REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Podpisnik: Sterle Viktor 2450239
Izdajatelj: simod-ca-restricted
Številka certifikata: 5ABD4C66
Potek veljavnosti: 08. 03. 2024
Čas podpisa: 06. 06. 2022 14:00
Št. dokumenta: 386-21/2022-86

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Pravila delovanja izdajatelja SIMoD-CA-Restricted, javni del

(javna pravila SIMoD-CA-Restricted)

Verzija 3.1

Zgodovina sprememb Pravil delovanja izdajatelja SIMoD-CA-Restricted, javni del:

Izdaja:	Spremembe glede na prejšnjo izdajo:
Pravila delovanja izdajatelja SIMoD-CA-Restricted, javni del, ver. 3.1	Ukinjen je Svet za upravljanje z infrastrukturo javnih ključev na MO. Prenehanje izdajanja kvalificiranih potrdil. Uskladitev izrazov; nadomestitev izrazov »overitelj« in »infrastruktura javnih ključev« z izrazom »ponudnik storitev zaupanja«. Odstranjeno je navajanje obveznosti v povezavi z Uredbo eIDAS. Uredniški popravki.
Pravila o spremembi in dopolnitvah Pravil delovanja izdajatelja SIMoD-CA-Restricted, javni del, ver. 3.0, številka: 386-12/2018-16, 28.03.2018	Dodan je imetnik digitalnega potrdila sistem za podpis programske kode. Svetu za upravljanje z infrastrukturo javnih ključev na MO so dodane obveznosti v povezavi z Uredbo eIDAS. Dodana je obveza pregledovanja pravil SIMoD-CA-Restricted in ostalih dokumentov, povezanih z delovanjem izdajatelja SIMoD-CA-Restricted. Dodana je obveza izvajanja vdornih testov in testov ranljivosti. Dodane so določbe glede preverjanja skladnosti oziroma nadzora.
Pravila delovanja izdajatelja SIMoD-CA-Restricted, javni del, ver. 3.0, številka: 386-12/2017-41, 03.05.2017	Uskladitev z Uredbo eIDAS in s spremembami priporočil ETSI. Uskladitev izrazov; konsistentna uporaba izrazov »overitelj« in »izdajatelj«. Ukinjena je možnost izdaje digitalnega potrdila po preklicu v izjemnih primerih brez identifikacije v prijavni službi. Ukinjena je omejitev ponovne izdaje digitalnih potrdil brez preverjanja istovetnosti maksimalno dvakrat zaporedoma. Veljavnost digitalnega potrdila in ključev izdajatelja SIMoD-CA-Restricted je povečana na dvajset let. Podaljšanje obdobja veljavnosti digitalnih potrdil in ključev.
Pravila o spremembah in dopolnitvah Pravil delovanja overitelja SIMoD-CA-Restricted, javni del, ver. 2.0, številka: 386-11/2014-23, 07.02.2014	Izenačena je veljavnost zasebnega in javnega ključa v digitalnem potrdilu overitelja SIMoD-CA-Restricted. Prenehanje uporabe algoritma SHA-1 in začetek uporabe algoritma SHA256.

Pravila o dopolnitvah in spremembah Pravil delovanja overitelja SIMoD-CA-Restricted, javni del, ver. 2.0, številka: 386-6/2011-336, 21.12.2011	Poenostavljen je postopek oddaje zahtevka za preklic digitalnega potrdila. Uvedena je možnost ponovne izdaje digitalnega potrdila v izjemnem primeru, ko prijavna služba ne deluje. Odstranjena so določila, ki se nanašajo na korenskega overitelja SIMoD-CA-Root.
Pravila delovanja overitelja SIMoD-CA-Restricted, javni del, ver. 2.0, številka: 382-5/2006-121, 23.11.2010	Pristojnost sprejemanja Pravil delovanja overitelja SIMoD-CA-Restricted je prenešena na Svet za upravljanje z infrastrukturo javnih ključev na MO. Spremenjeno je pravilo za določanje identifikacijskih oznak politik digitalnih potrdil. Dokument nima več identifikacijske oznake, Razširjen je nabor imetnikov potrdil z organizacijskimi in funkcijskimi vlogami. Vpeljana so kvalificirana digitalna potrdila v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu in priporočili ETSI. Dodana je NIZKA stopnja zaupanja v digitalno potrdilo. Predpisani so postopki za izdajo digitalnih potrdil z obvezno uporabo pametne kartice, kjer overitelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici. Predvidena je možnost ponovne izdaje digitalnega potrdila z uporabo PKCS#10 protokola brez osebnega preverjanja istovetnosti imetnika, če je elektronski zahtevek za ponovno izdajo podpisan z veljavnim digitalnim potrdilom.
Spremembe in dopolnitve Pravil delovanja overitelja SIMoD-CA-Restricted, javni del, številka: 382-5/2006-44, 27.12.2007	Spremenjeno je pravilo za določanje identifikacijske oznake dokumenta. Dopolnjena so določila glede razločevalnega imena imetnika. Dopolnjena so določila glede interpretacije imen. V postopku izdaje digitalnega potrdila je operativnemu osebju dodana obveza preverjanja pravilnosti naslova elektronske pošte bodočega imetnika.
Pravila delovanja overitelja SIMoD-CA-Restricted, javni del, šifra: 382-5/2006-13, 17.7.2006	V infrastrukturo javnih ključev na MO je umeščen korenski overitelj SIMoD-CA-Root in podrejeni overitelji.
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-Restricted
JAVNI DEL

(javna pravila SIMoD-CA-Restricted)

Verzija 3.1

1. UVOD

1.1. Pregled

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

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

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

Politika SIMoD-PKI predpisuje 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.

Izdajatelj SIMoD-CA-Restricted (ang. **S**lovenian **M**inistry **o**f **D**efence **Restricted C**ertification **A**uthority) je podrejeni izdajatelj korenskega izdajatelja SIMoD-CA-Root.

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

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

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

Javna pravila SIMoD-CA-Restricted podajajo opis infrastrukture in postopkov izdajatelja ter izpolnjevanje zahtev politike SIMoD-PKI. Za oceno zaupanja v SIMoD-PKI kot celoto je potrebno poleg tega dokumenta upoštevati še dokumenta [13] politika SIMoD-PKI in [14] pravila SIMoD-CA-Root.

Izdajatelj SIMoD-CA-Restricted izdaja digitalna potrdila za zagotavljanje naslednjih varnostnih storitev:

- digitalno podpisovanje podatkov,
- zagotavljanje zaupnosti pri hranjenju in prenosu podatkov,
- selektivno omejevanje dostopa do podatkov,
- zagotavljanje celovitosti podatkov,
- prepoznavanje in preverjanje istovetnosti oseb ter gradnikov informacijske infrastrukture, kot so strežniki, usmerjevalniki, požarne pregrade in imeniki,
- nezanikanje oddaje ali sprejema sporočil in
- ustvarjanje časovnih žigov in druge storitve overjanja.

Dokument je skladen z [15] 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

Izdajatelj SIMoD-CA-Restricted izdaja digitalna potrdila z naslednjimi identifikacijskimi oznakami politik (ang. Policy Object Identifier, Policy OID):

Imetniki	Namen uporabe digitalnega potrdila	Stopnja zaupanja	Identifikacijske oznake politik
Fizične osebe	preverjanje e-podpisa	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.1.2
	šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.2.2
	preverjanje e-podpisa in šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.3.2
	preverjanje e-podpisa	SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.1.1.2
	šifriranje	SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.1.2.2
	preverjanje e-podpisa in šifriranje	SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.1.3.2
	preverjanje e-podpisa	NIZKA	1.3.6.1.4.1.22295.10.1.2.2.1.1.2
	šifriranje	NIZKA	1.3.6.1.4.1.22295.10.1.2.2.1.2.2
	preverjanje e-podpisa in šifriranje	NIZKA	1.3.6.1.4.1.22295.10.1.2.2.1.3.2
Splošni nazivi (org. enote, funkcijske in organizacijske vloge	preverjanje e-žiga in šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.3.3.2
		SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.3.3.2
		NIZKA	1.3.6.1.4.1.22295.10.1.2.2.3.3.2
Strežniki, druga strojna in programska oprema	preverjanje e-podpisa in šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.4.3.2
		SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.4.3.2
		NIZKA	1.3.6.1.4.1.22295.10.1.2.2.4.3.2
Izdajatelji časovnih žigov	overjanje časovnih žigov	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.5.4.2
Sistemi za preverjanje veljavnosti digitalnih potrdil (OCSP)	overjanje odzivov OCSP	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.6.5.2
Sistemi za podpis programske kode	preverjanje e-podpisa programske kode	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.7.6.2
		SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.7.6.2
		NIZKA	1.3.6.1.4.1.22295.10.1.2.2.7.6.2

1.3. Udeleženci infrastrukture javnih ključev

1.3.1. Izdajatelj SIMoD-CA-Restricted

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

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

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

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

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

Prijavna služba sprejema zahtevke in preverja točnost podatkov naročnikov digitalnih potrdil. Naloge prijavne službe opravlja organizacijska enota MO, pristojna za kadrovske zadeve.

1.3.3. Imetniki digitalnih potrdil

Imetniki digitalnih potrdil izdajatelja SIMoD-CA-Restricted so:

- fizične osebe - zaposleni na MO,
- organizacijske enote in organi v sestavi MO (v nadaljevanju: organizacijske enote MO),
- funkcijske in organizacijske vloge,
- strežniki in druga strojna ter programska oprema,
- izdajatelji časovnih žigov, sistemi za preverjanje veljavnosti digitalnih potrdil in druge storitve overjanja.

Odgovorna oseba za digitalno potrdilo glede na imetnika potrdila je:

- za organizacijske enote MO vodja organizacijske enote MO,
- za funkcijske ali organizacijske vloge nosilec, skrbnik ali administrator vloge,
- za strežnike in drugo strojno ter programsko opremo skrbnik strežnika, druge strojne ali programske opreme,
- za izdajatelje časovnih žigov, sisteme za preverjanje veljavnosti potrdil in druge storitve overjanja vodja organizacijske enote, ki upravlja storitev.

