanju drugega overitelja

Korenski overitelj SIMoD-CA-Root prekliče digitalno potrdilo o priznavanju drugega overitelja iz naslednjih razlogov:

- dejanska ali domnevna zloraba zasebnih ključev drugega overitelja,
- spremembe podatkov o drugem overitelju, tako da je potrebno izdati novo digitalno potrdilo o priznavanju drugega overitelja,
- preklic digitalnega potrdila drugega overitelja,
- 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 overitelja

Razlogi za preklic digitalnega potrdila podrejenega overitelja so:

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

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 overitelja SIMoD-CA-Root

Preklic digitalnega potrdila korenskega overitelja 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 overitelja

Preklic digitalnega potrdila o priznavanju drugega overitelja zahteva:

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

4.9.2.4. Kdo lahko zahteva preklic digitalnega potrdila podrejenega overitelja

Preklic digitalnega potrdila overitelja lahko zahteva:

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

4.9.3. Postopki za preklic

4.9.3.1. Postopki preklica digitalnih potrdil imetnikov

Ni relevantno.

4.9.3.2. Postopki preklica digitalnega potrdila overitelja SIMoD-CA-Root

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

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

- preklicati vsa digitalna potrdila,
- zagotavljati razpoložljivost registrov preklicanih overiteljev vsaj še devetdeset (90) dni od preklica svojega digitalnega potrdila,
- objaviti preklic digitalnega potrdila v registru preklicanih overiteljev,
- 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 overiteljem nova digitalna potrdila.

4.9.3.3. Postopki preklica digitalnega potrdila o priznavanju drugega overitelja

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

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

Preklicano digitalno potrdilo mora bit objavljeno v registru preklicanih overiteljev.

4.9.3.4. Postopki preklica digitalnega potrdila podrejenega overitelja

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

Podrejeni overitelj 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 overitelj SIMoD-CA-Root mora ob preklicu digitalnega potrdila podrejenega overitelja izvesti naslednje postopke:

- preklicano digitalno potrdilo objaviti v registru preklicanih overiteljev,
- javno objaviti obvestilo o preklicu potrdila podrejenega overitelja 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 overitelja SIMoD-CA-Root

Korenski overitelj 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 overitelja

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

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

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

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 overitelja

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

4.9.6. Obveza preverjanja registra preklicanih potrdil

Tretje osebe, ki se zanašajo na digitalno potrdilo, so pred uporabo dolžne preveriti najnovejši register preklicanih potrdil. Kot del postopka preverjanja je potrebno preveriti tudi veljavnost in verodostojnost registra preklicanih potrdil. Tretja oseba mora za vsako uporabljeno digitalno potrdilo izvesti popoln postopek preverjanja poti zaupanja v skladu z [5] RFC 3280.

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

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

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

Infrastruktura javnih ključev na MO zagotavlja varnostne mehanizme ob predpostavki rednega preverjanja veljavnosti digitalnih potrdil. Aplikacija oziroma informacijska rešitev, ki uporablja varnostne mehanizme infrastrukture javnih ključev na MO, mora odstopanje od dolžnosti uporabe preverjenih digitalnih potrdil jasno navesti v svojih pravilih delovanja.

4.9.7. Pogostost objav registrov preklicanih potrdil

Overitelj SIMoD-CA-Root objavlja nov register preklicanih potrdil in register preklicanih overiteljev 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 do njegove objave je največ sto dvajset (120) minut.

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

4.9.9. Storitev sprotnega preverjanje statusa digitalnih potrdil

Storitev sprotnega preverjanja statusa digitalnih potrdil (ang. On-line Certificate Status Protocol, OCSP) ni na voljo.

4.9.10. Obveza sprotnega preverjanja statusa preklicanih potrdil

Ni relevantno.

4.9.11. Ostale oblike objavljanja preklicanih digitalnih potrdil

Ni relevantno.

4.9.12. Posebne zahteve glede zlorabe ključa

Ni predpisano.

4.9.13. Okoliščine za začasno ukinitev veljavnosti

Ni podprto.

4.9.14. Kdo lahko zahteva začasno ukinitev veljavnosti

Ni relevantno.

4.9.15. Postopki za začasno ukinitev veljavnosti

Ni relevantno.

4.9.16. Omejitve obdobja začasne ukinitve veljavnosti

Ni relevantno.

