REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Pravila delovanja izdajatelja SIMoD-CA-Root, javni del

(javna pravila SIMoD-CA-Root)

Verzija 3.1

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

Izdaja:	Spremembe glede na prejšnjo izdajo:
Pravila delovanja izdajatelja SIMoD-CA-Root, javni del, ver. 3.1	Ukinitev Sveta za upravljanje z infrastrukturo javnih ključev na MO. Uskladitev izrazov; nadomestitev izrazov »overitelj« in »infrastruktura javnih ključev« z izrazom »ponudnik storitev zaupanja«. Odstranjeno navajanje obveznosti v povezavi z Uredbo eIDAS. Uredniški popravki.
Pravila o dopolnitvah Pravil delovanja izdajatelja SIMoD-CA-Root, javni del, ver. 3.0, številka: 386-12/2018-15, 28.03.2018	Dodane obveznosti v povezavi z Uredbo eIDAS. Dodana obveza pregledovanja pravil SIMoD-CA-Root in ostalih dokumentov, povezanih z delovanjem izdajatelja SIMoD-CA-Root. Dodane določbe glede preverjanja skladnosti oziroma nadzora.
Pravila delovanja izdajatelja SIMoD-CA-Root, javni del, ver. 3.0, številka: 386-12/2017-38, 03. 05. 2017	Uskladitev z Uredbo eIDAS. Uskladitev s spremembami priporočil ETSI. Uskladitev izrazov; konsistentna uporaba izrazov »overitelj« in »izdajatelj«. Revidiran postopek za pridobitev digitalnega potrdila podrejenega izdajatelja.
Pravila o spremembah in dopolnitvah Pravil delovanja overitelja SIMoD-CA-Root, javni del, ver. 2.0, številka: 386-11/2014-22, 07.02.2014	Prenehanje uporabe algoritma SHA-1 in začetek uporabe algoritma SHA256.
Pravila o spremembah Pravil delovanja overitelja SIMoD-CA-Root, javni del, ver. 2.0, številka: 386-6/2011-337, 21.12.2011	Podaljšana veljavnost digitalnega potrdila oziroma javnega ključa in zasebnega ključa korenskega overitelja SIMoD-CA-Root.
Pravila delovanja overitelja SIMoD-CA-Root, javni del, ver. 2.0, številka: 382-5/2006-119, 23.11.2010	Pristojnost sprejemanja pravil delovanja overiteljev prenešena 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, 27.12.2007	Spremenjeno je pravilo za določanje identifikacijske oznake dokumenta.
Pravila delovanja overitelja SIMoD-CA-Root, javni del, šifra: 382-5/2006-12, 17.07.2006	V infrastrukturo javnih ključev na MO 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, 29.07.2005	

KAZALO

PRAVILA DELOVANJA IZDAJATELJA SIMoD-CA-Root
JAVNI DEL

(javna pravila SIMoD-CA-Root)

Verzija 3.1

1. UVOD

1.1. Pregled

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

SIMoD-PKI je ponudnik storitev zaupanja kot opredeljeno v [1] eIDAS za potrebe obrambe države.

V okviru SIMoD-PKI deluje korenski izdajatelj in podrejeni izdajatelji digitalnih potrdil.

Politika SIMoD-PKIpredpisuje pogoje, ki jih morajo izpolnjevati izdajatelji za zagotavljanje zaupanja v digitalna potrdila; predpisuje splošne zahteve za digitalna potrdila, minimalne zahteve za tehnične lastnosti in raven varnosti infrastrukture izdajateljev, postopke za upravljanje digitalnih potrdil, obveznosti in odgovornosti, ki jih morajo izpolnjevati izdajatelji, imetniki in tretje osebe, ki se zanašajo na digitalna potrdila, ter drugi izdajatelji, ki se želijo povezovati z izdajatelji SIMoD-PKI.

SIMoD-CA-Root (ang. **S**lovenian **M**inistry **o**f **D**efence **Root C**ertification **A**uthority) je korenski izdajatelj SIMoD-PKI oziroma ponudnika storitev zaupanja na MO.

Izdajatelj SIMoD-CA-Root deluje v skladu s politiko SIMoD-PKI.

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

Ta dokument imenujemo tudi javna pravila SIMoD-CA-Root.

Javna pravila SIMoD-CA-Root podajajo opis infrastrukture in postopkov izdajatelja ter izpolnjevanje zahtev politike SIMoD-PKI. Zainteresirane strani, ki potrebujejo informacije za oceno zaupanja v SIMoD-PKI kot celoto, oceno zaupanja v digitalna potrdila imetnikov, ali informacije o podrejenih izdajateljih, morajo poleg pričujočega dokumenta upoštevati še določila politike SIMoD-PKI in pravil delovanja podrejenih izdajateljev.

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

- podrejenim izdajateljem,
- medsebojno priznanim izdajateljem in
- operativnemu osebju za potrebe upravljanja izdajatelja SIMoD-CA-Root.

Dokument je skladen z [7] RFC 3647 in predstavlja pravila delovanja izdajatelja (ang. Certification Practices Statement, CPS) v odnosu na politiko SIMoD-PKI, ki predstavlja politiko delovanja (ang. Certificate Policy, CP).

1.2. Identifikacijske oznake politik delovanja

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

1.3. Udeleženci infrastrukture javnih ključev

1.3.1. Korenski izdajatelj SIMoD-CA-Root

Odgovorna oseba ponudnika storitev zaupanja na MO je minister za obrambo.

Izdajatelj SIMoD-CA-Root poseduje strojno in programsko opremo ter izvaja predpisane postopke in ukrepe, ki zagotavljajo varno in zanesljivo poslovanje.

Z izdajateljem SIMoD-CA-Root upravlja organizacijska enota, pristojna za informatiko.

Operativno osebje izdajatelja SIMoD-CA-Root so zaposleni organizacijske enote, pristojne za informatiko, ki upravljajo z digitalnimi potrdili in zagotavljajo varno ter zanesljivo delovanje informacijske infrastrukture izdajatelja SIMoD-CA-Root.

Kontaktni podatki ponudnika storitev zaupanja na MO so:

Naslov:	Ministrstvo za obrambo Sekretariat generalnega sekretarja Služba za informatiko in komunikacije Vojkova cesta 55, 1000 Ljubljana
Telefon:	01 230 53 14
Spletni naslov:	http://www.simod-pki.mors.si
Naslov elektronske pošte:	simod-pki@mors.si

1.3.2. Prijavna služba

Izdajatelj SIMoD-CA-Root nima vzpostavljene prijavne službe.

1.3.3. Imetniki digitalnih potrdil

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

1.3.4. Tretje osebe

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

1.3.5. Posredno odgovorni organi

Izdajatelj SIMoD-CA-Root deluje skladno s pravnimi akti MO za KIS MO. Posredno odgovorni organi za delovanje SIMoD-PKI so tudi organizacijske enote, ki so pristojne za varovanje in nadzor KIS MO.

1.4. Namen uporabe digitalnih potrdil

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

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

1.4.1. Dovoljena uporaba digitalnih potrdil

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

1.4.2. Nedovoljena uporaba digitalnih potrdil

Ni določb.

1.5. Upravljanje s pravili SIMoD-CA-Root

1.5.1. Organ, ki upravlja ta dokument

Organizacijska enota, pristojna za informatiko, vodi postopek izdelave javnih in zaupnih pravil SIMoD-CA-Root.

Spremembe in dopolnitve oziroma nova javna in zaupna pravila SIMoD-CA-Root sprejme vodja organizacijske enote, pristojne za informatiko.

1.5.2. Kontaktni podatki

Glej podpoglavje 1.3. Udeleženci infrastrukture javnih ključev.

1.5.3. Organ za odobritev skladnosti pravil SIMoD-CA-Root

Odgovorni organ za odobritev skladnosti javnih in zaupnih pravil SIMoD-CA-Root s politiko SIMoD-PKI je kolegij organizacijske enote, pristojne za informatiko.

1.5.4. Postopek odobritve pravil SIMoD-CA-Root

Kolegij organizacijske enote, pristojne za informatiko:

- preveri skladnost javnih in zaupnih pravil SIMoD-CA-Root s politiko SIMoD-PKI in
- vodi postopek potrditve javnih in zaupnih pravil SIMoD-CA-Root.