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-Restricted in korenskega izdajatelja SIMoD-CA-Root.

1.3.5. Posredno odgovorni organi

Izdajatelj SIMoD-CA-Restricted 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 ter nadzor KIS MO.

1.4. Namen uporabe digitalnih potrdil

1.4.1. Dovoljena uporaba digitalnih potrdil

Namen uporabe digitalnih potrdil je določen z namenom uporabe pripadajočih ključev:

Namen uporabe javnega ključa oziroma digitalnega potrdila	Namen uporabe zasebnega ključa
preverjanje e-podpisa	podpisovanje
šifriranje	dešifriranje
preverjanje e-podpisa / e-žiga in šifriranje	podpisovanje in dešifriranje
overjanje časovnih žigov	podpisovanje časovnih žigov
overjanje odzivov OSCP	podpisovanje odzivov OCSP
preverjanje e-podpisa programske kode	podpisovanje programske kode

Izdajatelj SIMoD-CA-Restricted glede na možnost upravljanja loči dva tipa digitalnih potrdil, ki jih izdaja v naslednjih kombinacijah:

upravljana digitalna potrdila (imenovana tudi *Entrust ID*)	
skupek dveh digitalnih potrdil	digitalno potrdilo za preverjanje e-podpisa
	digitalno potrdilo za šifriranje
eno digitalno potrdilo	digitalno potrdilo za preverjanje e-podpisa in šifriranje (z dvojno uporabo)
neupravljana digitalna potrdila (imenovana tudi spletna, *WEB*)	
eno digitalno potrdilo	digitalno potrdilo za preverjanje e-podpisa / e-žiga in šifriranje (z dvojno uporabo)

Izdajatelj SIMoD-CA-Restricted izdaja digitalna potrdila naslednjih stopenj zaupanja:

Pogoj:			
Ob prvi registraciji obvezno preverjanje identitete v prijavni službi	DA	DA	NE
Obvezna uporaba sredstva za varno hrambo zasebnih ključev oziroma ustvarjanje e-podpisa / e-žiga v strojni obliki	DA	NE	NE
Stopnja zaupanja:	VISOKA	SREDNJA	NIZKA

Smernice za uporabo digitalnih potrdil različnih stopenj zaupanja za implementacijo varnostnih storitev so podane v politiki SIMoD-PKI.

Digitalna potrdila se morajo uporabljati v skladu s politiko SIMoD-PKI in pravili izdajatelja SIMoD-CA-Restricted.

1.4.2. Nedovoljena uporaba digitalnih potrdil

Ni določb.

1.5. Upravljanje s pravili SIMoD-CA-Restricted

1.5.1. Organ, ki upravlja ta dokument

Organizacijska enote, pristojna za informatiko, vodi postopek izdelave pravil SIMoD-CA-Restricted.

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

1.5.2. Kontaktni podatki

Glej podpoglavje 1.3.1 Izdajatelj SIMoD-CA-Restricted.

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

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

1.5.4. Postopek odobritve pravil SIMoD-CA-Restricted

Kolegij organizacijske enote, pristojne za informatiko:

- preveri skladnost pravil SIMoD-CA-Restricted s politiko SIMoD-PKI in
- vodi postopek potrditve pravil SIMoD-CA-Restricted.

Pravila SIMoD-CA-Restricted sprejme vodja organizacijske enote, pristojne za informatiko.

1.6. Pojmi in kratice

Pojem	Definicija
Časovni žig	Podatki v elektronski obliki, ki druge podatke v elektronski obliki povezujejo z določenim trenutkom in tako zagotavljajo dokaz, da so slednji podatki v tistem trenutku obstajali.
Digitalno potrdilo	Potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z imetnikom potrdila.
Digitalno potrdilo izdajatelja časovnih žigov	Digitalno potrdilo, s katerim izdajatelj časovnih žigov izdaja časovne žige.
Digitalno potrdilo za preverjanje podpisa	Digitalno potrdilo, ki se uporablja za verifikacijo elektronskega podpisa in preverjanje celovitosti podatkov v elektronski obliki. V tem dokumentu uporabljen kot enakovreden 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.
Elektronsko sporočilo	Niz podatkov, ki so poslani ali prejeti na elektronski način, kar vključuje predvsem elektronsko izmenjavo podatkov in elektronsko pošto.
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 lastnosti in pripadajočimi vrednostmi. Imenik, ki vsebuje digitalna potrdila, je navadno v skladu s standardom X.500 oz. 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 oz. 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 oz. Priloge III [1] eIDAS.
Naprava	V tem dokumentu izraz za strežnik, drugo strojno ali programsko opremo, izdajatelja časovnih žigov, sistem za preverjanje veljavnosti digitalnih potrdil ali drugega ponudnika storitev overjanja.
Naprava za ustvarjanje elektronskega podpisa	Po definiciji 22. odstavka 3. člena [1] eIDAS konfigurirana programska in strojna oprema, ki se uporablja za ustvarjanje elektronskega podpisa.
Naprava za ustvarjanje kvalificiranega elektronskega podpisa	Po definiciji 23. odstavka 3. člena [1] eIDAS naprava za ustvarjanje elektronskega podpisa, ki izpolnjuje zahteve iz Priloge II [1] eIDAS.
Politika digitalnih potrdil	Nabor pravil, ki posledično definira uporabnost digitalnih potrdil v določeni skupini uporabnikov in/ali za določen nabor aplikacij s skupnimi varnostnimi zahtevami.
Ponudnik storitev zaupanja	Po definiciji 19. odstavka 3. člena [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«.
Potrdilo za elektronski žig	Po definiciji 29. odstavka 3. člena [1] eIDAS: elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega žiga s pravno osebo in potrjuje ime te osebe.
Prijavna služba	Služba oziroma organizacija, ki po pooblastilu izdajatelja sprejema zahtevke in preverja istovetnosti bodočih imetnikov.
Splošni naziv	V tem dokumentu izraz, ki skupno označuje naziv organizacijske enote MO, funkcijske in organizacijske vloge.
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.
Zasebni ključ	Ključ iz para ključev, ki mora ostati skriven, da se zagotovi zaupnost in celovitost podatkov v elektronski obliki.
Zloraba	Razkritje tajnega podatka, izguba celovitosti ali razpoložljivosti podatka.

Kratica	Opis
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)
FIPS	Standardi za informacijske tehnologije, ki se uporabljajo v ameriških zveznih usatnovah. 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, ki pripravlja priporočila (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)
LDAP	Protokol, ki določa dostop do imenika po priporočilu IETF RFC 1777 (ang. Leightweight Directory Access Protocol)

OCSP	Storitev sprotnega preverjanja statusa digitalnih potrdil (ang. On-line Certificate Status Protocol)
PKCS	Priporočila podjetja RSA Security za uporabo asimetričnih kriptografskih algoritmov (ang. Public Key Cryptographic Standards)
PKCS#1	Osnovna pravila za formatiranje podatkov ob implementaciji RSA funkcij. Predpisujejo, kako se izračuna elektronski podpis in kako se formatirajo podatki, ki se podpisujejo, ter format podpisa. Predpisujejo tudi sintakso javnega in zasebnega RSA ključa
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.
QSCD	Naprava za ustvarjanje kvalificiranega elektronskega podpisa (ang. Qualified Signature/Seal Creation Device); [5] ETSI EN 319 411-2
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-Restricted	Izdajatelj SIMoD-CA-Restricted (ang. **S**lovenian **M**inistry **o**f **D**efence **Restricted** **C**ertification **A**uthority)
SIMoD-CA-Root	Korenski izdajatelj ponudnika storitev zaupanja na MO (ang. **S**loven**i**an **M**inistry **o**f **D**efence **C**ertificate **A**uthority **Root**)
SIMoD-PKI	Infrastruktura javnih ključev Ministrstva za obrambo Republike Slovenije (ang. **S**loven**i**an **M**inistry **o**f **D**efence **P**ublic **K**ey **I**nfrastructure - SIMoD-PKI)
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-Restricted:

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

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

- digitalna potrdila imetnikov,
- registre preklicanih potrdil (ang. Certificate Revocation List, CRL)
    - delne registre in
    - kombinirani register.

Digitalna potrdila so objavljena v imeniku v spodaj navedenih poddrevesih, glede na tip imetnika digitalnega potrdila:

Poddrevo v imeniku:	Digitalno potrdilo glede na tip imetnika:
ou=cert-osebe-<X>, organizationIdentifier=VATSI-47978457, o=Ministrstvo za obrambo, c=SI	fizične osebe
ou=cert-splosno-<X>, organizationIdentifier =VATSI-47978457, o=Ministrstvo za obrambo, c=SI	• organizacijske enote oz. splošni nazivi • funkcijske in organizacijske vloge
ou=cert-naprave-<X>, organizationIdentifier =VATSI-47978457, o=Ministrstvo za obrambo, c=SI	• strežniki in druga strojna ter programska oprema • izdajatelji časovnih žigov in drugi ponudniki storitev overjanja • strežniki OCSP
ou=simod-pki,o=mors,c=si	izdajatelji digitalnih potrdil

Vrednost <X> je:

- »A« za upravljana potrdila in
- »B« za neupravljana (spletna) potrdila.

Registri preklicanih potrdil so v imeniku objavljeni v naslednjih vozliščih v atributu certificateRevocationList:

- deljeni registri so v cn=CRL*n*,cn=simod-ca-restricted,ou=simod-pki,o=mors,c=si, kjer je *n* 1, 2,...,
- kobinirani register je v cn=simod-ca-restricted,ou=simod-pki,o=mors,c=si.

Kombinirani register preklicanih potrdil je na primarnem in zrcalnem spletnem strežniku dostopen tudi po protokolu HTTP na naslovu http://www.simod-pki.mors.si/crl/simod-ca-restricted.crl.

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-Restricted, zaupni del, niso javno objavljena.