4.10. Storitve objavljanja statusa digitalnih potrdil

4.10.1. Tehnične lastnosti storitve

Storitve preverjanja statusa digitalnih potrdil niso implementirane. Možno je samo preverjanje veljavnosti digitalnih potrdil v registrih preklicanih potrdil.

4.10.2. Razpoložljivost storitve

Ni relevantno.

4.10.3. Dodatne možnosti

Ni relevantno.

4.11. Predčasna prekinitev veljavnosti digitalnih potrdil

Razlog za predčasno prekinitev veljavnosti digitalnega potrdila podrejenega overitelja 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.

Overitelj 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. Overitelj SIMoD-CA-Root ne izdaja digitalnih potrdil za šifriranje.

4.12.2. Odkrivanje kopije ključev za dešifriranje

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

4.12.3. Zaščita odkritega zasebnega ključa in postopek prenosa

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

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

5.1. Fizično varovanje

5.1.1. Lokacija in konstrukcija prostorov ter fizični dostop

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

Informacijska oprema overitelja SIMoD-CA-Root je nameščena na varni lokaciji v prostorih varnostnega območja II. stopnje.

5.1.2. Fizični dostop

Nadzor fizičnega dostopa izvaja pristojna služba MO.

Nadzor nad vstopom se izvaja z uporabo tehničnih sredstev, ki preprečujejo nepooblaščen vstop. Vstop v prostore je video nadzorovan. O vstopih in izstopih v prostore se vodi evidenca.

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

- da je overitelj SIMoD-CA-Root ugasnjen,
- da so varnostne omare pravilno zaklenjene,
- da so morebitni zapisi podatkov (npr. izpisi iz tiskalnika) primerno hranjeni, odvečno gradivo pa uničeno in
- da so varnostni mehanizmi varovanja vklopljeni in delujejo.

5.1.3. Napajanje in klimatske naprave

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

5.1.4. Zaščita pred poplavo

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

5.1.5. Zaščita pred ognjem

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

5.1.6. Shranjevanje medijev

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

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

5.1.7. Odstranjevanje odpadkov

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

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

5.1.8. Hranjenje na oddaljeni lokaciji

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

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

5.2. Organizacijski varnostni ukrepi

5.2.1. Organizacija upravljanja overitelja SIMoD-CA-Root

5.2.1.1. Operativno osebje

Naloge upravljanja z overiteljem SIMoD-CA-Root so porazdeljene med operativno osebje tako, da je zagotovljena ločitev med zaključenimi vsebinskimi področji upravljanja. Operativno osebje overitelja SIMoD-CA-Root je glede na vsebinska področja upravljanja razdeljeno na zaključeni organizacijski skupini:

- upravljanje z digitalnimi potrdili in
- upravljanje s programsko in strojno opremo overitelja SIMoD-CA-Root.

Operativni osebi overitelja SIMoD-CA-Root je dovoljeno opravljanje nalog samo znotraj ene zaključene organizacijske skupine. Oseba, ki izvaja naloge v okviru operativnega osebja overitelja SIMoD-CA-Root, lahko opravlja naloge tudi za druge overitelje SIMoD-PKI, pri čemer mora biti pri vsakem overitelju član natanko ene organizacijske skupine.

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

- prvi varnostni inženir in
- drugi varnostni inženirji.

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

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

V vsaki organizacijski skupini za upravljane z digitalnimi potrdili so najmanj tri (3) osebe, v organizacijski skupini za upravljane s programsko in strojno opremo overiteljev sta najmanj dve osebi (2).

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

5.2.1.2. Prijavna služba

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

5.2.1.3. Druge funkcije

Pristojne organizacijske enote v MO skrbijo za:

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

5.2.2. Število oseb, potrebnih za izvedbo postopkov

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

- generiranje kriptografskih ključev overitelja SIMoD-CA-Root,
- preklic overiteljevega potrdila,
- spreminjanje gesel aplikacije za delo z overiteljem SIMoD-CA-Root,
- ponovno šifriranje overiteljeve baze podatkov,
- nastavitev števila potrebnih prisotnih varnostnih inženirjev za izvedbo kritičnih operacij pri upravljanju s potrdili,
- restavriranje prijavnih imen varnostnih inženirjev,

- spreminjanje nastavitve zgoščevalnih algoritmov,
- spreminjanje nastavitev kriptografskih algoritmov,
- aktiviranje avtomatskega zagona overiteljevih servisov in
- ukinitev obvezne prisotnosti vsaj dveh oseb za izvedbo zgoraj navedenih operacij.