Javna in zaupna pravila SIMoD-CA-Root sprejme vodja organizacijske enote, pristojne za informatiko.

1.6. Pojmi in kratice

Pojem	Definicija
Digitalno potrdilo	Potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z imetnikom potrdila.
Digitalno potrdilo za preverjanje podpisa	Digitalno potrdilo, ki se uporablja za verifikacijo digitalnega podpisa in preverjanje celovitosti podatkov v elektronski obliki. V tem dokumentu uporabljen kot ekvivalenten izraz za »potrdilo za elektronski podpis ali žig« po [1] eIDAS.
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.
Elektronski žig	Niz podatkov v elektronski obliki, ki so dodani k drugim podatkom v elektronski obliki ali so z njimi logično povezani, da se zagotovita izvor in celovitost povezanih podatkov.
Imenik	Podatkovna struktura, ki vsebuje objekte z določenimi lastnostmi in pripadajočimi vrednostmi. Imenik, ki vsebuje digitalna potrdila, običajno v skladu s standardom X.500 oziroma razširjenim standardom X.509 ver.3.
Imetnik potrdila	Fizična oseba, navedena v digitalnem potrdilu v polju *Subject*. Lastnik zasebnega ključa, ki ustreza javnemu ključu, vsebovanem v digitalnem potrdilu oziroma odgovorna oseba za uporabo digitalnega potrdila.
Infrastruktura javnih ključev	Pravila, postopki, vloge in informacijski sistem za implementacijo varnostnih storitev na osnovi kriptografije javnih ključev oziroma za upravljanje digitalnih potrdil.
Izdajatelj	Izdajatelj digitalnih potrdil, ki deluje v okviru ponudnika storitev zaupanja.

Kvalificirano digitalno potrdilo	V tem dokumentu izraz uporabljen za kvalificirano potrdilo za elektronski podpis ali elektronski žig. Potrdilo, ki ga izda ponudnik kvalificiranih storitev zaupanja in izpolnjuje zahteve iz Priloge I oziroma Priloge III [1] eIDAS.
Politika digitalnih potrdil	Pravila, ki posledično definirajo uporabnost digitalnih potrdil v določeni skupini uporabnikov in/ali za določene aplikacije s skupnimi varnostnimi zahtevami.
Ponudnik storitev zaupanja	Po definiciji 19. odstavka 3. člena [1] eIDAS: fizična ali pravna oseba, ki zagotavlja eno ali več storitev zaupanja.
Potrdilo za elektronski podpis	Po definiciji 14. odstavka 3. člena [1] eIDAS: elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega podpisa s fizično osebo in potrjuje vsaj ime ali psevdonim te osebe. V tem dokumentu se namesto izraza »potrdilo za elektronski podpis« uporablja izraz »digitalno potrdilo«.
Prijavna služba	Služba oziroma organizacija, ki po pooblastilu izdajatelja sprejema zahtevke in preverja istovetnosti bodočih imetnikov.
Storitev zaupanja	Elektronska storitev po definiciji 16. odstavka 3. člena [1] eIDAS: a) ustvarjanje, preverjanje in potrjevanje veljavnosti elektronskih podpisov, elektronskih žigov ali elektronskih časovnih žigov, storitev elektronske priporočene dostave in potrdil, povezanih s temi storitvami, b) ustvarjanje, preverjanje in potrjevanje veljavnosti potrdil za avtentikacijo spletišč ali c) hramba elektronskih podpisov, žigov ali potrdil, povezanih s temi storitvami.
Tretja oseba	Subjekt, ki ni aktivno udeležen v storitev, vendar zaupa izvajalcu in rezultatu storitve.
Uporabnik	Naročnik ali imetnik digitalnega potrdila.
Zloraba	Razkritje tajnega podatka, izguba celovitosti ali razpoložljivosti podatka.

Kratica	Opis
CN	Splošno ime objekta v imeniku (ang. Common Name)
CRL	Register preklicanih potrdil (ang. Certificate Revocation List)
DN	Razločevalno ime objekta v imeniku, tudi polno ime objekta v imeniku (ang. Distinguished Name)
eIDAS	Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi direktive 1999/93/ES.
ETSI	Evropski inštitut za standardizacijo na področju telekomunikacij, izdaja serijo standardov s področja elektronskega podpisa in delovanja ponudnikov storitev zaupanja (ang. European Telecommunications Standards Institute).
HTTP	Protokol za prenos podatkov v spletnem okolju (ang. Hypertext Transfer Protocol).
IETF	Združenje strokovnjakov s področja internetnih tehnologij, ki pripravlja priporočila (ang. Internet Engineering Task Force).
LDAP	Protokol, ki določa dostop do imenika po priporočilu IETF RFC 1777 (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 funkcij RSA. Predpisujejo, kako se izračuna elektronski podpis in kako se formatirajo podatki, ki se podpisujejo, ter format podpisa. Predpisujejo tudi sintakso javnega in zasebnega ključa RSA.

PKCS#10	Sintaksa zahtevka za digitalno potrdilo. Zahtevek za digitalno potrdilo vsebuje razločevalno ime, javni ključ in druge atribute. Daljše ime je Certification Request Syntax Standard.
PKCS#7	Sintaksa za kriptografsko obdelane podatke, kot so elektronski podpisi in 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, ki je 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 izdajatelja (ang. PKIX Certificate Management Protocol). Vključuje PKCS#7 in PKCS#10.
RFC	Priporočila, ki jih izdaja IETF (ang. Request for Comment).
RFC 5280	Priporočilo, ki določa elemente digitalnih potrdil in registra preklicanih potrdil.
RFC 3647	Priporočilo, ki določa elemente, ki naj bodo zajeti v politiki infrastrukture javnih ključev (ang. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework).
RFC 4210	Priporočilo, ki določa postopke za izmenjavo podatkov, ki se nanašajo na digitalna potrdila. Vsebuje PKIX-CMP.
RSA	Nesimetrični kriptografski sistem, patentiran leta 1983, imenovan po odkriteljih Rivestu, Shamirju in Adelmanu.
SIMoD-CA-Root	Korenski izdajatelj ponudnika storitev zaupanja na MO (ang. **S**loveni**a**n **M**inistry **o**f **D**efence **C**ertificate **A**uthority **Root**)
SIMoD-PKI	Infrastruktura javnih ključev Ministrstva za obrambo Republike Slovenije (ang. **S**loveni**a**n **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 5280.

2. ODGOVORNOST ZA OBJAVE IN IMENIK

2.1. Repozitoriji

Podatki o izdajateljih SIMoD-PKI in digitalnih potrdilih se objavljajo v naslednjih repozitorijih:

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

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

Zrcalni imeniki vsebujejo kopijo podatkov iz primarnega imenika. Zrcalni imeniki so nameščeni v komunikacijsko informacijskih podsistemih, ki med seboj niso povezani (KIS MO INTRANET, KIS MO TAJNO, KIS MO PUB). Vsi imajo naslov imenik.simod-pki.mors.si.

Obstaja več instanc spletne strani, in sicer primarna v KIS MO INTRANET ter več zrcalnih instanc. Zrcalne spletne strani so kopija primarne spletne strani in so nameščene v komunikacijsko informacijskih podsistemih, ki med seboj niso povezani (na primer v KIS MO PUB). Vse spletne strani imajo naslov http://www.simod-pki.mors.si.

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

2.2. Objave informacij o digitalnih potrdilih

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

- digitalno potrdilo izdajatelja SIMoD-CA-Root ter podrejenih izdajateljev (http://www.simod-pki.mors.si/izdajatelji/),
- register preklicanih potrdil izdajatelja SIMoD-CA-Root (http://www.simod-pki.mors.si/registri-crl/),
- javna pravila SIMoD-CA-Root in
- druge javne objave.

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

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

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

Register preklicanih potrdil izdajatelja SIMoD-CA-Root je v imeniku objavljen v vozlišču 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.