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

3. PREPOZNAVANJE IN PREVERJANJE ISTOVETNOSTI

3.1. Določanje imen

3.1.1. Oblika imen

Podatki o izdajatelju in imetniku digitalnega potrdila so v digitalnem potrdilu zapisani v obliki razločevalnega imena, in sicer v skladu s priporočili [16] RFC 5280, [8] ETSI EN 319 412-2, [9] ETSI EN 319 412-3 ter [10] ETSI EN 319 412-4.

Digitalno potrdilo vsebuje polje *Subject* z edinstvenim razločevalnim imenom imetnika.

Razločevalno ime (ang. Distinguished Name, DN) izdajatelja je cn=SIMoD-CA-Restricted,ou=simod-pki,o=mors,c=si in je shranjeno v polju *Issuer*.

Razločevalno ime imetnika je v polje *Subject* zapisano v obliki X.501 UTF8String.

Razločevalno ime je sestavljeno iz dveh delov:
- kratkega razločevalnega imena (ang. Relative Distinguished Name, RDN) in
- ostanka razločevalnega imena.

Celotno razločevalno ime je tako oblike:
DN = RDN, ostanek

V tabeli so različne oblike razločevalnega imena, glede na vrsto imetnika:

Imetnika	RDN	ostanek
fizične oseba	cn=<splošno ime> + givenName=<ime> + sn=<priimek>	ou=cert-osebe-<X>, organizationIdentifier=VATSI-47978457, o=Ministrstvo za obrambo, c=SI
splošni naziv	cn=<splošno ime> + description=<opis>	ou=cert-splosno-<X>, organizationIdentifier=VATSI-47978457, o=Ministrstvo za obrambo, c=SI
naprava	cn=<splošno ime>	ou=cert-naprave-<X>, organizationIdentifier=VATSI-47978457, o=Ministrstvo za obrambo, c=SI

Vrednost <X> je:
- »A« za upravljana potrdila in
- »B« za neupravljana (spletna) potrdila.

V vrednosti polja za *splošno ime* (ang. common name, cn) se nacionalni simboli ne uporabljajo, pač pa le črke iz angleške abecede. Vrednost polj *givenName*, *sn* in *description*, ki natančneje opisujejo imetnika digitalnega potrdila, pa lahko vsebuje nacionalne simbole.

Polje *cn* pri fizičnih osebah oziroma parameter <*splošno ime*> ima obliko »Priimek Ime *Številka*«, kjer *Številka* zagotavlja enoličnost razločevalnega imena in je:
- številka delavca iz kadrovske evidence pri zaposlenih osebah in
- številka objekta iz centralnega imenika pri ostalih osebah.

Imetnik ima lahko tudi eno ali več alternativnih imen, ki so zapisana v razširitvenem polju *subjectAltName*. Tip alternativnega imena je običajno:
- *rfc822Name*; vrednost polja je naslov elektronske pošte ali
- *DNS Name*; vrednost je domensko ime strežnika ali naprave.

Podrobnosti o konverziji nacionalnih simbolov v polju *cn* in določanju alternativnega imena so v zaupnih pravilih SIMoD-CA-Restricted.

3.1.2. Potreba po smiselnosti imen

Predlog za splošno ime (polje *cn*, ang. common name) je del zahtevka za izdajo digitalnega potrdila. Prijavna služba in operativno osebje SIMoD-CA-Restricted si pridržujeta pravico za zavrnitev imena. V tem primeru predlagata drugačno ime.

Splošno ime v digitalnih potrdilih mora enolično in nedvoumno označevati imetnika.

Splošno ime v digitalnih potrdilih za fizične osebe vsebuje priimek in ime osebe ter številko zaposlenega iz kadrovske evidence.

Splošno ime v digitalnih potrdilih za naprave praviloma vsebuje polno domensko ime naprave.

3.1.3. Anonimnost imetnikov in uporaba psevdonimov

Uporaba psevdonimov ni dovoljena. Izdajatelj SIMoD-CA-Restricted 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 enolično označuje imetnika potrdila.

Pri fizičnih osebah se edinstvenost zagotavlja s številko zaposlenega, ki je del splošnega imena.

Pri splošnih nazivih je v imenu praviloma serijska številka entitete v imeniškem sistemu MO.

Pri napravah je že polno domensko ime naprave, ki je v splošnem imenu, enolično.

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

Dokazovanje lastništva zasebnega ključa, ki pripada javnemu ključu v digitalnemu potrdilu, se zagotavlja z varnimi postopki pred prevzemom digitalnega potrdila in ob njem, kot sta:

- RFC 4210 PKIX-CMP,
- PKCS#10 Certification Request Syntax Standard.

3.2.2. Preverjanje istovetnosti za imetnike, ki niso fizične osebe

Zahtevek za pridobitev digitalnega potrdila za splošni naziv za organizacijsko enoto MO mora vsebovati uradni naziv organizacijske enote MO in podatke o odgovorni osebi, to je vodji organizacijske enote MO.

Zahtevek za pridobitev digitalnega potrdila za splošni naziv za funkcijsko ali organizacijsko vlogo mora vsebovati podatke o vlogi, odgovorni osebi, to je nosilcu, skrbniku ali administratorju vloge ter vodji organizacijske enote MO.

Zahtevek za pridobitev digitalnega potrdila za naprave, to je strežnike, drugo strojno in programsko opremo, izdajatelje časovnih žigov, sisteme za preverjanje veljavnosti digitalnih potrdil ter druge storitve overjanja, mora vsebovati podatke o napravi oziroma storitvi, odgovorni osebi, to je skrbniku naprave oziroma storitve in vodji organizacijske enote MO.

Za pravilnost podatkov na zahtevkih jamči vodja organizacijske enote MO.

Za digitalna potrdila SREDNJE in VISOKE stopnje zaupanja prijavna služba preveri podatke o odgovorni osebi v kadrovski evidenci in opravi osebno identifikacijo odgovorne osebe.

Za digitalna potrdila NIZKE stopnje zaupanja preverjanje podatkov in osebna identifikacija nista obvezna. Zahtevke prejme in obdela operativno osebje SIMoD-CA-Restricted.

3.2.3. Preverjanje istovetnosti za fizične osebe

Zahtevek za pridobitev digitalnega potrdila za zaposlene na MO mora vsebovati podatke o bodočem imetniku in vodji organizacijske enote MO.

Za pravilnost podatkov na zahtevku jamči vodja organizacijske enote MO.

Za digitalna potrdila SREDNJE in VISOKE stopnje zaupanja prijavna služba preveri podatke o bodočem imetniku v kadrovski evidenci in opravi osebno identifikacijo.

Za digitalna potrdila NIZKE stopnje zaupanja preverjanje podatkov in osebna identifikacija nista obvezna. Zahtevke prejme in obdela operativno osebje SIMoD-CA-Restricted.

3.2.4. Podatki o naročniku, ki se ne preverjajo

Prijavna služba ne preverja naslednjih podatkov:

- splošni naziv oziroma ime organizacijske enote MO,
- ustreznost splošnega naziva in obstoj funkcijske ali organizacijske vloge,
- naziv strežnika in druge strojne ali programske opreme,
- naziv izdajatelja časovnih žigov, sistema za preverjanje veljavnosti digitalnih potrdil ali drugega ponudnika overjanja.

Za pravilnost zgoraj navedenih podatkov jamči vodja organizacijske enote MO.

3.2.5. Preverjanje pooblastil

Vodja organizacijske enote MO s podpisom na zahtevku za pridobitev digitalnega potrdila jamči, da želi za določeno osebo, da pridobi digitalno potrdilo zase, organizacijsko enoto MO, funkcijsko ali organizacijsko vlogo, napravo oziroma storitev.

3.2.6. Merila za medsebojno povezovanje

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

3.3. Preverjanje imetnikov za ponovno izdajo digitalnega potrdila

3.3.1. Preverjanje istovetnosti pri rutinski ponovni izdaji digitalnih potrdil

Ob rutinski ponovni izdaji upravljanih digitalnih potrdil, ki so bila izdana po protokolu PKIX-CMP, imetnik izkaže svojo istovetnost s posedovanjem veljavnega zasebnega ključa.

Rutinska ponovna izdaja digitalnih potrdil, izdanih z uporabo protokola PKCS#10, ni mogoča. Dovoljena je ponovna izdaja digitalnega potrdila brez osebnega preverjanja istovetnosti imetnika, če je elektronski zahtevek za ponovno izdajo podpisan z veljavnim digitalnim potrdilom. Imetnik izkaže svojo istovetnost s posedovanjem veljavnega zasebnega ključa.

3.3.2. Preverjanje istovetnosti za ponovno izdajo digitalnega potrdila po preklicu

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

3.4. Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila

Oseba, ki želi preklicati digitalno potrdilo, se identificira:

- z veljavnim digitalnim podpisom na zahtevku za preklic digitalnega potrdila,
- z lastnoročnim podpisom na zahtevku za preklic digitalnega potrdila ali
- ob telefonski zahtevi za preklic s skrivnim geslom, ki ga je določila ob oddaji zahtevka za izdajo digitalnega potrdila.

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 oddajo:

- za fizične osebe zaposleni v MO,
- za organizacijske enote MO predstojniki organizacijske enote vsaj na ravni vodje sektorja,
- za funkcijske ali organizacijske vloge nosilci, skrbniki ali administratorji vloge,
- za naprave in storitve skrbniki naprave oziroma storitve.

4.1.2. Postopek za pridobitev digitalnega potrdila in odgovornosti

Zahtevki za pridobitev digitalnega potrdila in navodila za izpolnjevanje ter oddajo zahtevkov so dostopni na spletni strani: http://www.simod-pki.mors.si.

Bodoči imetnik odda zahtevek za pridobitev digitalnega potrdila SREDNJE in VISOKE stopnje zaupanja v prijavno službo. Prijavna služba deluje v okviru rednega delovnega časa oziroma uradnih ur.

Bodoči imetnik posreduje odda zahtevek za izdajo digitalnega potrdila NIZKE stopnje zaupanja operativnemu osebju izdajatelja SIMoD-CA-Restricted.