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

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

5.2.3. Preverjanje istovetnosti operativnega osebja

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

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

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

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

5.3. Zahteve za osebje overitelja SIMoD-CA-Root

5.3.1. Kvalifikacije, izkušnje in varnostno preverjanje

Operativno osebje overitelja SIMoD-CA-Root:

- mora biti ustrezno usposobljeno in o tem imeti dokazila,
- mora imeti za opravljanje nalog pri overitelju SIMoD-CA-Root imenovanje Sveta za upravljanje z infrastrukturo javnih ključev na MO,
- ne sme opravljati drugih nalog, ki bi bile v nasprotju z opravljanjem nalog pri overitelju 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 [7] ZTP.

5.3.3. Usposabljanje osebja

5.3.3.1. Usposabljanje osebja overitelja SIMoD-CA-Root

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

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

5.3.3.2. Usposabljanje osebja za pomoč uporabnikom

Ni relevantno.

5.3.4. Pogostost dodatnih usposabljanj

Osebje mora pridobiti potrebna znanja pred vsako nadgradnjo.

5.3.5. Kroženje med delovnimi mesti

Ni predpisano.

5.3.6. Ukrepi ob kršitvah pooblastil

Proti operativni osebi, 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 [7] ZTP oziroma implementacijo pravil na lokacijah overitelja.

5.3.8. Dokumentacija za osebje overitelja SIMoD-CA-Root

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

5.4. Postopki varnostnih pregledov sistema

5.4.1. Vrste beleženih dogodkov

Overitelj SIMoD-CA-Root beleži dogodke:

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

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

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

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

5.4.2. Pogostost pregleda dnevnikov beleženih dogodkov

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

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

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

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

5.4.3. Obdobje hranjenja dnevnikov beleženih dogodkov

Overitelj SIMoD-CA-Root hrani dnevnike beleženih dogodkov na sistemu najmanj do naslednjega rednega pregleda in najmanj pet (5) let v arhivu.

5.4.4. Zaščita dnevnikov beleženih dogodkov

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

Dostop do dnevnikov beleženih dogodkov je dovoljen samo pooblaščenim osebam:

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

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

5.4.5. Varnostne kopije dnevnikov beleženih dogodkov

Varnostne kopije dnevnikov beleženih dogodkov v elektronski obliki se izdeluje v okviru varnostnega kopiranja sistemov. Enkrat mesečno se en izvod varnostne kopije dnevnikov v elektronski obliki prenese na oddaljeno lokacijo.

5.4.6. Način zbiranja beleženih dogodkov

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

5.4.7. Obveščanje povzročitelja dogodka

Povzročitelja dogodka o dogodku ni treba obvestiti.

5.4.8. Ocena in odprava ranljivosti

Dnevnike beleženih dogodkov pregleduje operativno osebje overitelja SIMoD-CA-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

Overitelj SIMoD-CA-Root hrani naslednje podatke:

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

5.5.2. Obdobje hranjenja arhiva

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

Overitelj SIMoD-CA-Root hrani odobritve/zavrnitve zahtevkov za izdajo digitalnih potrdil in spremljajoče dokumente, dokumentacijo o izvedbi postopkov izdaje digitalnih potrdil in korespondenco s subjekti, katerim je overitelj SIMoD-CA-Root izdal digitalno potrdilo, najmanj pet (5) let od zaključka zadeve oziroma od zadnjega dne veljavnosti digitalnega potrdila, ki je povezano s hranjenim dokumentom.

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

5.5.3. Zaščita arhiva

Podatki, ki sodijo v dokumentarno gradivo (odobritve/zavrnitve zahtevkov za izdajo digitalnih potrdil in spremljajoče dokumente in spremljajoči dokumenti, dokumentacija o izvedbi postopka izdaje digitalnih potrdil, korespondenca s subjekti, katerim je overitelj SIMoD-CA-Root izdal digitalno potrdilo in verzije pravil delovanja overitelja SIMoD-CA-Root) se hranijo in arhivirajo v skladu s predpisi za delo z dokumentarnim gradivom.