2.3. Čas in pogostost objav

Izdajatelj objavi digitalno potrdilo takoj, ko ga izda. Izdajatelj uvrsti preklicano digitalno potrdilo v register preklicanih potrdil takoj po preklicu. Objava registrov preklicanih potrdil je v skladu s podpoglavjema 4.9.7 Pogostost objav registrov preklicanih potrdil in 4.9.8 Dovoljene zakasnitve pri objavi registrov preklicanih potrdil.

2.4. Dostop do podatkov v repozitorijih

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

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

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

Pravila delovanja izdajatelja SIMoD-CA-Root, zaupni del, niso javno objavljena.

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

3. PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI

3.1. Določanje imen

3.1.1. Oblika imen

Podatki o imetniku digitalnega potrdila so v digitalnem potrdilu zapisani v obliki razločevalnega imena v skladu s priporočilom [8] RFC 5280.

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

3.1.2. Potreba po smiselnosti imen

Splošno ime (ang. Common Name, CN) mora nedvoumno označevati izdajatelja.

3.1.3. Anonimnost imetnikov in uporaba psevdonimov

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

3.1.4. Pravila za interpretacijo različnih oblik imen

Ni posebnih določil.

3.1.5. Edinstvenost imen

Razločevalno ime (ang. Distinguished Name, DN) je edinstveno in enolično identificira izdajatelja.

3.1.6. Priznavanje, preverjanje istovetnosti in vloga registriranih znamk

Uporaba registriranih znamk je urejena s predpisi s področja intelektualne lastnine in avtorskih pravic.

3.2. Preverjanje istovetnosti imetnikov ob prvi registraciji

3.2.1. Metode dokazovanja lastništva zasebnega ključa

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

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

3.2.2. Preverjanje istovetnosti za imetnike, ki niso fizične osebe

Za pravilnost podatkov o bodočem podrejenem izdajatelju jamči kolegij organizacijske enote, pristojne za informatiko.

3.2.3. Preverjanje istovetnosti za fizične osebe

Izdajatelj SIMoD-CA-Root izdaja digitalna potrdila za fizične osebe le svojemu operativnemu osebju za opravljanje nalog v okviru svoje vloge.

Vodja organizacijske enote, pristojne za informatiko, z imenovanjem operativnega osebja izdajatelja SIMoD-CA-Root jamči za njihovo istovetnost.

3.2.4. Podatki o naročniku, ki se ne preverjajo

Ni relevantno.

3.2.5. Preverjanje pooblastil

Vodja organizacijske enote, pristojne za informatiko, z imenovanjem operativne osebe izdajatelja SIMoD-CA-Root jamči, da je to oseba, ki opravlja naloge operativne osebe.

3.2.6. Merila za medsebojno povezovanje

Medsebojno povezovanje je mogoče samo na nivoju korenskega izdajatelja SIMoD-CA-Root.

Način in pogoji medsebojnega povezovanja bodo določeni dogovorno.

3.3. Preverjanje istovetnosti za ponovno izdajo digitalnega potrdila

3.3.1. Preverjanje istovetnosti pri rutinski ponovni izdaji digitalnih potrdil

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

Rutinska ponovna izdaja digitalnega potrdila podrejenemu izdajatelju ni možna.

3.3.2. Preverjanje istovetnosti za ponovno izdajo digitalnega potrdila po preklicu

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

3.4. Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila

Ni relevantno.

4. UPRAVLJANJE Z DIGITALNIMI POTRDILI

4.1. Pridobitev digitalnega potrdila

4.1.1. Kdo lahko zaprosi za izdajo digitalnega potrdila

Kolegij organizacijske enote, pristojne za informatiko, na podlagi potreb po storitvah zaupanja v KIS MO odloči o uvedbi podrejenega izdajatelja in izdaji digitalnega potrdila podrejenega izdajatelja.

Operativno osebje izdajatelja SIMoD-CA-Root pridobi digitalno potrdilo za opravljanje svojih nalog na osnovi imenovanja vodje organizacijske enote, pristojne za informatiko.

4.1.2. Postopek za pridobitev digitalnega potrdila in odgovornosti

Bodoči podrejeni izdajatelj posreduje zahtevek za pridobitev digitalnega potrdila kolegiju organizacijske enote, pristojne za informatiko.

Odločitev kolegija organizacijske enote, pristojne za informatiko, o izdaji digitalnega potrdila podrejenega izdajatelja vsebuje:

- obrazložitev odločitve,
- predlog za razločevalno ime podrejenega izdajatelja, če ni razvidno iz pravil delovanja podrejenega izdajatelja,
- predlog morebitnega alternativnega imena podrejenega izdajatelja,
- dokazila o izpolnjevanju pogojev npr. oceno skladnosti pravil delovanja bodočega podrejenega izdajatelja s politiko SIMoD-PKI.

4.2. Obdelava zahtevka za izdajo digitalnega potrdila

4.2.1. Preverjanje istovetnosti bodočega imetnika

Za pravilnost podatkov o bodočem podrejenem izdajatelju jamči kolegij organizacijske enote, pristojne za informatiko.

Operativno osebje SIMoD-CA-Root pred pričetkom postopka izdaje digitalnega potrdila podrejenemu izdajatelju preveri istovetnost pooblaščene osebe podrejenega izdajatelja, ki v postopku izdaje digitalnega potrdila preda operativnemu osebju SIMoD-CA-Root zahtevek z javnim ključem, za katerega se izdaja digitalno potrdilo. Istovetnost preveri na osnovi uradnega osebnega dokumenta s sliko in službene izkaznice MO, ob tem preveri ujemanje s podatki o pooblaščeni osebi v nalogu za izdajo digitalnega potrdila.

4.2.2. Odobritev ali zavrnitev izdaje digitalnega potrdila

Kolegij organizacijske enote, pristojne za informatiko, pred odločitvijo o izdaji digitalnega potrdila podrejenemu izdajatelju:

- oceni skladnost pravil delovanja podrejenega izdajatelja s politiko SIMoD-PKI, v ta namen lahko zahteva poročilo o varnostnem pregledu infrastrukture,
- v primeru odobritve izda operativnemu osebju SIMoD-CA-Root nalog za izdajo digitalnega potrdila podrejenemu izdajatelju.

4.2.3. Čas za obdelavo zahtevka za izdajo digitalnega potrdila

Časovni rok od prejema zahtevka do njegove odobritve ali zavrnitve in izdaje digitalnega potrdila podrejenega izdajatelja ni predpisan. Udeleženci v postopku (kolegij organizacijske enote, pristojne za informatiko, operativno osebje izdajatelja SIMoD-CA-Root in osebje bodočega podrejenega izdajatelja) se glede rokov dogovorijo.

4.3. Izdaja digitalnega potrdila

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

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

- preveri istovetnost pooblaščene osebe podrejenega izdajatelja kot predpisano v podpoglavju 4.2.1 Preverjanje istovetnosti bodočega imetnika,
- preveri integriteto PKCS#10 zahtevka za izdajo digitalnega potrdila,
- preveri podatke o podrejenem izdajatelju, tako da jih primerja s podatki v nalogu,
- če so izpolnjeni zgoraj navedeni pogoji, izda digitalno potrdilo,
- zapiše digitalno potrdilo in vsebino ASN.1 strukture digitalnega potrdila v berljivi obliki na medij in ga preda pooblaščeni osebi podrejenega izdajatelja in
- izdela zapisnik o izvedenem postopku.

4.3.2. Obvestilo naročnikom o izdaji digitalnega potrdila

Prevzem digitalnega potrdila podrejenega izdajatelja na mediju s strani pooblaščene osebe podrejenega izdajatelja se šteje kot potrditev prejema obvestila o izdaji digitalnega potrdila.

4.4. Prevzem digitalnega potrdila

4.4.1. Postopek potrditve prevzema digitalnega potrdila

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

4.4.2. Objava digitalnega potrdila

V skladu s podpoglavjem 2.2. Objave informacij o digitalnih potrdilih.

4.4.3. Obveščanje drugih udeležencev o izdaji digitalnega potrdila

Ni predvideno.

4.5. Uporaba ključev in digitalnih potrdil

Uporaba ključev in digitalnih potrdil je določena v podpoglavju 1.4. Namen uporabe digitalnih potrdil in je definirana v razširitvenih poljih v digitalnem potrdilu *Key Usage* in *Extended Key Usage*.