4.2. Obdelava zahtevka za izdajo digitalnega potrdila

4.2.1. Preverjanje istovetnosti bodočega imetnika

Prijavna služba preveri zahtevek za izdajo digitalnega potrdila SREDNJE in VISOKE stopnje zaupanja in preveri istovetnost naročnika v skladu s poglavji 3.2.2 Preverjanje istovetnosti za imetnike, ki niso fizične osebe in 3.2.3 Preverjanje istovetnosti za fizične osebe.

Za digitalna potrdila NIZKE stopnje zaupanja se istovetnost naročnika ne preverja.

4.2.2. Odobritev ali zavrnitev izdaje digitalnega potrdila

Zahtevek za pridobitev digitalnega potrdila izdajatelja SIMoD-CA-Restricted ne obvezuje k izdaji digitalnega potrdila.

Ob pomanjkljivih podatkih, neupravičenosti do digitalnega potrdila ali neuspešnem preverjanju istovetnosti prijavna služba zavrne izdajo digitalnega potrdila SREDNJE ali VISOKE stopnje zaupanja.

Ob pomanjkljivih podatkih ali neupravičenosti do digitalnega potrdila NIZKE stopnje zaupanja operativno osebje izdajatelja SIMoD-CA-Restricted zavrne izdajo digitalnega potrdila.

Odobritev ali zavrnitev izdaje digitalnega potrdila SREDNJE ali VISOKE stopnje zaupanja je diskrecijska pravica prijavne službe. Prijavna služba pošlje obvestilo o zavrnitvi vlagatelju zahtevka po elektronski pošti, odobritev pa posreduje operativnemu osebju izdajatelja SIMoD-CA-Restricted.

Odobritev ali zavrnitev izdaje digitalnega potrdila NIZKE stopnje zaupanja je diskrecijska pravica operativnega osebja izdajatelja SIMoD-CA-Restricted. Obvestilo o zavrnitvi pošlje operativno osebje izdajatelja SIMoD-CA-Restricted vlagatelju zahtevka po elektronski pošti.

Bodoči imetnik je o odobritvi izdaje digitalnega potrdila obveščen hkrati s prejemom aktivacijskih podatkov ali pametne kartice z digitalnim potrdilom.

4.2.3. Čas za obdelavo zahtevka za izdajo digitalnega potrdila

Najdaljši dopusten čas od sprejema zahtevka za pridobitev digitalnega potrdila do izdaje aktivacijskih podatkov, ki jih bodoči imetnik potrebuje za generiranje ključev, ali pametne kartice z digitalnim potrdilom je 21 dni.

4.3. Izdaja digitalnega potrdila

4.3.1. Postopki izdajatelja SIMoD-CA-Restricted ob izdaji potrdil

Operativno osebje izdajatelja SIMoD-CA-Restricted začne postopke izdajanja digitalnega potrdila SREDNJE in VISOKE stopnje zaupanja po prejemu odobrenega zahtevka od prijavne službe.

Operativno osebje izdajatelja SIMoD-CA-Restricted začne postopke izdajanja digitalnega potrdila NIZKE stopnje zaupanja po prejemu in odobritvi zahtevka.

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

Operativno osebje izdajatelja SIMoD-CA-Restricted pošlje bodočemu imetniku obvestilo o odobritvi izdaje digitalnega potrdila in aktivacijske podatke, razdeljene v dva dela, in sicer referenčno številko po elektronski pošti, avtorizacijsko kodo pa v kuverti po pošti.

Za digitalna potrdila z obvezno uporabo pametne kartice, če izdajatelj SIMoD-CA-Restricted ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, operativno osebje bodočemu imetniku ne pošilja aktivacijskih podatkov. Ključe in digitalna potrdila generira operativno osebje. Pametno kartico z digitalnim potrdilom in zasebnim ključem varno dostavi imetniku.

4.3.2. Obvestilo naročnikom o izdaji digitalnega potrdila

Operativno osebje izdajatelja SIMoD-CA-Restricted obvesti bodočega imetnika o odobritvi izdaje digitalnega potrdila z istim elektronskim sporočilom, s katerim mu pošlje referenčno številko, in z obvestilom po pošti, s katerim mu pošlje avtorizacijsko kodo.

Za digitalna potrdila z obvezno uporabo pametne kartice, če izdajatelj SIMoD-CA-Restricted ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, velja, da je bodoči imetnik prejel obvestilo o izdaji potrdila, ko prevzeme pametno kartico z digitalnim potrdilom.

4.4. Prevzem digitalnega potrdila

4.4.1. Postopek prevzema digitalnega potrdila

Bodoči imetnik praviloma samostojno prevzame digitalno potrdilo z aktivacijskimi podatki, in sicer referenčno številko in avtorizacijsko kodo.

Veljavnost aktivacijskih podatkov je 60 dni od izdaje.

Tehnični postopek prevzema je odvisen od tipa digitalnega potrdila in uporabniške programske opreme.

Prevzem upravljanih digitalnih potrdil (*Entrust ID*) po protokolu PKIX-CMP se izvede z namensko programsko opremo. Navodila za namestitev in uporabo programske opreme se nahajajo na spletni strani http://www.simod-pki.mors.si.

Prevzem neupravljanih digitalnih potrdil (*spletna* oz *WEB*) po protokolu PKCS#10 se izvede preko spletnega vmesnika. Spletni naslov vmesnika in navodila za prevzem so dostopna na spletnem naslovu http://www.simod-pki.mors.si.

Digitalno potrdilo z obvezno uporabo pametne kartice, če izdajatelj SIMoD-CA-Restricted ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, prevzame operativno osebje. Nato pametno kartico s prevzetim digitalnim potrdilom varno dostavi imetniku.

Ob prevzemu digitalnega potrdila mora imetnik preveriti vsebino digitalnega potrdila, ali je digitalno potrdilo podpisal izdajatelj SIMoD-CA-Restricted in polno pot digitalnih podpisov do korenskega izdajatelja SIMoD-CA-Root. S prvo uporabo oziroma če imetnik osem dni od prevzema digitalnega potrdila izdajatelja SIMoD-CA-Restricted 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 Odgovornost in jamstva imetnikov digitalnih potrdil.

4.4.2. Objava digitalnega potrdila

Digitalno potrdilo z javnim ključem za šifriranje je po izdaji objavljeno v imenikih iz podpoglavja 2.2. Objave informacij o digitalnih potrdilih.

Izdajatelj SIMoD-CA-Restricted praviloma ne objavlja digitalnih potrdil z javnimi ključi za preverjanje elektronskega podpisa.

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

Imetnik digitalnega potrdila izdajatelja SIMoD-CA-Restricted mora:

- uporabljati ključe in digitalna potrdila samo za namene, ki so definirani v politiki SIMoD-PKI in pravilih SIMoD-CA-Restricted,
- po prevzemu digitalnega potrdila preveriti podatke v digitalnem potrdilu in ob morebitnih napakah takoj obvestiti operativno osebje SIMoD-CA-Restricted oziroma zahtevati preklic digitalnega potrdila,
- vse spremembe, ki so povezane s digitalnimi potrdili, v osmih dneh sporočiti prijavni službi ali operativnemu osebju SIMoD-CA-Restricted,
- uporabljati zasebne ključe in digitalna potrdila le v obdobju njihove veljavnosti,
- podpisovati ali šifrirati le podatke, katerih veljavnost je krajša od veljavnosti digitalnega potrdila oziroma pred potekom veljavnosti digitalnega potrdila ponovno podpisati oziroma šifrirati podatke, če to ni rešeno na drug način (z aplikacijo),
- varovati svoje zasebne ključe in pametne kartice ali druge nosilce zasebnih ključev ter upoštevati vse ukrepe, da se prepreči izguba, razkritje, sprememba ali nepooblaščena uporaba,
- ob sumu zlorabe svojega zasebnega ključa ukrepati po postopku, ki je opisan v podpoglavju 4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila.

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, določene v politiki SIMoD-PKI in pravilih SIMoD-CA-Restricted,
- ob domnevni zlorabi zasebnega ključa ali če so spremenjeni podatki iz digitalnega potrdila, na katerega se zanaša, obvestiti operativno osebje SIMoD-CA-Restricted,
- preveriti, ali je bil podpis ustvarjen v času veljavnosti digitalnega potrdila,
- za uporabljeno digitalno potrdilo opraviti popoln postopek preverjanja poti zaupanja,
- preveriti status digitalnega potrdila v veljavnem registru preklicanih potrdil.

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 za preverjanje e-podpisa in digitalnega potrdila za preverjanje e-podpisa ter šifriranje pomeni generiranje novega para ključev in novega digitalnega potrdila.

Ponovna izdaja digitalnega potrdila za šifriranje pomeni generiranje novega para ključev in novega digitalnega potrdila ter praviloma tudi povrnitev zgodovine ključev v skladu s podpoglavjem 4.12.1 Povrnitev zgodovine ključev za dešifriranje.

4.7.1. Razlogi za ponovno izdajo digitalnega potrdila

Ponovna izdaja digitalnega potrdila se izvede:

- po preklicu,
- po preteku veljavnosti,
- pred pretekom veljavnosti, če je imetnik pozabil geslo za dostop do zasebnih ključev, izgubil ali poškodoval pametno kartico ali drugi nosilec zasebnih ključev.

4.7.2. Kdo lahko zahteva ponovno izdajo digitalnega potrdila

Za ponovno izdajo digitalnega potrdila lahko zaprosijo imetniki oziroma subjekti kot za prvo izdajo skladno s podpoglavjem 4.1.1 Kdo lahko zaprosi za izdajo digitalnega potrdila.

4.7.3. Obdelava zahtevkov za ponovno izdajo digitalnega potrdila

Za ponovno izdajo digitalnega potrdila po preklicu ali preteku veljavnosti oddajo imetniki enak zahtevek kot za prvo pridobitev digitalnega potrdila. Zahtevek se obdela v skladu s podpoglavjema 4.1. Pridobitev digitalnega potrdila in 4.2. Obdelava zahtevka za izdajo digitalnega potrdila.