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

5.5.4. Varnostna kopija arhiva

Podatkom, ki sodijo v dokumentarno gradivo (odobritve/zavrnitve zahtevkov za izdajo digitalnih potrdil in spremljajoče dokumente in spremljajoči dokumenti, dokumentacija o izvedbi postopka izdaje digitalnih potrdil, korespondenca s subjekti, katerim je overitelj SIMoD-CA-Root izdal digitalno potrdilo in verzije pravil delovanja overitelja SIMoD-CA-Root), se zagotavlja razpoložljivost v skladu s predpisi za delo z dokumentarnim gradivom.

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

5.5.5. Časovno žigosanje zapisov

Ni predpisano.

5.5.6. Način arhiviranja

Ni predpisano.

5.5.7. Postopek vpogleda v in verifikacije arhiva

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

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

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

5.6. Zamenjava ključev overitelja SIMoD-CA-Root

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

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

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

Zamenjava digitalnega potrdila overitelja SIMoD-CA-Root se izvede po predpisanem in nadzorovanem postopku. Posamezne korake postopka izvaja operativno osebje overitelja SIMoD-CA-Root. Prisotne so tudi priče, ki nadzorujejo izvajanje postopka. Izvedba postopka je dokumentirana v zapisniku, ki ga podpišejo vsi prisotni.

5.7. Okrevalni načrt

5.7.1. Postopki v primeru okvar in zlorab

Okrevalni načrt je predpisan v zaupnem delu pravil delovanja overitelja SIMoD-CA-Root.

5.7.2. Uničenje programske, strojne opreme ali podatkov overitelja

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

V primeru okvare, kjer pride do uničenja zasebnega ključa overitelja 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 overitelja SIMoD-CA-Root.

V posebnih primerih lahko aplikacije še naprej določen čas uporabljajo digitalna potrdila, podpisana z uničenim zasebnim ključem overitelja s poglavjem 4.9.3.2 Postopki preklica digitalnega potrdila overitelja SIMoD-CA-Root. Ta možnost mora biti predvidena v pravilih uporabe konkretne aplikacije.

5.7.3. Zloraba zasebnega ključa overitelja SIMoD-CA-Root

Postopki ob zlorabi zasebnega ključa korenskega overitelja SIMoD-CA-Root so predpisani v poglavju 4.9.3.2 Postopki preklica digitalnega potrdila overitelja 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 overitelja SIMoD-CA-Root oziroma uničenje in poškodovanje varovanih prostorov overitelja, so del okrevalnega načrt, ki je predpisan v zaupnem delu pravil delovanja overitelja SIMoD-CA-Root.

5.8. Prenehanje delovanja overitelja SIMoD-CA-Root

Vzroki za prenehanje delovanja overitelja SIMoD-CA-Root so podani v poglavju 4.9.1.2 Okoliščine preklica digitalnega potrdila overitelja SIMoD-CA-Root. Odločitev o prenehanju delovanja izda Svet za upravljanje z infrastrukturo javnih ključev na MO.

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

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

- operativno osebje,
- medsebojno priznane ali podrejene overitelje in
- ministrstvo, pristojno za registracijo overiteljev v Republiki Sloveniji.

Overitelj bo po prenehanju delovanja izvedel postopke predpisane v poglavju 4.9.3.2 Postopki preklica digitalnega potrdila overitelja SIMoD-CA-Root.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev para ključev

6.1.1. Generiranje para ključev

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

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

6.1.2. Dostava zasebnega ključa imetniku

Ni relevantno. Overitelj SIMoD-CA-Root ne generira zasebnih ključev podrejenim ali medsebojno priznanim overiteljem.

6.1.3. Dostava imetnikovega javnega ključa overitelju SIMoD-CA-Root

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

6.1.4. Dostava javnega ključa overitelja SIMoD-CA-Root tretjim osebam

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

6.1.5. Dolžina ključev

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

Dolžina RSA zasebnega ključa podrejenih overiteljev SIMoD-PKI je 2048 bitov.

6.1.6. Parametri za generiranje javnih ključev in preverjanje parametrov

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

6.1.7. Namen uporabe ključev

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

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

Dovoljene vrednosti razširitvenega polja za digitalna potrdila overiteljev so:

- *KeyCertSign* in
- *CRLSign*.