4.5.1. Uporaba ključev in digitalnih potrdil imetnikov

Izdajatelj SIMoD-CA-Root uporablja svoj zasebni ključ za podpisovanje digitalnih potrdil podrejenih in medsebojno priznanih izdajateljev ter registrov preklicanih izdajateljev.

V povezavi s fizičnimi osebami izdajatelj SIMoD-CA-Root uporablja svoj zasebni ključ samo za podpisovanje digitalnih potrdil in registrov preklicanih potrdil svojega operativnega osebja.

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

4.5.2. Uporaba digitalnih potrdil s strani tretjih oseb

Tretja oseba mora:

- pred uporabo digitalnega potrdila preveriti, ali je ustrezno za predvideno uporabo,
- uporabiti digitalno potrdilo le za namene, ki so določeni v politiki SIMoD-PKI in pravilih SIMoD-CA-Root,
- ob domnevni zlorabi zasebnega ključa ali če so spremenjeni podatki iz digitalnega potrdila, na katerega se zanaša, obvestiti operativno osebje izdajatelja SIMoD-CA-Root,
- preveriti, ali je bil podpis ustvarjen v času veljavnosti digitalnega potrdila,
- za vsako uporabljeno digitalno potrdilo opraviti popoln postopek preverjanja poti zaupanja,
- preveriti status digitalnega potrdila v veljavnem registru preklicanih potrdil oziroma registru preklicanih izdajateljev.

4.6. Ponovna izdaja digitalnega potrdila brez spremembe javnega ključa

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

4.7. Ponovna izdaja digitalnih potrdil

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

4.7.1. Razlogi za ponovno izdajo digitalnega potrdila

Razlog za ponovno izdajo digitalnega potrdila izdajatelja SIMoD-CA-Root in digitalnih potrdil podrejenih izdajateljev je prenehanje veljavnosti trenutnega digitalnega potrdila.

Ponovna izdaja digitalnega potrdila se z namenom neprekinjenega zagotavljanja storitve izvede pred pretekom veljavnosti trenutnega digitalnega potrdila.

4.7.2. Kdo lahko zahteva ponovno izdajo digitalnega potrdila

Digitalno potrdilo se ponovno izda obstoječemu izdajatelju.

4.7.3. Obdelava zahtevkov za ponovno izdajo digitalnega potrdila

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

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

4.7.4. Obvestilo imetniku o izdaji novega digitalnega potrdila

Enako kot 4.3.2 Obvestilo naročnikom o izdaji digitalnega potrdila.

4.7.5. Postopek potrditve prevzema 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

Razlogi za preklic digitalnega potrdila izdajatelja so:

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

Razlog za preklic digitalnega potrdila korenskega izdajatelja SIMoD-CA-Root je tudi sklep ministra za obrambo o prenehanju delovanja ponudnika storitev zaupanja na MO.

Razlog za preklic digitalnega potrdila podrejenega izdajatelja je tudi sklep predstojnika organizacijske enote, pristojne za informatiko, o prenehanju delovanja podrejenega izdajatelja.

4.9.2. Kdo lahko zahteva preklic

Preklic digitalnega potrdila izdajatelja zahteva predstojnik organizacijske enote, pristojne za informatiko.

Preklic digitalnega potrdila korenskega izdajatelja SIMoD-CA-Root lahko zahteva tudi minister za obrambo s sklepom o prenehanju delovanja ponudnika storitev zaupanja na MO.

4.9.3. Postopki za preklic

Preklic digitalnega potrdila izdajatelja izvede operativno osebje.

Izdajatelj ob preklicu svojega digitalnega potrdila:

- zagotavlja razpoložljivost registrov preklicanih potrdil vsaj še 90 dni,
- objavi preklic digitalnega potrdila v registru preklicanih izdajateljev,
- objavi obvestilo o preklicu svojega potrdila 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 okoliščino preklica.

4.9.5. Čas od prejema zahtevka za preklic do preklica

Korenski izdajatelj SIMoD-CA-Root prekliče svoje digitalno potrdilo oziroma digitalno potrdilo podrejenega izdajatelja takoj, ko prejme zahtevek, ali v roku, ki ga določi predstojnik organizacijske enote, pristojne za informatiko.

4.9.6. Obveza preverjanja registra preklicanih potrdil

Tretje osebe, ki se zanašajo na digitalno potrdilo, morajo pred uporabo preveriti najnovejši register preklicanih potrdil. V postopku preverjanja je treba preveriti tudi veljavnost in verodostojnost registra preklicanih potrdil. Tretja oseba mora za vsako uporabljeno digitalno potrdilo opraviti popoln postopek preverjanja poti zaupanja v skladu s [8] RFC 5280.

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

4.9.7. Pogostost objav registrov preklicanih potrdil

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

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

4.9.8. Dovoljene zakasnitve pri objavi registrov preklicanih potrdil

Dovoljena zakasnitev od izdaje novega registra preklicanih potrdil oziroma registra preklicanih izdajateljev do njegove objave je največ 120 minut.

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

4.9.9. Sprotno preverjanje statusa digitalnih potrdil

Ni relevantno. Korenski izdajatelj ne omogoča sprotnega preverjanja statusa digitalnih potrdil.

4.9.10. Obveza sprotnega preverjanja statusa preklicanih potrdil

Tretje osebe morajo ob uporabi digitalnega potrdila z vpogledom v register preklicanih potrdil oziroma register preklicanih izdajateljev preveriti, ali je digitalno potrdilo, na katerega se zanašajo, preklicano.

4.9.11. Druge oblike objavljanja preklicanih digitalnih potrdil

Niso podprte.

4.9.12. Posebne zahteve glede zlorabe ključa

Niso predpisane.

4.9.13. Okoliščine za začasno ukinitev veljavnosti

Niso podprte.

4.9.14. Kdo lahko zahteva začasno ukinitev veljavnosti

Ni podprto.

4.9.15. Postopki za začasno ukinitev veljavnosti

Niso podprti.

4.9.16. Omejitve obdobja začasne ukinitve veljavnosti

Niso podprte.

4.10. Preverjanje statusa digitalnih potrdil

4.10.1. Tehnične lastnosti storitve

Registri preklicanih potrdil so v skladu z [8] RFC 5280.

4.10.2. Razpoložljivost storitve

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

4.10.3. Dodatne možnosti

Niso predpisane.

4.11. Predčasna prekinitev veljavnosti digitalnih potrdil

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

4.12. Varnostno kopiranje in odkrivanje zasebnega ključa

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

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

4.12.1. Povrnitev zgodovine ključev za dešifriranje

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

4.12.2. Odkrivanje kopije ključev za dešifriranje

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

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

5.1. Fizično varovanje

5.1.1. Lokacija in konstrukcija prostorov

Informacijska oprema korenskega izdajatelja SIMoD-CA-Root je nameščena v namenskem ločenem prostoru, ki je varovan z več nivojskim sistemom fizičnega in tehničnega varovanja.

Prostor je varnostno območje II. stopnje po [10] ZTP.

5.1.2. Fizični dostop

Fizičnega dostop nadzira pristojna služba MO.

Nadzor fizičnega dostopa se izvaja z uporabo tehničnih sredstev, ki preprečujejo nepooblaščen vstop. Vstop je dovoljen le operativnemu osebju korenskega izdajatelja SIMoD-CA-Root. Druge osebe, ki izkažejo upravičeni interes, smejo vstopiti v prostore le v spremstvu operativnega osebja.

O vstopih in izstopih v prostore se vodi evidenca.

5.1.3. Napajanje in klimatske naprave

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

5.1.4. Zaščita pred poplavo

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

5.1.5. Zaščita pred ognjem

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

5.1.6. Shranjevanje medijev

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

Mediji, hranjeni na oddaljeni lokaciji, so v prostorih, ki zagotavljajo enake pogoje, kot so zagotovljeni na primarni lokaciji korenskega izdajatelja SIMoD-CA-Root.