Ponovna izdaja digitalnih potrdil pred pretekom veljavnosti se za upravljana digitalna potrdila (*Entrust ID*), izdana po protokolu PKIX-CMP, opravi samodejno ob uporabi digitalnega potrdila z neposrednim dostopom do izdajatelja SIMoD-CA-Restricted v obdobju stotih dni pred pretekom veljavnosti zasebnega ključa. Generiranje novih parov ključev se izvede le, če je digitalno potrdilo veljavno. Postopek imenujemo tudi rutinska ponovna izdaja digitalnih potrdil.

Ponovna izdaja digitalnih potrdil pred pretekom veljavnosti se za neupravljana digitalna potrdila (*spletna* oziroma *WEB*), izdana po protokolu PKCS#10, opravi na podlagi ustreznega elektronskega zahtevka, ki je podpisan z veljavnim digitalnim potrdilom.

Za ponovno izdana digitalna potrdila velja politika, veljavna ob datumu generiranja novih parov ključev.

4.7.4. Obvestilo imetniku o izdaji novega digitalnega potrdila

Ob rutinski ponovni izdaji upravljanega digitalnega potrdila po protokolu PKIX-CMP namenska programska oprema imetnika obvesti o uspešnem prevzemu digitalnega potrdila.

Za digitalna potrdila, ki so ponovno izdana na osnovi zahtevka, prejmejo imetniki obvestilo o izdaji skladno s poglavjem 4.3.2 Obvestilo naročnikom o izdaji digitalnega potrdila.

4.7.5. Postopek potrditve prevzema novega digitalnega potrdila

Enako kot 4.4.1 Postopek 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 podatkov v digitalnem potrdilu ni mogoča. Ob spremembah podatkov v digitalnem potrdilu je treba digitalno potrdilo preklicati.

4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila

4.9.1. Okoliščine preklica

Razlogi za preklic digitalnih potrdil imetnikov so:

- dejanska ali domnevna zloraba zasebnih ključev,
- neizpolnjevanje obveznosti iz politike SIMoD-PKI ali pravil SIMoD-CA-Restricted,
- sprememba podatkov, ki so vsebovani v digitalnem potrdilu,
- razlogi, navedeni v podpoglavju 4.11. Predčasna prekinitev veljavnosti digitalnih potrdil.

4.9.2. Kdo lahko zahteva preklic

Zahtevo za preklic digitalnega potrdila imetnika lahko poda:

- imetnik za svoje digitalno potrdilo,
- vodja organizacijske enote MO,
- nosilec, skrbnik oziroma administrator funkcijske ali organizacijske vloge,
- skrbnik strežnika, druge strojne ali programske opreme, izdajatelja časovnih žigov, sistema za preverjanje veljavnosti digitalnih potrdil ali druge storitve overjanja,
- varnostnega inženir izdajatelja SIMoD-CA-Restricted, če sumi, da imetnik krši pravila varnega ravnanja z digitalnim potrdilom.

4.9.3. Postopki za preklic

Zahtevki za preklic se lahko posredujejo:

- kot digitalno podpisano elektronsko sporočilo operativni osebi ali na skupinski elektronski naslov izdajatelja SIMoD-CA-Restricted,
- kot digitalno podpisan zahtevek v elektronskem dokumentacijskem sistemu,
- kot lastnoročno podpisan zahtevek ali
- po telefonu na dežurno številko za preklic.

Pri telefonsko posredovanem zahtevku dežurna oseba posreduje zahtevek za preklic operativnemu osebju, ki izvrši preklic in o preklicu obvesti imetnika ali odgovorno osebo.

Preklicano digitalno potrdilo se objavi v registru preklicanih potrdil.

4.9.4. Čas za posredovanje zahtevka za preklic

Osebe, ki lahko zahtevajo preklic, morajo posredovati zahtevek za preklic takoj, ko zvejo za okoliščino preklica.

4.9.5. Čas od prejema zahtevka za preklic do preklica

Operativno osebje opravi preklic v osmih urah po prejemu zahtevka za preklic ob:

- dejanski ali domnevni zlorabi zasebnih ključev ali
- neizpolnjevanju obveznosti iz politike SIMoD-PKI ali pravil SIMoD-CA-Restricted.

Operativno osebje opravi preklic 24 urah po prejemu zahtevka za preklic ob:

- spremembi podatkov v digitalnem potrdilu,
- prenehanju delovnega razmerja imetnika,
- prenehanju obstoja organizacijske enote MO, organizacijske ali funkcijske vloge,
- prenehanju delovanja strežnika, programske ali strojne opreme, izdajatelja časovnih žigov, sistema za preverjanje veljavnosti digitalnih potrdil oziroma druge storitve overjanja.

V primerih, ko je bil zahtevek oddan pred uveljavitvijo spremembe, se preklic opravi na dan uveljavitve spremembe.

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 z [16] 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

Izdajatelj SIMoD-CA-Restricted objavi nov register preklicanih potrdil:

- vsaj na 25 ur,
- ob preklicu digitalnega potrdila.

4.9.8. Dovoljene zakasnitve pri objavi registrov preklicanih potrdil

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

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

4.9.9. Sprotno preverjanje statusa digitalnih potrdil

Podprto je protokol za sprotno preverjanje statusa digitalnih potrdil (ang. On-line Certificate Status Protocol, OCSP) po priporočilu [19] RFC 6960.

4.9.10. Obveza sprotnega preverjanja statusa preklicanih potrdil

Tretje osebe morajo ob uporabi digitalnega potrdila vedno preveriti ali je digitalno potrdilo veljavno. To lahko opravijo z vpogledom v register preklicanih potrdil ali z uporabo protokola za sprotno preverjanje statusa digitalnih potrdil OCSP.

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

Ni podprto.

4.9.14. Kdo lahko zahteva začasno ukinitev veljavnosti

Ni podprto.

4.9.15. Postopki za začasno ukinitev veljavnosti

Ni podprto.

4.9.16. Omejitve obdobja začasne ukinitve veljavnosti

Ni podprto.

4.10. Preverjanje statusa digitalnih potrdil

4.10.1. Tehnične lastnosti storitve

Registri preklicanih potrdil so dostopni skladno s podpoglavjem 2.2. Objave informacij o digitalnih potrdilih.

Storitev sprotnega preverjanja statusa digitalnih potrdil OCSP je dostopna na naslovu http://ocsp.simod-pki.mors.si.

Registri preklicanih potrdil so v skladu z [16] RFC 5280.

Sprotno preverjanje statusa potrdil je v skladu z [19] RFC 6960.

4.10.2. Razpoložljivost storitve

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

4.10.3. Dodatne možnosti

Niso določene.

4.11. Predčasna prekinitev veljavnosti digitalnih potrdil

Predčasno se prekine veljavnost digitalnega potrdila iz naslednjih razlogov:

- prenehanje delovnega razmerja imetnika,
- prenehanje delovanja organizacijske enote MO,
- prenehanje obstoja organizacijske ali funkcijske vloge,
- prenehanje delovanja strežnika, druge strojne ali programske opreme, izdajatelja časovnih žigov, sistema za preverjanje veljavnosti digitalnih potrdil ali druge storitve overjanja.

4.12. Varnostno kopiranje in odkrivanje zasebnega ključa

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

Izdajatelj SIMoD-CA-Restricted varnostno kopira (Key Backup) zasebne ključe za dešifriranje v povezavi z upravljanimi digitalnimi potrdili za šifriranje po protokolu PKIX-CMP.

Varnostno kopiranje zasebnih ključev za digitalna potrdila, izdana po protokolu PKCS#10, ni mogoče.

4.12.1. Povrnitev zgodovine ključev za dešifriranje

Izdajatelj SIMoD-CA-Restricted omogoča povrnitev zgodovine ključev (Key Recovery) za dešifriranje le za upravljana digitalna potrdila za šifriranje, izdana po protokolu PKIX-CMP.

Povrnitev zgodovine ključev za dešifriranje se opravi ob ponovni izdaji digitalnega potrdila po protokolu PKIX-CMP.

4.12.2. Odkrivanje kopije ključev za dešifriranje

Odkrivanje kopije ključev za dešifriranje drugim osebam, kot je imetnik povezanih digitalnih potrdil za šifriranje, ni dovoljeno.

Imetniku digitalnega potrdila je odkrivanje kopije ključev za dešifriranje omogočeno kot predpisano v podpoglavju 4.12.1 Povrnitev zgodovine ključev za dešifriranje

Aplikacije in informacijske rešitve MO morajo šifrirati službene podatke tako, da so selektivno dostopni vsem osebam, ki so pooblaščene za dostop do teh podatkov.

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

5.1. Fizično varovanje

5.1.1. Lokacija in konstrukcija prostorov

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

Prostori so varnostno območje II. stopnje po [21] ZTP.

5.1.2. Fizični dostop

Nadzor fizičnega dostopa izvaja pristojna služba MO.

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

O vstopih in izstopih v prostore se vodi evidenca.

5.1.3. Napajanje in klimatske naprave

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

- sistemom za brezprekinitveno napajanje naprav,
- klimatsko napravo za nadzor temperature in vlage.

5.1.4. Zaščita pred poplavo

Prostori s komunikacijsko in informacijsko opremo izdajatelja SIMoD-CA-Restricted so na lokaciji, kjer je verjetnost poplave majhna.

5.1.5. Zaščita pred ognjem

Prostori s komunikacijsko in informacijsko opremo izdajatelja SIMoD-CA-Restricted so opremljeni z detektorji temperature in dima.

5.1.6. Shranjevanje medijev

Mediji z varnostnimi kopijami in arhivom podatkov se hranijo v protivlomnih omarah.

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

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 izdajatelja SIMoD-CA-Restricted

5.2.1.1. Operativno osebje

Operativno osebje izdajatelja SIMoD-CA-Restricted je razdeljeno na tri zaključene organizacijske skupine.

V skupini za upravljanje digitalnih potrdil so:

- prvi varnostni inženir,
- varnostni inženirji in
- administratorji potrdil.

V skupini za upravljanje programske in strojne opreme so:

- prvi administrator in
- administratorji.

V skupini za varovanje in nadzor komunikacijskega sistema so:

- prvi administrator in
- administratorji sistema.