6.2. Zaščita zasebnih ključev in zahteve za kriptografske module

6.2.1. Standardi za kriptografski modul

Overitelj SIMoD-CA-Root uporablja strojni varnostni kriptografski modul, ki ima potrdilo o skladnosti z enim od sledečih standardov:

- FIPS 140-2 Level 3 ali višji,

- CEN CWA 14167-2, 14167-3 ali 14167-4,
- CEN CWA 14169 ali ISO/IEC 15408 Level EAL4+ ali višji.

6.2.2. Nadzor zasebnega ključa overitelja z več pooblaščenimi osebami

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

6.2.3. Odkrivanje zasebnega ključa

Odkrivanje zasebnega ključa overitelja SIMoD-CA-Root overitelja 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 overitelja 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.

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

6.2.5. Arhiviranje zasebnega ključa

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

6.2.6. Zapis zasebnega ključa v kriptografski modul in iz njega

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

6.2.8. Postopek za aktiviranje zasebnega ključa

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

6.2.9. Postopek za deaktiviranje zasebnega ključa

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

6.2.10. Postopek za uničenje zasebnega ključa

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

6.2.11. Stopnja varnosti kriptografskih modulov

Opisano v poglavju 6.2.1 Standardi za kriptografski modul.

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

6.3. Ostali vidiki upravljanja s pari ključev

6.3.1. Arhiviranje javnega ključa

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

6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil

Veljavnost digitalnega potrdila oziroma javnega ključa overitelja SIMoD-CA-Root je največ 20 let, veljavnost pripadajočega zasebnega ključa je največ 15 let.

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.

6.5. Varnostne zahteve za računalnike

6.5.1. Specifične tehnične varnostne zahteve za računalnike

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

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

6.5.2. Raven varnostne zaščite računalnikov

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

6.6. Tehnični nadzor življenjskega cikla overitelja

6.6.1. Nadzor razvoja sistema

Strojna in programska oprema overitelja SIMoD-CA-Root so komercialni proizvodi.

6.6.2. Upravljanje varnosti

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

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

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

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

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

6.6.3. Upravljanje varnosti čez življenjski cikel

Nadgradnje, nove verzije in popravki delov informacijskih sistemov overitelja 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 overitelj SIMoD-CA-Root ni povezan v nobeno računalniško omrežje.

6.8. Časovno žigosanje

Ni predpisano.

7. PROFIL DIGITALNIH POTRDIL IN REGISTROV PREKLICANIH POTRDIL

7.1. Profil digitalnih potrdil

7.1.1. Verzija digitalnih potrdil

Overitelj SIMoD-CA-Root izdaja digitalna potrdila X.509 verzije 3 v skladu s priporočilom [5] RFC 3280, ki vsebujejo naslednja osnovna polja:

Osnovno polje (Field)	Potrdilo overitelja SOMoD-CA-Root	Potrdilo podrejenega overitelja
X.509 verzija *(version)*	2 (kar pomeni verzijo 3)	2 (kar pomeni verzijo 3)
serijska številka *(serialNumber)*	enolična serijska številka na nivoju SIMoD-CA-Root	enolična serijska številka na nivoju SIMoD-CA-Root
overiteljev podpis *(signature*)	*sha1WithRSAEncryption*	*sha1WithRSAEncryption*
overitelj *(Issuer)*	razločevalno ime SIMoD-CA-Root	razločevalno ime SIMoD-CA-Root
Veljavnost potrdila *(validity)*	<*pričetek veljavnosti po GMT*> <*konec veljavnosti po GMT*>	<*pričetek veljavnosti po GMT*> <*konec veljavnosti po GMT*>
imetnik *(subject)*	razločevalno ime SIMoD-CA-Root	razločevalno ime podrejenega overitelja
podatki o imetnikovem javnem ključu *(subjectPublicKeyInfo)*	*rsaEncryption*, modul, eksponent, vrednost javnega ključa	*rsaEncryption*, modul, eksponent, vrednost javnega ključa

7.1.2. Razširitvena polja

Standardna razširitvena polja po priporočilu [5] RFC 3280, uporabljena v digitalnih potrdilih overitelja SIMoD-CA-Root in podrejenih overiteljev:

Standardno razširitveno polje (Field)	Potrdilo overitelja SiMoD-CA-Root	Potrdilo podrejenega overitelja
odtis javnega ključa overitelja (*AuthorityKeyIdentifier*)	ni uporabljeno	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Root,s katerim je podpisano potrdilo
odtis imetnikovega javnega ključa (*SubjectKeyIdentifier*)	SHA-1 odtis javnega ključa overitelja SIMoD-CA-Root	SHA-1 odtis javnega ključa podrejenega overitelja
namen uporabe ključa (*KeyUsage*)	**Kritično** *keyCertSign* *cRLSign*	**Kritično** *keyCertSign* *cRLSign*
razširjen namen uporabe ključa (*extendedKeyUsage*)	ni uporabljeno	ni uporabljeno
veljavnost zasebnega ključa (*privateKeyUsagePeriod*)	<*pričetek veljavnosti po GMT*> <*konec veljavnosti po GMT*>	<*pričetek veljavnosti po GMT*> <*konec veljavnosti po GMT*>
oznaka politike potrdila (*certificatePolicies*)	ni uporabljeno	ni uporabljeno

naslovi registra preklicanih potrdil (*CRLDistributionPoints*)	ni uporabljeno	LDAP in http URL naslov registra preklicanih potrdil podrejenega overitelja
alternativno ime imetnika (subjectAltName)	ni uporabljeno	ni uporabljeno
osnovne omejitve (*basicConstraint*)	**Kritično** *CA =: True* *pathLenConstraint = 1*	**Kritično** *CA =: True* *pathLenConstraint = 0*

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

7.1.3. Identifikacijske oznake algoritmov

identifikacijski oznaki kriptografskih algoritmov, uporabljena v digitalnih potrdilih, ki jih izdaja overitelj SIMoD-CA-Root, sta:

Algoritem	Identifikacijska oznaka
rsaEncryption	1.2.840.113549.1.1.1
Sha1WithRSAEncryption	1.2.840.113549.1.1.5

7.1.4. Oblike imen

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.

7.1.6. Identifikacijska oznaka politik

Digitalna potrdila overitelja SIMoD-CA-Root in podrejenih overiteljev nimajo identifikacijske oznake politike.

7.1.7. Način uporabe razširitvenega polja za omejitev uporabe politik

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

7.1.8. Specifični podatki o politiki

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

7.1.9. Procesiranje oznake kritičnosti razširitvenih polj

Uporabniške aplikacije morajo procesirati razširitvena polja digitalnega potrdila, označena kot kritična, v skladu s priporočili [5] RFC 3280.

7.2. Profil registrov preklicanih potrdil

7.2.1. Verzija registrov preklicanih potrdil

Overitelj SIMoD-CA-Root izdaja registre preklicanih potrdil verzije 2 v skladu s priporočilom [5] RFC 3280, ki vsebujejo naslednja osnovna polja:

Osnovno polje - angleški naziv	Osnovno polje - slovenski opis	Vrednost
version	verzija	v2
signature	algoritem za podpis registra	*sha1WithRSAEncryption*
Issuer	izdajatelj	razločevalno ime overitelja
thisUpdate	čas izdaje registra	čas izdaje po GMT
nextUpdate	čas izdaje naslednjega registra	čas naslednje izdaje po GMT
revokedCertificates:	preklicana potrdila	
userCertificate	preklicano potrdilo	serijska številka preklicanega potrdila
revocationDate	datum preklica	čas preklica
reasonCode	vzrok za preklic	Možne vrednosti: *Unspecified (0), keyCompromise (1), cACompromise (2), affiliationChanged(3), superseded (4), cessationOfOperation (5), certificateHold (6), removeFromCRL (8), privilegeWithdrawn (9), aACompromise (10)*

7.2.2. Razširitvena polja registrov preklicanih potrdil

Overitelj SIMoD-CA-Root izdaja registre preklicanih potrdil verzije 2 v skladu s priporočilom [5] RFC 3280, ki vsebujejo naslednja standardna razširitvena polja:

Razširitveno polje - angleški naziv	Razširitveno polje - slovenski opis	Vrednost
CRLNumber	zaporedna številka registra	zaporedna številka registra
AuthorityKeyIdentifier	identifikator javnega ključa overitelja, ki podpisuje register preklicanih potrdil	*KeyID* = <SHA-1 odtis javnega ključa overitelja>

7.3. Profil OSCP

7.3.1. Verzija OSCP

Ni podprto.