5.1.7. Odstranjevanje odpadkov

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

5.1.8. Hranjenje na oddaljeni lokaciji

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

5.2. Organizacijski varnostni ukrepi

5.2.1. Organizacija upravljanja izdajatelja SIMoD-CA-Root

Operativno osebje korenskega izdajatelja SIMoD-CA-Root je razdeljeno v dve zaključeni organizacijski skupini.

V skupini za upravljanje digitalnih potrdil so:

- prvi varnostni inženir in
- varnostni inženirji.

V skupini za upravljanje programske in strojne opreme so:

- prvi administrator in
- administratorji.

Razdelitev pristojnosti in nalog:

Vloga	Pristojnosti in naloge	Min. št. oseb
Upravljanje digitalnih potrdil		
Prvi varnostni inženir	• Določanje in izvajanje pravil varnega delovanja sistema za upravljanje potrdil, • določanje uporabniških pravic drugih varnostnih inženirjev, • upravljanje s potrdili, • pregled in analiza varnostnih beležk, • nadzor hranjenja varnostnih kopij.	1
Varnostni inženir	• Izvajanje pravil varnega delovanja sistema za upravljanje potrdil, • upravljanje s potrdili, • pregled in analiza varnostnih beležk.	2
Upravljanje programske in strojne opreme izdajatelja		
Prvi administrator izdajatelja	• Odgovornost za delovanje strojne in programske opreme izdajatelja, • namestitev in začetna konfiguracija strojne in programske opreme izdajatelja, • načrtovanje in izvedba sprememb strojne in programske opreme izdajatelja, • izdelava in vzdrževanje varnostnih kopij, • ponovna vzpostavitev delovanja iz varnostnih kopij, • pregled in analiza varnostnih beležk.	1
Administrator izdajatelja	• Namestitev in začetna konfiguracija strojne in programske opreme izdajatelja, • vzdrževanje delovanja strojne in programske opreme izdajatelja, • izvedba sprememb strojne in programske opreme, • izdelava in vzdrževanje varnostnih kopij.	1

5.2.2. Število oseb za izvedbo postopkov

V skupini za upravljanje z digitalnimi potrdili so najmanj tri osebe, v skupini za upravljanje programske in strojne opremo sta najmanj dve osebi.

5.2.3. Preverjanje istovetnosti operativnega osebja

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

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

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

- pripadati eni sami fizični osebi in
- omogočati avtorizacijo za opravljanje nalog le v obsegu predpisanih nalog.

5.3. Zahteve za osebje izdajatelja SIMoD-CA-Root

5.3.1. Kvalifikacije, izkušnje in varnostno preverjanje

Operativno osebje korenskega izdajatelja SIMoD-CA-Root:

- je ustrezno usposobljeno,
- ne sme opravljati drugih nalog, ki bi bile v nasprotju z opravljanjem nalog pri izdajatelju SIMoD-CA-Root.

5.3.2. Dovoljenja za dostop do tajnih podatkov

V skladu z [10] ZTP.

5.3.3. Usposabljanje osebja

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

- varnostna načela in mehanizmi infrastrukture javnih ključev,
- delo s strojno in programsko opremo izdajatelja,
- opravljanje posebnih nalog, za katere so odgovorni in
- ukrepanje ob izrednih dogodkih in zagotavljanje neprekinjenega delovanja.

5.3.4. Pogostost dodatnih usposabljanj

Operativno osebje se usposablja glede na izkazane potrebe oziroma novosti v povezavi s korenskim izdajateljem SIMoD-CA-Root.

5.3.5. Kroženje med delovnimi mesti

Ni določeno.

5.3.6. Ukrepi ob kršitvah pooblastil

Proti operativni osebi, ki ne izvaja svojih nalog ali zlorabi pooblastila, se ukrepa skladno s predpisi.

5.3.7. Zunanji izvajalci

Zunanji izvajalci morajo izpolnjevati vse pogoje, določene v [10] ZTP, in varnostne zahteve korenskega izdajatelja SIMoD-CA-Root.

5.3.8. Dokumentacija za operativno osebje

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

5.4. Postopki varnostnih pregledov sistema

5.4.1. Vrste beleženih dogodkov

Korenski izdajatelj SIMoD-CA-Root beleži dogodke:

- na operacijskem sistemu, programski in strojni opremi,
- glede svojih ključev,
- glede ključev in digitalnih potrdili podrejenih izdajateljev,
- glede varnostne politike in upravljanja svojega informacijskega sistema.

Izdajatelj SIMoD-CA-Root beleži tudi podatke, ki vplivajo na varnost, niso pa del njegovega informacijskega sistema:

- dogodke glede fizičnega dostopa do sistemov izdajatelja in lokacije,
- kadrovske spremembe operativnega osebja izdajatelja SIMoD-CA-Root,
- zapise o uničenju občutljivega materiala, na primer kriptografskih ključev in nosilcev kriptografskih ključev.

5.4.2. Pogostost pregleda dnevnikov beleženih dogodkov

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

5.4.3. Obdobje hranjenja dnevnikov beleženih dogodkov

Najmanj sedem let v arhivu.

5.4.4. Zaščita dnevnikov beleženih dogodkov

Dnevniki beleženih dogodkov se hranijo na sistemu, na katerem nastanejo. Zaščiteni so z varnostnimi mehanizmi, ki zagotavljajo čim višjo raven varnosti.

Dostop do dnevnikov beleženih dogodkov je dovoljen le:

- operativnemu osebju v okviru delovnih nalog,
- izvajalcem nadzora in pregleda skladnosti.

5.4.5. Varnostne kopije dnevnikov beleženih dogodkov

Varnostne kopije dnevnikov beleženih dogodkov v elektronski obliki se ustvarjajo ob varnostnem kopiranju sistemov.

Periodično se en izvod varnostne kopije prenese na oddaljeno lokacijo.

5.4.6. Način zbiranja beleženih dogodkov

Zapisi o dogodkih se zbirajo samodejno, 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 izdajatelja SIMoD-CA-Root z namenom odkrivanja in odprave ranljivosti. Ugotovljena ranljivost se oceni s stališča verjetnosti povzročitve škode in predvidijo se ukrepi za zmanjšanje grožnje.

5.5. Arhiviranje podatkov

5.5.1. Vrste arhiviranih podatkov

Korenski izdajatelj SIMoD-CA-Root hrani naslednje podatke:

- dnevnike beleženih dogodkov iz podpoglavja 5.4.1 Vrste beleženih dogodkov,
- naloge za izdajo digitalnih potrdil podrejenih izdajateljev,
- korespondenco s subjekti, katerim je izdajatelj SIMoD-CA-Root izdal digitalno potrdilo,
- dokumentacijo o izvedbi postopkov izdaje digitalnih potrdil,
- sklenjene medsebojne dogovore in pogodbe,
- digitalna potrdila, registre preklicanih potrdil in registre preklicanih izdajateljev,
- svoja javna in zaupna pravila delovanja.

5.5.2. Obdobje hranjenja arhiva

Arhivirani podatki glede digitalnih potrdil in ključi se hranijo vsaj sedem let po preteku veljavnosti digitalnega potrdila, na katerega se podatek nanaša.

Drugi arhivirani podatki se hranijo vsaj sedem let po njihovem nastanku.

5.5.3. Zaščita arhiva

Nalogi za izdajo digitalnih potrdil, korespondenca s subjekti, katerim je izdajatelj SIMoD-CA-Root izdal digitalno potrdilo, dokumentacija o izvedbi postopka izdaje digitalnih potrdil, sklenjeni medsebojni dogovori in pogodbe ter pravila delovanja se hranijo in arhivirajo v skladu z internimi splošnimi akti, ki urejajo delo z dokumentarnim gradivom na MO.

Arhivirani podatki, ki se beležijo v okviru informacijskega sistema, kot so samodejno generirani dnevniki beleženih dogodkov, digitalna potrdila, registri preklicanih potrdil in registri preklicanih izdajateljev, se hranijo na vsaj dveh kopijah na ločenih lokacijah. Arhiv, ki se hrani na drugi lokaciji, je zaščiten z enakovrednimi varnostnimi mehanizmi, kot so v prostorih izdajatelja SIMoD-CA-Root.