Podrobnejša razdelitev pristojnosti in nalog:

Vloga	Pristojnosti in naloge	Min. št. oseb
Upravljanje z digitalnimi potrdil		
Prvi varnostni inženir	• Določanje in izvajanje pravil varnega delovanja sistema za podeljevanje potrdil, • določanje uporabniških pravic drugih varnostnih inženirjev in administratorjev digitalnih potrdil, • 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.	1
Administrator digitalnih potrdil	• Upravljanje s potrdili.	1
Upravljanje s strojno in programsko opremo izdajatelja		
Prvi administrator izdajatelja	• Odgovornost za operativno 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, • administracija in vzdrževanje delovanja strojne in programske opreme izdajatelja, • izvedba sprememb strojne in programske opreme izdajatelja, • izdelava in vzdrževanje varnostnih kopij.	1

Varovanje in nadzor komunikacijskega sistema		
Prvi administrator komunikacijskega sistema	• Odgovornost za operativno delovanje sistema za varovanje in nadzor komunikacijskega sistema izdajatelja, • namestitev in začetna konfiguracija komunikacijskih naprav, varnostnih pregrad in sistemov za odkrivanje ter preprečevanje vdorov, • načrtovanje in izvedba sprememb na komunikacijskih napravah, varnostnih pregradah in sistemih za odkrivanje ter preprečevanje vdorov, • izdelava in vzdrževanje varnostnih kopij, • ponovna vzpostavitev delovanja iz varnostnih kopij, • pregled in analiza varnostnih beležk.	1
Administrator komunikacijskega sistema	• Namestitev in začetna konfiguracija komunikacijskih naprav, varnostnih pregrad in sistemov za odkrivanje ter preprečevanje vdorov, • administracija in vzdrževanje delovanja komunikacijskih naprav, varnostnih pregrad in sistemov za odkrivanje ter preprečevanje vdorov, • izvedba sprememb na komunikacijskih napravah, varnostnih pregradah in sistemih za odkrivanje ter preprečevanje vdorov, • izdelava in vzdrževanje varnostnih kopij.	1

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

- sprejemanje zahtevkov za izdajo in preklic digitalnih potrdil,
- preverjanje identitete naročnikov in točnosti podatkov v zahtevkih,
- posredovanje zahtevkov operativnemu osebju,
- obveščanje operativnega osebje o spremembah podatkov o imetnikih digitalnih potrdil.

5.2.2. Število oseb za izvedbo postopkov

V skupini za upravljanje digitalnih potrdil so najmanj tri osebe, v skupini za upravljanje programske in strojne opreme sta najmanj dve osebi, v skupini za varovanje in nadzor komunikacijskega sistema sta najmanj dve osebi.

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

5.2.3. Preverjanje istovetnosti operativnega osebja

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

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

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

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

5.3. Zahteve za osebje izdajatelja SIMoD-CA-Restricted

5.3.1. Kvalifikacije, izkušnje in varnostno preverjanje

Operativno osebje izdajatelja SIMoD-CA-Restricted:

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

5.3.2. Dovoljenja za dostop do tajnih podatkov

V skladu z [21] ZTP.

5.3.3. Usposabljanje osebja

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

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

Osebje prijavne službe se usposoblja za:

- preverjanje identitete naročnikov in preverjanje pravilnosti podatkov v zahtevkih,
- delo s programsko opremo prijavne službe

5.3.4. Pogostost dodatnih usposabljanj

Osebje se usposablja glede na izkazane potrebe oziroma novosti v povezavi z delovanjem izdajatelja SIMoD-CA-Restricted.

5.3.5. Kroženje med delovnimi mesti

Ni določeno.

5.3.6. Ukrepi ob kršitvah pooblastil

Proti operativni osebi izdajatelja SIMoD-CA-Restricted, ki ne opravlja svojih nalog ali zlorabi svoja pooblastila, se ukrepa skladno s predpisi.

5.3.7. Zunanji izvajalci

Zunanji izvajalci morajo izpolnjevati vse pogoje, določene v [21] ZTP, in varnostne zahteve izdajatelja SIMoD-CA-Restricted.

5.3.8. Dokumentacija za operativno osebje

Operativnemu osebju izdajatelja SIMoD-CA-Restricted 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

Izdajatelj SIMoD-CA-Restricted beleži dogodke:

- na operacijskem sistemu, programski in strojni opremi izdajatelja SIMoD-CA-Restricted ter imeniku,
- na operacijskih sistemih, programski in strojni opremi elementov komunikacijskega sistema,
- glede svojih ključev,
- glede imetniških ključev in digitalnih potrdil,
- glede varnostne politike in upravljanja informacijskega sistema in imenika,
- glede varnostne politike in upravljanja komunikacijskega sistema.

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

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

5.4.2. Pogostost pregleda dnevnikov beleženih dogodkov

Operativno osebje izdajatelja SIMoD-CA-Restricted uporablja nadzorne sisteme za spremljanje stanja sistemov in sprotno obveščanje o dogodkih. Ob vsakem opozorilu iz nadzornih sistemov osebje pregleda dnevnike beleženih dogodkov.

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 izdajatelja 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-Restricted z namenom odkrivanja in odprave ranljivosti. Ugotovljeno 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

Izdajatelj SIMoD-CA-Restricted hrani naslednje podatke:

- dnevnike beleženih dogodkov iz podpoglavja 5.4.1 Vrste beleženih dogodkov,
- zahtevke za pridobitev in preklic digitalnih potrdil,
- korespondenco imetnikov digitalnih potrdil z izdajateljem SIMoD-CA-Restricted,
- dokumentacijo o izvedbi identifikacije naročnikov digitalnih potrdil,
- digitalna potrdila in registre preklicanih potrdil,
- svoja javna in zaupna pravila delovanja,
- zasebne ključe za dešifriranje.

5.5.2. Obdobje hranjenja arhiva

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

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

5.5.3. Zaščita arhiva

Zahtevki za pridobitev in preklic digitalnih potrdil, korespondenca imetnikov digitalnih potrdil z izdajateljem, dokumentacija o izvedbi identifikacije, pravila delovanja SIMoD-CA-Restricted in dnevniki beleženih dogodkov v pisni obliki se hranijo in arhivirajo v skladu s internimi splošnimi pravnimi 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 zasebni dešifrirni ključi, se hranijo vsaj 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.

5.5.4. Varnostna kopija arhiva

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

Ob vzpostavitvi arhiva podatkov, ki se beležijo v okviru informacijskega sistema, 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-Restricted.

5.5.7. Postopek vpogleda v arhiv in njegova verifikacija

Dostop do arhiva je dovoljen le:

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

Ob kreiranju arhiva se preveri integriteta medija.

5.6. Zamenjava ključev izdajatelja SIMoD-CA-Restricted

Veljavnost digitalnega potrdila izdajatelja SIMoD-CA-Restricted je vedno daljša, kot je veljavnost katerega koli digitalnega potrdila imetnika, podpisanega s pripadajočim zasebnim ključem.

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

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

Ponovna izdaja digitalnega potrdila izdajatelja SIMoD-CA-Restricted poteka po predpisanem in nadzorovanem postopku. Postopek izvede operativno osebje korenskega izdajatelja SIMoD-CA-Root in izdajatelja SIMoD-CA-Restricted. 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 delovanja.

5.7.2. Uničenje programske, strojne opreme ali podatkov izdajatelja

Ob okvari strojne ali programske opreme oziroma podatkov, pri kateri zasebni ključ izdajatelja ni bil uničen, bodo storitve izdajatelja ponovno vzpostavljene v najkrajšem možnem času. Prioriteta je vzpostavitev funkcionalnosti preklica digitalnih potrdil in objavljanja registra preklicanih potrdil. Skrajni rok za vzpostavitev je sedem dni. Po tem roku bo izdajatelj ukrepal v skladu s podpoglavjem 5.8. Prenehanje delovanja izdajatelja SIMoD-CA-Restricted.

Ob uničenju izdajateljevega zasebnega ključa in vseh njegovih kopij, se ravna v skladu s podpoglavjem 5.8. Prenehanje delovanja izdajatelja SIMoD-CA-Restricted.

5.7.3. Zloraba zasebnega ključa izdajatelja SIMoD-CA-Restricted

Ob zlorabi zasebnega ključa izdajatelja SIMoD-CA-Restricted, ki zahteva preklic digitalnega potrdila izdajatelja, je potrebno ukrepati v skladu s podpoglavjem 5.8. Prenehanje delovanja izdajatelja SIMoD-CA-Restricted.

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, so del okrevalnega načrta, ki je del zaupnih pravil.

5.8. Prenehanje delovanja izdajatelja SIMoD-CA-Restricted

Razlogi za prenehanje delovanja oziroma preklic digitalnega potrdila izdajatelja SIMoD-CA-Restricted so:

- domnevna ali dejanska zloraba zasebnega ključa,
- nezmožnost pravočasne ponovne vzpostavitve delovanja po okvari oziroma nesreči,
- preklic digitalnega potrdila korenskega izdajatelja SIMoD-CA-Root,
- sklep predstojnika organizacijske enote, pristojne za informatiko, o prenehanju delovanja izdajatelja SIMoD-CA-Restricted,
- druge okoliščine, ki lahko ogrozijo zaupanje v digitalno potrdilo izdajatelja SIMoD-CA-Restricted.

Preklic digitalnega potrdila izdajatelja SIMoD-CA-Restricted opravi operativno osebje na zahtevo predstojnika organizacijske enote, pristojne za informatiko.

Izdajatelj SIMoD-CA-Restricted mora ob preklicu svojega digitalnega potrdila opraviti naslednje postopke:

- preklicati vsa digitalna potrdila,
- zagotavljati razpoložljivost registrov preklicanih potrdil vsaj še 90 dni,
- objaviti obvestilo o preklicu svojega potrdila na spletni strani http://www.simod-pki.mors.si.

Ob prenehanju delovanja bo ponudnik storitev zaupanja na MO ukrepal v skladu z veljavno zakonodajo.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev para ključev

Par ključev izdajatelja SIMoD-CA-Restricted se vedno generira v varnostnem kriptografskem modulu pod nadzorom operativnega osebja.