7.3.2. Razširitve OSCP

Ni podprto.

8. PREVERJANJE SKLADNOSTI IN OSTALE OBLIKE NADZORA

8.1. Pogostost inšpekcije

Pogostost inšpekcijskega nadzora je v pristojnosti inšpekcijske službe, ki je določena z [1] ZEPEP.

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

8.2. Pogoji za inšpektorja

Izvajalec inšpekcijskega nadzora mora imeti ustrezno dovoljenje za dostop do tajnih podatkov.

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

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

Inšpektor mora biti neodvisen od infrastrukture javnih ključev na MO.

8.4. Področja inšpekcije

Inšpekcijski nadzor preverja skladnost delovanja overiteljev z [1] ZEPEP, Politiko SIMoD-PKI in pravili delovanja overitelja SIMoD-CA-Root.

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

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

8.5. Postopki po opravljeni inšpekciji

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

- opozori na pomanjkljivosti, vendar kljub temu dovoli obratovanje overitelja SIMoD-CA-Root do naslednje predvidene inšpekcije ali
- pred preklicem overiteljevega potrdila dodeli overitelju SIMoD-CA-Root 30 dni za odpravo pomanjkljivosti, v tem času dovoli delovanje ali
- odredi preklic overiteljevega potrdila.

8.6. Prejemniki ugotovitev o inšpekciji

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

Overitelj SIMoD-CA-Root se na osnovi ugotovitev inšpektorja odloči ali je potrebno o ugotovitvah obvestiti podrejene overitelje.

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

9. OSTALE POSLOVNE IN PRAVNE ZADEVE

9.1. Cenik

9.1.1. 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 zavarovano svojo odgovornost skladno z [1] ZEPEP oziroma [2] Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje.

9.2.2. Druge oblike zavarovanja

Ni predpisano.

9.2.3. Zavarovanje ali jamstva za končne uporabnike

Ni predpisano.

9.3. Zaupnost poslovnih informacij

Ni predpisano.

9.3.1. Obseg zaupnih poslovnih informacij

Ni predpisano.

9.3.2. Informacije izven obsega zaupnih poslovnih informacij

Ni predpisano.

9.3.3. Odgovornost za zagotavljanje zaupnosti poslovnih informacij

Ni predpisano.

9.4. Zaupnost osebnih podatkov

9.4.1. Načrt zagotavljanja zaupnosti osebnih podatkov

Overitelj SIMoD-CA-Root pridobi osebne podatke z zahtevki za izdajo digitalnega potrdila. Pridobljeni podatki se uporabljajo izključno za potrebe izdaje in upravljanja digitalnih potrdil. Osebni podatki imetnikov se obdelujejo kot določa [8] Zakon o varstvu osebnih podatkov.

9.4.2. Obseg osebnih podatkov, ki se obravnavajo kot zaupni

Osebne podatke in rokovanje z njimi določa [8] Zakon o varstvu osebnih podatkov.

9.4.3. Osebni podatki, ki se ne obravnavajo kot zaupni

Osebne podatke in rokovanje z njimi določa [8] Zakon o varstvu osebnih podatkov.

9.4.4. Odgovornost glede varovanja osebnih podatkov

Za varovanje osebnih podatkov so odgovorni Svet za upravljanje z infrastrukturo javnih ključev na MO in operativno osebje overitelja SIMoD-CA-Root.

9.4.5. Dovoljenje za uporabo osebnih podatkov

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

9.4.6. Posredovanje osebnih podatkov v sodnih in upravnih postopkih

Osebne podatke se v sodnih in upravnih postopkih posreduje v skladu z [8] Zakon o varstvu osebnih podatkov in ostalimi predpisi.

9.4.7. Druge okoliščine posredovanja osebnih podatkov

Ni predpisano.

9.5. Zaščita intelektualne lastnine

Ministrstvo za obrambo Republike Slovenije je lastnik 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 overitelja SIMoD-CA-Root

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

9.6.2. Odgovornosti in jamstva prijavne službe

Overitelj 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 zahtevkih.