5.5.4. Varnostna kopija arhiva

Podatkom iz prvega odstavka prejšnjega podpoglavja se zagotavlja razpoložljivost arhiva v skladu z internimi pravnimi akti, ki urejajo delo z dokumentarnim gradivom na MO.

Ob vzpostavitvi arhiva podatkov, ki se beležijo v okviru informacijskega sistema izdajatelja SIMoD-CA-Restricted, se ustvari varnostna kopija.

5.5.5. Časovno žigosanje zapisov

Ni določeno.

5.5.6. Način arhiviranja

Način zbiranja arhivskih podatkov je del zaupnih pravil SIMoD-CA-Root.

5.5.7. Postopek vpogleda v arhiv in njegova verifikacija

Dostop do arhiva je dovoljen le:

- operativnemu osebju izdajatelja SIMoD-CA-Root v okviru delovnih nalog in
- izvajalcem nadzora in pregleda skladnosti.

Ob kreiranju arhiva se preveri integriteta medija.

5.6. Zamenjava ključev korenskega izdajatelja SIMoD-CA-Root

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

Za podpisovanje digitalnih potrdil podrejenih izdajateljev se vedno uporablja najnovejši zasebni ključ korenskega izdajatelja SIMoD-CA-Root. Za preverjanje veljavnosti digitalnih potrdil podrejenih izdajateljev se uporablja predhodno potrdilo korenskega izdajatelja SIMoD-CA-Root do konca veljavnosti zadnjega digitalnega potrdila, podpisanega s pripadajočim zasebnim ključem. Zasebni ključ se vedno uporablja krajše obdobje, kot je veljavnost pripadajočega digitalnega potrdila.

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

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

5.7. Okrevalni načrt

5.7.1. Postopki ob okvarah in zlorabah

Postopki ob okvarah in zlorabah so del okrevalnega načrta, ki je del zaupnih pravil.

5.7.2. Uničenje programske ali strojne opreme oziroma podatkov izdajatelja

Ob okvari strojne ali programske opreme oziroma podatkov, pri kateri zasebni ključ izdajatelja SIMoD-CA-Root ni bil uničen, bodo storitve izdajatelja ponovno vzpostavljene v najkrajšem možnem času. Prioriteta je vzpostavitev funkcionalnosti preklica digitalnih potrdil in objavljanja

registra preklicanih izdajateljev. Skrajni rok je sedem dni. Po tem roku bo izdajatelj SIMoD-CA-Root ukrepal v skladu s podpoglavjem 4.9.3 Postopki za preklic.

Ob okvari, pri kateri pride do uničenja zasebnega ključa korenskega izdajatelja SIMoD-CA-Root in vseh njegovih kopij, se ravna, kot da je prišlo do zlorabe ključa v skladu s podpoglavjem 4.9.3 Postopki za preklic.

5.7.3. Zloraba zasebnega ključa izdajatelja SIMoD-CA-Root

Postopki ob zlorabi zasebnega ključa korenskega izdajatelja SIMoD-CA-Root so predpisani v podpoglavju 4.9.3 Postopki za preklic.

5.7.4. Zagotavljanje kontinuitete delovanja po nesrečah

Postopki ob naravnih in drugih nesrečah, ki imajo za posledico fizično uničenje ali varnostno vprašljivo delovanje programske ali strojne opreme, ogroženo celovitost podatkov oziroma uničenje in poškodovanje varovanih prostorov izdajatelja SIMoD-CA-Root, so del okrevalnega načrta, ki je del zaupnih pravil SIMoD-CA-Root.

5.8. Prenehanje delovanja korenskega izdajatelja SIMoD-CA-Root

Vzroki za prenehanje delovanja izdajatelja SIMoD-CA-Root so podani v podpoglavju 4.9.1 Okoliščine preklica.

Izdajatelj SIMoD-CA-Root bo po prenehanju delovanja izvedel postopke določene v podpoglavju 4.9.3 Postopki za preklic.

Ob prenehanju delovanja bo izdajatelj SIMoD-CA-Root kot del ponudnika storitev zaupanja na MO ukrepal v skladu z veljavno zakonodajo.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev para ključev

6.1.1. Generiranje para ključev

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

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

6.1.2. Dostava zasebnega ključa imetniku

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

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

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

6.1.4. Dostava izdajateljevega javnega ključa uporabnikom

Javni ključ oziroma digitalno potrdilo izdajatelja SIMoD-CA-Root in njegov odtis ter izpis vsebine ASN.1 strukture v berljivi obliki se izroči pooblaščeni osebi podrejenega izdajatelja na mediju hkrati z izdanim digitalnim potrdilom v postopku izdaje digitalnega potrdila podrejenega izdajatelja.

Digitalno potrdilo izdajatelja SIMoD-CA-Root je vedno mogoče pridobiti iz imenika, ob tem je potrebno preveriti istovetnost izdajatelja SIMoD-CA-Root in celovitost digitalnega potrdila.

6.1.5. Dolžina ključev

Dolžina RSA zasebnega ključa korenskega izdajatelja SIMoD-CA-Root mora biti najmanj 4096 bitov.

Dolžina RSA zasebnega ključa podrejenih izdajateljev mora biti najmanj 3072 bitov.

6.1.6. Parametri za generiranje javnih ključev in preverjanje parametrov

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

6.1.7. Namen uporabe ključev

Namen uporabe ključev je določen v razširitvenem polju *Key Usage* in *Extended Key Usage* po priporočilu [8] RFC 5280.

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

Dovoljeni vrednosti razširitvenega polja *Key Usage* za digitalna potrdila korenskega izdajatelja SIMoD-CA-Root in podrejene izdajatelje sta: *KeyCertSign* in *CRLSign*.

6.2. Zaščita zasebnih ključev in zahteve za kriptografske module

6.2.1. Standardi za kriptografski modul

Korenski izdajatelj SIMoD-CA-Root uporablja strojni varnostni kriptografski modul, ki ustreza varnostnemu tehničnemu standardu, določenemu v [4] ETSI EN 319 411-1.

6.2.2. Nadzor zasebnega ključa z več pooblaščenimi osebami

Za upravljanje zasebnega ključa korenskega izdajatelja SIMoD-CA-Root oziroma varnostnega kriptografskega modula 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 korenskega izdajatelja SIMoD-CA-Root ni dovoljeno. Tehnična izvedba varnostnega kriptografskega modula ne omogoča prikaza zasebnega ključa v nešifrirani obliki.

6.2.4. Varnostno kopiranje zasebnih ključev

Varnostna kopija zasebnega ključa korenskega izdajatelja SIMoD-CA-Root se zagotavlja z mehanizmi varnostnega kriptografskega modula. Datoteka z zasebnim ključem oziroma varnostna kopija se pred izvozom iz varnostnega kriptografskega modula šifrira. Dešifrirni ključ je porazdeljen na N od M administratorskih pametnih karticah ($N \geq 2$, $M \geq 3$, $M > N$).

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

6.2.5. Arhiviranje zasebnega ključa

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

6.2.6. Zapis zasebnega ključa v kriptografski modul in iz njega

Zasebni ključ korenskega izdajatelja SIMoD-CA-Root se generira v varnostnem kriptografskem modulu.

Zasebni ključ izdajatelja se kasneje lahko prenese v varnostni kriptografski modul tudi iz šifrirane datoteke z zasebnim ključem ob predložitvi N od M administratorskih pametnih kartic.

Izvoz zasebnega ključa iz varnega kriptografskega modula je onemogočen.

6.2.7. Hranjenje zasebnega ključev v kriptografskem modulu

Zasebni ključi korenskega izdajatelja SIMoD-CA-Root se hranijo v varnostnem kriptografskem modulu in v šifrirani datoteki. Zunaj modula se nikoli ne pojavijo v nešifrirani obliki.

6.2.8. Postopek za aktiviranje zasebnega ključa

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

6.2.9. Postopek za deaktiviranje zasebnega ključa

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

6.2.10. Postopek za uničenje zasebnega ključa

Zasebni ključi korenskega izdajatelja SIMoD-CA-Root se uničijo, ko jim poteče obdobje uporabe oziroma se ne uporabljajo več iz drugih razlogov. Uniči se aktivni ključ v varnostnem kriptografskem modulu in vse šifrirane datoteke z zasebnim ključem.