Par ključev izdajateljev časovnih žigov in za storitev OCSP se vedno generira v varnostnem kriptografskem modulu pod nadzorom skrbnika storitve.

Ključi imetniških digitalnih potrdil se generirajo in hranijo kot navedeno v tabeli:

Namen uporabe ključa	Stopnja zaupanja	Kje se ključ generira	Kje se ključ hrani	Kje se hrani kopija ključa
Digitalno potrdilo za šifriranje, vedno upravljano digitalno potrdilo (*Entrust ID*)				
zasebni ključ za dešifriranje	VISOKA	pri izdajatelju	na uporabnikovi pametni kartici	šifrirana v bazi izdajatelja
javni ključ za šifriranje				digitalno potrdilo za šifriranje
zasebni ključ za dešifriranje	SREDNJA NIZKA	pri izdajatelju	v programski opremi pri uporabniku	šifrirana v bazi izdajatelja
javni ključ za šifriranje				digitalno potrdilo za šifriranje
Digitalno potrdilo za preverjanje e-podpisa, vedno upravljano digitalno potrdilo (*Entrust ID*)				
zasebni ključ za e-podpis	VISOKA	na uporabnikovi pametni kartici		ne obstaja
javni ključ za preverjanje e-podpisa				digitalno potrdilo za preverjanje e-podpisa
zasebni ključ za e-podpis	SREDNJA NIZKA	v programski opremi pri uporabniku		ne obstaja
javni ključ za preverjanje e-podpisa				digitalno potrdilo za preverjanje e-podpisa
Digitalno potrdilo za preverjanje e-podpisa / e-žiga in šifriranje; upravljano ali neupravljano (spletno, *WEB*)				
zasebni ključ za e- podpis / e-žig in dešifriranje	VISOKA	na uporabnikovi pametni kartici		ne obstaja
javni ključ za preverjanje e-podpisa / e-žiga in šifriranje				digitalno potrdilo za preverjanje e-podpisa / e-žiga in šifriranje
zasebni ključ za e-podpis / e-žig in dešifriranje	SREDNJA NIZKA	v programski opremi pri uporabniku		ne obstaja
javni ključ za preverjanje e-podpisa / e-žiga in šifriranje				digitalno potrdilo za preverjanje e-podpisa /e-žiga in šifriranje

Za digitalna potrdila z obvezno uporabo pametne kartice, če izdajatelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, to je za neupravljana digitalna potrdila za preverjanje e-podpisa / e-žiga in šifriranje VISOKE stopnje zaupanja, se zasebni ključ za oba namena uporabe generira na pametni kartici pri izdajatelju.

6.1.1. Dostava zasebnega ključa imetniku

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

Par ključev za podpisovanje se vedno ustvari pri bodočem imetniku. Zasebni ključ za podpisovanje se nikdar ne generira, ne prenaša in ne hrani pri izdajatelju.

Za digitalna potrdila z obvezno uporabo pametne kartice, če izdajatelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, to je za neupravljana digitalna potrdila za preverjanje e-podpisa / e-žiga in šifriranje VISOKE stopnje zaupanja, se zasebni ključ za oba namena uporabe generira na pametni kartici pri izdajatelju. Pametna kartica se nato varno dostavi imetniku.

6.1.2. Dostava imetnikovega javnega ključa izdajatelju

Javni ključ, ki se generira pri imetniku, se dostavi izdajatelju po protokolu PKIX-CMP ali PKCS#10.

6.1.3. Dostava izdajateljevega javnega ključa uporabnikom

Javni ključ izdajatelja oziroma izdajateljevo digitalno potrdilo, ki vsebuje javni ključ, se pošlje bodočemu imetniku digitalnega potrdila kot integralni del postopka za prevzem potrdila v obeh uporabljenih protokolih, PKIX-CMP in PKCS#10.

Izdajateljevo digitalno potrdilo lahko uporabniki pridobijo tudi iz imenika in na spletnih straneh izdajatelja SIMoD-CA-Restricted, pri tem morajo preveriti istovetnost izdajatelja in celovitost izdajateljevega digitalnega potrdila.

6.1.4. Dolžina ključev

Dolžina RSA zasebnega ključa izdajatelja SIMoD-CA-Restricted mora biti vsaj 3072 bitov.

Dolžina RSA zasebnega ključa v imetniških digitalnih potrdilih mora biti vsaj 2048 bitov.

6.1.5. Parametri za generiranje javnih ključev in preverjanje parametrov

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

6.1.6. Namen uporabe ključev

Namen uporabe ključev je določen v razširitvenem polju *Key Usage* in *Extended Key Usage* po priporočilu [16] RFC 5280.

Dovoljene vrednosti razširitvenega polja *Key Usage* glede na vrsto digitalnega potrdila so:

Digitalno potrdilo za:		*keyUsage*	*extKeyUsage*
izdajatelj SIMoD-CA-Restricted		*keyCertSign, cRLSign*	
končni imetniki:			
preverjanje e-podpisa		*digitalSignature, nonRepudiation*	
šifriranje		*keyEncipherment*	
preverjanje e-podpisa / e-žiga in šifriranje	fizične osebe	*digitalSignature, keyEncipherment, nonRepudiation*	
	splošni nazivi	*digitalSignature, keyEncipherment*	
	strežniki	*digitalSignature, keyEncipherment*	*serverAuth, clientAurh*
izdajatelji časovnih žigov		*digitalSignature*	*Time Stamping*
sistemi OCSP		*digitalSignature*	*OCSP Signing*
sistemi za podpis programske kode		*digitalSignature*	*codeSigning*

6.2. Zaščita zasebnih ključev in zahteve za kriptografske module

6.2.1. Standardi za kriptografski modul

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

Imetniki digitalnih potrdil VISOKE stopnje zaupanja morajo uporabljati pametne kartice ali podobne nosilce ključev, ki ustrezajo kriterijem za napravo za ustvarjanje kvalificiranega e-podpisa / e-žiga QSCD (ang. Qualified Signature/Seal Creation Device), ref. [5] ETSI EN 319 411-2 oziroma ustreza standardu [12] CC EAL5+ / PP QSCD.

Imetniki digitalnih potrdil SREDNJE stopnje zaupanja morajo uporabljati programske kriptografske module vsaj stopnje varnosti FIPS 140-2 level 1 ali primerljive.

6.2.2. Nadzor zasebnega ključa z več pooblaščenimi osebami

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

Povrnitev zgodovine imetniških zasebnih ključev za dešifriranje je mogoče ob pogojih iz podpoglavja 4.12.1 Povrnitev zgodovine ključev za dešifriranje.

6.2.4. Varnostno kopiranje zasebnih ključev

Varnostna kopija zasebnega ključa izdajatelja SIMoD-CA-Restricted 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 ($N \geq 2$, $M \geq 3$, $M > N$).

Kopije zasebnih ključev za dešifriranje za digitalna potrdila, za katera izdajatelj SIMoD-CA-Restricted zagotavlja povrnitev zgodovine ključev, se hranijo pri izdajatelju v šifrirani obliki.

6.2.5. Arhiviranje zasebnega ključa

Zasebni ključ izdajatelja SIMoD-CA-Restricted se ne arhivira.

Arhivirajo se le zasebni dešifrirni ključi v povezavi z imetniškimi digitalnimi potrdili, za katere izdajatelj SIMoD-CA-Restricted zagotavlja povrnitev zgodovine.

6.2.6. Zapis zasebnega ključa v kriptografski modul in iz njega

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

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

Zasebni ključi za e-podpisovanje se pri digitalnih potrdil VISOKE stopnje zaupanja generirajo na pametni kartici ali podobnem nosilcu ključev, pri digitalnih potrdilih SREDNJE in NIZKE stopnje zaupanja pa v programskem modulu pri bodočem imetniku.

Zasebni ključi za dešifriranje, za katera izdajatelj SIMoD-CA-Restricted zagotavlja povrnitev zgodovine, se generirajo v izdajateljevem kriptografskem modulu in prenesejo bodočemu imetniku z uporabo protokola PKIX-CMP.

Izvoz zasebnega ključa iz varnega kriptografskega modula ali s pametne kartice je onemogočen.

6.2.7. Hranjenje zasebnega ključev v kriptografskem modulu

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

Uporabniška programska oprema imetnikov digitalnih potrdil mora preveriti istovetnost uporabnika z geslom in šele po uspešnem preverjanju istovetnosti aktivirati zasebni ključ.

6.2.9. Postopek za deaktiviranje zasebnega ključa

Zasebni ključ izdajatelja SIMoD-CA-Restricted se deaktivira z ustavitvijo aplikativne programske opreme.

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

Ob zaustavitvi aplikativne programske opreme izdajatelja SIMoD-CA-Restricted se ključi, ki so v delovnem pomnilniku varnostnega kriptografskega modula, uničijo. Zasebni ključi nikoli niso v sistemskem pomnilniku, temveč le v strojni opremi varnostnega kriptografskega modula.

Zasebni ključi pri digitalnih potrdilih VISOKE stopnje zaupanja nikoli niso v sistemskem pomnilniku, vedno le v strojni opremi pametne kartice.

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

6.2.10. Postopek za uničenje zasebnega ključa

Zasebni ključi izdajatelja SIMoD-CA-Restricted se uničijo, ko jim poteče obdobje uporabe oziroma se ne uporabljajo več iz drugih razlogov. Uniči se aktivni ključ v varnostnem kriptografskem modulu in kopije v šifrirani datoteki z zasebnim ključem.

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

V primeru, da 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 s pari ključev

6.3.1. Arhiviranje javnega ključa

Izdajatelj SIMoD-CA-Restricted arhivira svoj javni ključ za preverjanje podpisa in imetniške javne ključe v povezavi z digitalnimi potrdili za preverjanje podpisa kot del arhiviranja digitalnih potrdil, kot je predpisano v podpoglavju 5.5. Arhiviranje podatkov.

Javni ključi v povezavi s šifrirnimi digitalnimi potrdili se ne arhivirajo.

6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil

Veljavnost digitalnega potrdila oziroma javnega in zasebnega ključa izdajatelja SIMoD-CA-Restricted je največ dvajset let oziroma do poteka veljavnosti digitalnega potrdila korenskega izdajatelja SIMoD-CA-Root.