9.6.3. Odgovornosti in jamstva imetnikov digitalnih potrdil

Odgovorna oseba podrejenega overitelja jamči, da:

- je bila seznanjen s Politiko SIMoD PKI in pravili delovanja overitelja SIMoD-CA-Root pred podpisom zahtevka za izdajo digitalnega potrdila,
- ravna v skladu s Politiko SIMoD-PKI, pravili delovanja overitelja SIMoD-CA-Root, svojimi pravili delovanja in ostalimi pravnimi akti,

- spremlja obvestila overitelja SIMoD-CA-Root in ravna v skladu z njimi,
- je Svetu za upravljanje z infrastrukturo javnih ključev na MO posredovala popolne in točne podatke in
- se strinja z javno objavo digitalnega potrdila podrejenega ali medsebojno priznanega overitelja.

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 overitelja SIMoD-CA-Root

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

- je bilo digitalno potrdilo izdano kot rezultat napake ali neverodostojnosti podatkov v zahtevku,
- je bilo digitalno potrdilo spremenjeno ali kakor koli drugače modificirano,
- je bilo digitalno potrdilo uporabljeno po preteku veljavnosti,
- je bilo digitalno potrdilo uporabljeno po preklicu in objavi v registru preklicanih potrdil,
- je bil zasebni ključ zlorabljen ali obstaja sum, da je bil zlorabljen,
- je bilo digitalno potrdilo uporabljeno v drugačne namene, kot je dovoljeno s Politiko SIMoD-PKI, pravili delovanja overitelja SIMoD-CA-Root, svojimi pravili delovanja overitelja ali morebitni drugi pogodbi,
- podrejeni overitelj, imetnik ali tretja oseba ni postopala v skladu s predpisanimi postopki v Politiki SIMoD-PKI, pravilih delovanja overitelja SIMoD-CA-Root, svojih pravilih delovanja, morebitni drugi pogodbi in obvestilih overitelja SIMoD-CA-Root ali
- je nastala škoda zaradi napake v delovanju strojne ali programske opreme, podrejenega overitelja, imetnika ali tretje osebe,
- je do ravnanja v nasprotju s Politiko SIMoD-PKI ali ostalimi dokumenti prišlo zaradi višje sile, to je izredne nepredvidljive okoliščine na katere udeleženci infrastrukture javnih ključev na MO ne morejo vplivati (na primer naravne nesreče, terorizem, …).

9.8. Omejitve odgovornosti overitelja SIMoD-CA-Root

Overitelj 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 naslednji dan po podpisu, uporabljati pa se začnejo trideset (30) dni po podpisu.

9.10.2. Prenehanje veljavnosti

Veljavnost Javnih pravil SIMoD-CA-Root ni časovna omejena in velja do uveljavitve nove verzije.

9.10.3. Posledice prenehanja veljavnosti

Po prenehanju veljavnosti Javnih pravil SIMoD-CA-Root zaradi objave nove verzije podrejeni overitelji praviloma uporabljajo obstoječa digitalna potrdila v skladu s Javnimi pravili SIMoD-CA-Root, po katerih so bila izdana. V primeru, da zaradi spremenjenih okoliščin to ne bo več mogoče, bo overitelj SIMoD-CA-Root ob izdaji nove verzije Javnih pravil SIMoD-CA-Root obvestil imetnike.

9.11. Obvestila in komuniciranje z udeleženci

Overitelj 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

Overitelj 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 pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06)

[3] Politika SIMoD-PKI Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, Verzija 2.0., št. 382-5/2006-109, datum: 24.08.2010

[4] RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

[5] RFC 3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

9.15. Ostala relevantna zakonodaja

Overitelj SIMoD-CA-Root mora pri svojem delovanju upoštevati tudi:

[6] ZObr Zakon o obrambi (Uradni list RS, št. 103/04 – UPB1)

[7] ZTP Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – UPB2, 9/10)

[8] Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – UPB1)

9.16. Razne določbe

Poleg Javnih pravil SIMoD-CA-Root opredeljujejo delovanje overitelja 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. Varnostna okrepitev HP-UX strežnikov

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

9.17. Končne določbe

To neuradno prečiščeno besedilo Pravil delovanja overitelja SIMoD-CA-Root, javni del, ver. 2.0, združuje dokumenta Pravila delovanja overitelja SIMoD-CA-Root, javni del, verzija 2.0, številka: 382-5/2006-119 in Pravila o spremembah Pravil delovanja overitelja SIMoD-CA-Root, javni del, verzija 2.0, številka: 386-6/2011-337.