Fizično uničenje varnostnega kriptografskega modula ni predvideno. Ob prenehanju uporabe se ga inicializira oziroma povrne v tovarniško stanje.

Ko se operativna ali administratorska pametna kartica varnostnega kriptografskega modula preneha uporabljati, se jo inicializira oziroma povrne v tovarniško stanje. Če kartice ni mogoče povrniti v tovarniško stanje, se jo po prenehanju uporabe fizično uniči.

6.2.11. Stopnja varnosti kriptografskih modulov

Opisano v poglavju 6.2.1 Standardi za kriptografski modul.

6.3. Drugi vidiki upravljanja para ključev

6.3.1. Arhiviranje javnega ključa

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

6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil

Največja veljavnost digitalnega potrdila oziroma javnega in zasebnega ključa je:

- za korenskega izdajatelja SIMoD-CA-Root štiriindvajset let,
- za podrejene izdajatelje dvajset let oziroma do poteka veljavnosti digitalnega potrdila korenskega izdajatelja SIMoD-CA-Root.

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 oziroma za administratorske in operaterske kartice za upravljanje z modulom se določijo med inicializacijo varnostnega kriptografskega modula.

6.4.2. Zaščita gesel

Gesla se morajo hraniti na način, da se zagotavlja njihova tajnost.

6.4.3. Druge zahteve za gesla

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

6.5. Varnostne zahteve za računalnike

6.5.1. Specifične tehnične varnostne zahteve

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

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

6.5.2. Raven varnostne zaščite računalnikov

Informacijski sistem izdajatelja SIMoD-CA-Root izpolnjuje varnostni kriterij vsaj CC EAL4+.

Na nivoju operacijskega sistema izdajatelja SIMoD-CA-Root so za doseganje visoke ravni zaščite implementirani naslednji varnostni mehanizmi:

- nameščen je minimalen operacijski sistem, brez nepotrebnih funkcionalnosti,
- nameščeni so najnovejši varnostni popravki,
- tečejo le nujni procesi in servisi,
- nameščeni so le uporabniki, ki so potrebni za delovanje sistema,
- z nastavitvami pravic na datotečnem sistemu so neprivilegiranim uporabnikom onemogočeni nepooblaščeni dostopi.

6.6. Tehnični nadzor življenjskega cikla izdajatelja

6.6.1. Nadzor razvoja sistema

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

6.6.2. Upravljanje varnosti

Za programsko opremo korenskega izdajatelja SIMoD-CA-Root se da preveriti izvor in celovitost.

Informacijska in aplikativna oprema je konfigurirana tako, da so izpolnjene varnostne zahteve skladno s pravili SIMoD-CA-Root.

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

Če informacijski sistem to omogoča, se postopki oziroma nastavitve beležijo elektronsko, sicer pa ročno. Elektronsko beleženje med drugim dosežemo s ciljnim beleženjem dogodkov (npr. uporabo ukaza »script« na operacijskem sistemu unix, ki zabeleži vse vhodne in izhodne parametre), izpisi iz log datotek in izpisi konfiguracijskih datotek.

6.6.3. Upravljanje varnosti med življenjskim ciklom

Nadgradnje, nove verzije in popravki na informacijski opremi korenskega izdajatelja SIMoD-CA-Root, oziroma upravljanje varnosti se izvaja skozi celotno življenjski obdobje opreme.

Operativno osebje vzdržuje tehnično dokumentacijo korenskega izdajatelja SIMoD-CA-Root, ki obsega arhitekturo in tehnične lastnosti posameznih naprav.

Izvajajo se pregledi konfiguracij informacijske opreme in sicer po nadgradnji ali spremembi, za katero administrator izdajatelja SIMoD-CA-Root oceni, da je dovolj velika, da je potrebno izvesti pregled konfiguracije oziroma vsaj enkrat letno.

6.7. Varnostne kontrole na ravni računalniškega omrežja

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

6.8. Časovno žigosanje

Ni določeno.

7. PROFIL DIGITALNIH POTRDIL IN REGISTROV PREKLICANIH POTRDIL

7.1. Profil digitalnih potrdil

7.1.1. Verzija digitalnih potrdil

Korenski izdajatelj SIMoD-CA-Root izdaja digitalna potrdila X.509 verzije 3 v skladu s priporočilom [8] RFC 5280, ki vsebujejo naslednja osnovna polja:

Ime osnovnega polja / prevod ali opis	Vrednost polja v potrdilu korenskega izdajatelja SIMoD-CA-Root	Vrednost polja v potrdilu podrejenega izdajatelja
Version X.509 verzija	*3*	*3*
Serial Number serijska številka	enolična serijska številka na nivoju SIMoD-CA-Root	enolična serijska številka na nivoju SIMoD-CA-Root
Signature Algorithm algoritem za podpis	*sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11)*	*sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11)*
Issuer izdajatelj, razločevalno ime	*cn=simod-ca-root, ou=simod-pki, o=mors, c=si*	*cn=simod-ca-root, ou=simod-pki, o=mors, c=si*
Validity veljavnost potrdila	*Not Before:* začetek veljavnosti po GMT *Not After:* konec veljavnosti po GMT	*Not Before:* začetek veljavnosti po GMT *Not After:* konec veljavnosti po GMT
Subject imetnik, razločevalno ime	*cn=simod-ca-root, ou=simod-pki, o=mors, c=si*	razločevalno ime izdajatelja
Public Key Algorithm algoritem za javni ključ	*rsaEncryption (OID 1.2.840.113549.1.1.1)*	*rsaEncryption (OID 1.2.840.113549.1.1.1)*
Public Key Length *dolžina ključa*	minimalno *4096*	minimalno *3072*
Public Key podatki o imetnikovem javnem ključu	modul, eksponent, vrednost javnega ključa	modul, eksponent, vrednost javnega ključa

7.1.2. Razširitvena polja

Standardna razširitvena polja po priporočilu [8] RFC 5280, uporabljena v digitalnih potrdilih korenskega izdajatelja SIMoD-CA-Root in podrejenih izdajateljev:

Ime razširitvenega polja / prevod ali opis	Vrednost polja v potrdilu korenskega izdajatelja SIMoD-CA-Root	Vrednost polja v potrdilu podrejenega izdajatelja
Authority Key Identifier odtis javnega ključa izdajatelja	ni uporabljeno	SHA256 odtis javnega ključa izdajatelja SIMoD-CA-Root, s katerim je podpisano potrdilo
Subject Key Identifier odtis imetnikovega javnega ključa	SHA256 odtis javnega ključa izdajatelja SIMoD-CA-Root	SHA256 odtis javnega ključa izdajatelja
Key Usage namen uporabe ključa	**Kritično** *keyCertSign* *cRLSign*	**Kritično** *keyCertSign* *cRLSign*

CRL Distribution Points DN, LDAP in http naslovi registra preklicanih potrdil korenskega izdajatelja SIMoD-CA-Root	ni uporabljeno	DN: *cn=CRL1,* *cn=simod-ca-root* *ou=simod-pki,* *o=mors,* *c=si* URL: *ldap://imenik.simod-pki.mors.si/cn=WinCombined2,cn=simod-ca-root,ou=simod-pki,o=mors,c=si?certificateRevocationList* *http://www.simod-pki.mors.si/crl/simod-ca-root2.crl*
Basic Constraints osnovne omejitve	**Kritično** *cA =: True* *pathLenConstraint = undefined*	**Kritično** *cA =: True* *pathLenConstraint = undefined*

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

7.1.3. Identifikacijske oznake algoritmov

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

Algoritem	Identifikacijska oznaka
rsaEncryption	1.2.840.113549.1.1.1
sha256WithRSAEncryption	1.2.840.113549.1.1.11

7.1.4. Oblike imen

Predpisano v podpoglavju 3.1.1 Oblika imen.

7.1.5. Omejitve imen

Korenski izdajatelj SIMoD-CA-Root ne predpisuje načina uporabe polja *nameConstraints*.

7.1.6. Identifikacijske oznake politik

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

7.1.7. Način uporabe razširitvenega polja za omejitev uporabe politik

Omejitve uporabe politik niso predpisane. Uporaba razširitvenega polja *policyConstrains* v potrdilu o priznavanju drugega izdajatelja se določi ob medsebojnem priznavanju.

7.1.8. Posebni podatki o politiki

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

7.1.9. Procesiranje oznake kritičnosti razširitvenih polj

Uporabniške aplikacije morajo procesirati razširitvena polja, označena kot kritična, v skladu s priporočili [8] RFC 5280.

7.2. Profil registrov preklicanih potrdil

7.2.1. Verzija registrov preklicanih potrdil

Korenski izdajatelj SIMoD-CA-Root izdaja registre preklicanih potrdil verzije 2 v skladu s priporočilom [8] RFC 5280, ki vsebujejo naslednja osnovna polja:

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

7.2.2. Razširitvena polja registrov preklicanih potrdil

Korenski izdajatelj SIMoD-CA-Root izdaja registre preklicanih potrdil verzije 2 v skladu s priporočilom [8] RFC 5280, ki vsebujejo naslednja standardna razširitvena polja:

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

7.3. Profil sprotnega preverjanja statusa potrdil

7.3.1. Verzija sprotnega preverjanja statusa digitalnih potrdil

Ni relevantno. Na nivoju korenskega izdajatelja storitev sprotnega preverjanja statusa digitalnih potrdil ni implementirana.

7.3.2. Razširitve sprotnega preverjanja statusa digitalnih potrdil

Ni relevantno.

8. PREVERJANJE SKLADNOSTI IN OSTALE OBLIKE NADZORA

8.1. Pogostost preverjanja skladnosti

Pogostost preverjanja skladnosti in druge oblike nadzora so določene z veljavnimi predpisi.

8.2. Pogoji za izvajalca preverjanja skladnosti

Preverjanje skladnosti z veljavnimi predpisi in druge oblike nadzora vključno s pogoji za izvajalce so določeni z veljavnimi predpisi.

8.3. Neodvisnost izvajalca preverjanja skladnosti

Presojevalec skladnosti oziroma izvajalec preverjanja skladnosti mora biti neodvisen od ponudnika storitev zaupanja na MO.

8.4. Področja preverjanja skladnosti

Preverja se skladnost delovanja ponudnika storitev zaupanja z veljavno zakonodajo, politiko SIMoD-PKI in pravili delovanja izdajatelja.

8.5. Postopki po opravljenem pregledu skladnosti

Postopki po opravljeni presoji skladnosti so v skladu s predpisi.

Ob ugotovljenih nepravilnostih mora ponudnik storitev zaupanja na MO pripraviti načrt za odpravo pomanjkljivosti in poročilo o odpravi pomanjkljivosti.

8.6. Prejemniki ugotovitev o pregledu skladnosti

Predstojnik organizacijske enote, pristojne za informatiko, odloči, ali je o ugotovitvah pregleda skladnosti potrebno obvestiti imetnike digitalnih potrdil in druge udeležence.

9. OSTALE POSLOVNE IN PRAVNE ZADEVE

9.1. Cenik

Ni določeno.

9.2. Finančna odgovornost

Skladno s predpisi.

9.3. Zaupnost poslovnih informacij

Skladno s predpisi.

9.4. Zaupnost osebnih podatkov

Skladno s predpisi.

9.5. Zaščita intelektualne lastnine

Skladno s predpisi.

9.6. Odgovornosti in jamstva

9.6.1. Odgovornosti in jamstva izdajatelja SIMoD-CA-Root

Korenski izdajatelj SIMoD-CA-Root jamči, da deluje v skladu s politiko SIMoD-PKI in pravili SIMoD-CA-Root.

Vodja organizacijske enote, pristojne za informatiko in komunikacije, predstavlja izdajatelja SIMoD-CA-Root in jamči za izpolnjevanje njegovih obveznosti.

9.6.2. Odgovornosti in jamstva prijavne službe

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

Kolegij organizacijske enote, pristojne za informatiko in komunikacije, je odgovoren za ustreznost identifikacijskih postopkov in točnost podatkov v okviru delovanja korenskega izdajatelja SIMoD-CA-Root.

9.6.3. Odgovornosti in jamstva imetnikov digitalnih potrdil

Podrejeni izdajatelj jamči, da deluje v skladu s politiko SIMoD-PKI, pravili delovanja SIMoD-CA-Root in svojimi pravili delovanja.

Predstojnik organizacijske enote predstavlja, odgovarja in jamči za podrejenega izdajatelja, ki deluje v okviru njegove organizacijske enote.

9.6.4. Odgovornost in jamstva tretjih oseb

Tretja oseba, ki se zanaša na digitalna potrdila izdajatelja SIMoD-CA-Root, jamči, da uporablja digitalna potrdila le za namene, določene v politiki SIMoD-PKI in pravilih SIMoD-CA-Root.

Obveznosti tretjih oseb glede uporabe digitalnih potrdil so opisane v podpoglavju 4.5.2 Uporaba digitalnih potrdil s strani tretjih oseb.

9.6.5. Odgovornost in jamstva drugih udeležencev

Ni predpisano.

9.7. Zanikanje odgovornosti

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

Korenski izdajatelj SIMoD-CA-Root ni odgovoren za škodo, ki bi lahko nastala zaradi višje sile.

9.8. Omejitve odgovornosti

Skladno s predpisi.

9.9. Poravnava škode

Skladno s predpisi.

9.10. Začetek in prenehanje veljavnosti

9.10.1. Začetek veljavnosti

Nova verzija pravil SIMoD-CA-Root se objavi na spletni strani http://www.simod-pki.mors.si

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

9.10.2. Prenehanje veljavnosti

Veljavnost pravil SIMoD-CA-Root ni časovna omejena oziroma veljajo do uveljavitve nove verzije.

9.10.3. Posledice prenehanja veljavnosti

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

9.11. Obvestila in komuniciranje z udeleženci

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

9.12. Spreminjanje dokumenta

9.12.1. Postopek uveljavitve spremembe

V skladu s podpoglavjem 1.5. Upravljanje s pravili SIMoD-CA-Root.

9.12.2. Postopek in roki obveščanja

V skladu s podpoglavjem 9.11. Obvestila in komuniciranje z udeleženci.

9.12.3. Spremembe, ki zahtevajo novo identifikacijsko oznako politike

Ni relevantno.

9.13. Reševanje sporov

V skladu s predpisi.

9.14. Predpisi in priporočila

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

[1]	eIDAS	Uredba (EU) št. 910/2014 Evropskega parlamenta in sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (Uradni list EU, št. L 257/83 z dne 28.8.2014)
[2]	ETSI ES 319 401	Electronic Signatures and Infrastructures (ESI); General Policy requirements for Trust Service Providers
[3]	ETSI EN 319 411	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Provider issuing certificates:
[4]	ETSI EN 319 411-1	Part 1: General requirements
[5]	ETSI EN 319 411-2	Part 2: Requirements for trust service providers issuing EU qualified certificates
[6]	Politika SIMoD-PKI	Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, Verzija 3.1
[7]	RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[8]	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[9]	ZObr	Zakon o obrambi (Uradni list RS, št. 103/04 – UPB1, 95/15 in 139/20)
[10]	ZTP	Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – UPB2, 9/10, 60/11 in 8/20)
[11]	ZVOP-1	Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – UPB1, 177/20)

Delovanje korenskega izdajatelja SIMoD-CA-Root opredeljujejo še naslednji dokumenti:

A.1. Načrt varovanja tajnih podatkov v prostorih Centralnega registra NATO/EU

A.2. Postopkovnik o hranjenju varnostno občutljivega materiala v infrastrukturi javnih ključev na MO

A.3. Postopek tvorjenja prvega para ključev overitelja SIMoD-CA-Root

A.4. Postopkovnik obnove ključev overitelja SIMoD-CA-Root

A.5. Postopkovnik o tehnični arhitekturi SIMoD-PKI

A.6. Postopkovnik o izdelavi varnostnih kopij strežnikov infrastrukture SIMoD-PKI

A.7. Pravila delovanja izdajatelja SIMoD-CA-Root, zaupni del