Veljavnost imetniških digitalnih potrdil oziroma javnih in zasebnih ključev je:

Digitalno potrdilo za:	Ključ	Veljavnost
preverjanje e-podpisa	zasebni	štiri (4) leta
	javni	pet (5) let
šifriranje	zasebni	neomejeno
	javni	pet (5) let
preverjanje e-podpisa / e-žiga in šifriranje (vsa digitalna potrdila z dvojnim namenom uporabe razen za spodaj navedena imetnika)	zasebni	pet (5) let
	javni	pet (5) let
izdajatelja časovnih žigov	zasebni	tri (3) leta
	javni	pet (5) let
sistemi OCSP	zasebni	tri (3) leta
	javni	tri (3) leta

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 v postopku inicializacije modula.

Imetniki pametnih kartic ali drugih nosilcev zasebnih ključev morajo imeti popoln nadzor nad geslom za aktiviranje pametne kartice oziroma nosilca. Imeti morajo možnost določitve gesla med inicializacijo pametne kartice ali nosilca oziroma morajo imeti možnost predhodno nastavljeno geslo spremeniti.

Za dostop do zasebnih ključev, ki se hranijo v programski obliki (npr. Microsoft Cryptographic Store) morajo uporabniki uporabljati visoko stopnjo zaščite.

6.4.2. Zaščita gesel

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

Če je bilo geslo za aktivacijo imetniške pametne kartice ali drugega varnega nosilca zasebnih ključev določeno pri izdajatelju, ga izdajatelj varno dostavi imetniku.

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, pametnih kartic ali drugih nosilcev ne omogoča določitve kompleksnega gesla, je potrebno izbrati najmočnejše geslo v okviru tehničnih možnosti.

6.5. Varnostne zahteve za računalnike

6.5.1. Specifične tehnične varnostne zahteve

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

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

6.5.2. Raven varnostne zaščite računalnikov

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

Na nivoju operacijskega sistema 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 sistemi in programska oprema izdajatelja SIMoD-CA-Restricted so komercialni proizvodi.

6.6.2. Upravljanje varnosti

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

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

Izdajatelj SIMoD-CA-Restricted evidentira postopke inštalacije, spremembe konfiguracije in nadgradenje.

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

6.6.3. Upravljanje varnosti čez življenjski cikel

Nadgradnje, nove verzije in popravki na informacijski, komunikacijski in aplikativni opremi oziroma upravljanje varnosti se izvaja skozi celotno življenjsko obdobje opreme.

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

Izvajajo se pregledi konfiguracij informacijske, komunikacijske in aplikativne opreme in sicer po nadgradnji ali spremembi, za katero administrator izdajatelja ali administrator komunikacijskega sistema oceni, da je dovolj velika, da je potrebno izvesti pregled konfiguracije, oziroma vsaj enkrat letno.

6.7. Varnostne kontrole na ravni računalniškega omrežja

Komunikacijsko informacijski sistem izdajatelja SIMoD-CA-Restricted deluje v izoliranem omrežju, ki je z drugimi omrežji KIS MO povezan preko varnostnih pregrad, ki dovoljujejo prehod le protokolom za dostop do storitev izdajatelja.

V komunikacijsko informacijskem sistemu izdajatelja SIMoD-CA-Restricted se izvede pregled ranljivosti in/ali vdorni test ob nadgradnji ali spremembi, za katero administrator izdajatelja ali administrator komunikacijskega sistema oceni, da je dovolj velika, da je potrebno izvesti pregled ranljivosti in/ali vdorni test oziroma vsaj enkrat letno.

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

Izdajatelj SIMoD-CA-Restricted izdaja digitalna potrdila X.509 verzije 3 v skladu s priporočilom [16] RFC 5280, ki vsebujejo naslednja osnovna polja:

Ime osnovnega polja / prevod ali opis	Vrednost
Version / X.509 verzija	*v3*
Serial Number / serijska številka	enolična serijska številka
Signature Algorithm / algoritem za podpis	*sha256WithRSAEncryption* *(OID 1.2.840.113549.1.1.11)*
Issuer / izdajatelj, razločevalno ime	CN = simod-ca-restricted OU = simod-pki O = mors C = si
Validity / veljavnost potrdila	*Not Before*: začetek veljavnosti po GMT *Not After:* konec veljavnosti po GMT
Subject / imetnik, razločevalno ime	razločevalno ime imetnika v skladu s poglavjem 3.1. Določanje imen
Public Key Algorithm / algoritem za javni ključ	*rsaEncryption (OID 1.2.840.113549.1.1.1)*
Public Key Length / dolžina ključa	*2048*
Public Key / podatki o imetnikovem javnem ključu	modul, eksponent, vrednost javnega ključa

7.1.2. Razširitvena polja

Standardna razširitvena polja po priporočilu [16] RFC 5280 uporabljena v digitalnih potrdilih izdajatelja SIMoD-CA-Restricted, izdajateljev časovnega žiga, sistemov OCSP in sistemov za podpis programske kode so:

<table>
<tr><td colspan="4">Ime razširitvenega polja / prevod ali opis</td></tr>
<tr><td>SIMoD-CA-Restricted</td><td>izdajatelji časovnih žigov</td><td>OCSP</td><td>sistemi za podpis programske kode</td></tr>
<tr><td colspan="4">Authority Key Identifier / odtis javnega ključa izdajatelja</td></tr>
<tr><td>SHA256 odtis javnega ključa SIMoD-CA-Root</td><td colspan="3">SHA256 odtis javnega ključa SIMoD-CA-Restricted</td></tr>
<tr><td colspan="4">Subject Key Identifier / odtis imetnikovega javnega ključa</td></tr>
<tr><td colspan="4">SHA256 odtis imetnikovega javnega ključa</td></tr>
<tr><td colspan="4">Key Usage / namen uporabe ključa</td></tr>
<tr><td>Kritično
keyCertSign, CRLSign</td><td>Kritično
digitalSignature</td><td>Kritično
digitalSignature</td><td>Kritično
digitalSignature</td></tr>
<tr><td colspan="4">Extended Key Usage / razširjen namen uporabe</td></tr>
<tr><td>Ni uporabljeno</td><td>Kritično
timeStamping</td><td>Kritično
OCSP Signing</td><td>codeSigning</td></tr>
<tr><td colspan="4">Private Key Usage Period / veljavnost zasebnega ključa</td></tr>
<tr><td>Ni uporabljeno</td><td>Not Before:
Not After:</td><td>Ni uporabljeno</td><td>Ni uporabljeno</td></tr>
<tr><td rowspan="3">Certificate Policies / politike potrdila</td><td colspan="3">Policy Identifier / oznaka politike</td></tr>
<tr><td colspan="3">Policy Qualifier / podatki o politiki</td></tr>
<tr><td rowspan="2">Ni uporabljeno</td><td>1.3.6.1.4.1.22295.10.1.1.1.5.4.2</td><td>1.3.6.1.4.1.22295.10.1.1.1.6.5.2</td><td>1.3.6.1.4.1.22295.10.1.1.1.7.6.2
1.3.6.1.4.1.22295.10.1.1.2.7.6.2
1.3.6.1.4.1.22295.10.1.2.2.7.6.2</td></tr>
<tr><td colspan="3">Policy Qualifier Id=CPS
Qualifier: http:/www.simod-pki.mors.si</td></tr>
<tr><td colspan="4">CRL Distribution Point / LDAP in http URL naslovi registrov preklicanih potrdil</td></tr>
<tr><td>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</td><td colspan="3">DN:
cn=CRLn (n = številka delnega registra),
cn=simod-ca-restricted
ou=simod-pki,
o=mors,
c=si

URL:
ldap://imenik.simod-pki.mors.si/cn=CRLn,cn=simod-ca-restricted,ou=simod-pki,o=mors,c=si?certificateRevocationList

ldap://imenik.simod-pki.mors.si/cn=WinCombinedN,cn=simod-ca-restricted,ou=simod-pki,o=mors,c=si?certificateRevocationList

http://www.simod-pki.mors.si/crl/simod-ca-restrictedN.crl</td></tr>
<tr><td colspan="4">subject Alternative Name / alternativno ime imetnika</td></tr>
<tr><td>Ni uporabljeno</td><td>Ni uporabljeno</td><td>Ni uporabljeno</td><td>DNS ime sistema</td></tr>
<tr><td colspan="4">Basic Constraints / osnovne omejitve</td></tr>
<tr><td>Kritično
CA =: True
pathLenConstraint = 0</td><td>Kritično
CA =: False</td><td>Kritično
CA =: False</td><td>Kritično
CA =: False</td></tr>
<tr><td colspan="4">Authority Info Access / dostop do podatkov o izdajatelju</td></tr>
<tr><td>Ni uporabljeno</td><td colspan="3">Access Method: Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
Access Location: URL http://www.simod-pki.mors.si/certs/simod-ca-restricted.p7b

Access Method: ocsp (1.3.6.1.5.5.7.48.1)
Access Location: URL http://ocsp.simod-pki.mors.si/simod-ca-restricted</td></tr>
</table>

Imetniška digitalna potrdila, ki jih izdaja izdajatelj SIMoD-CA-Restricted, vsebujejo naslednja razširitvena polja po priporočilu [16] RFC 5280:

Ime razširitvenega polja / prevod ali opis	Potrdilo za preverjanje e-podpisa	Potrdilo za šifriranje	Potrdilo za preverjanje e-podpisa in šifriranje
Authority Key Identifier / odtis javnega ključa izdajatelja	SHA256 odtis javnega ključa izdajatelja SIMoD-CA-Restricted, s katerim je podpisano potrdilo		
Subject Key Identifier / odtis imetnikovega javnega ključa	SHA256 odtis imetnikovega javnega ključa		
Key Usage / namen uporabe ključa	**Kritično** *digitalSignature* *nonRepudiation*	**Kritično** *keyEncipherment*	**Kritično** *DigitalSignature* *keyEncipherment* fizične osebe še *nonRepudiation*
extended Key Usage / razširjen namen uporabe	Ni uporabljeno	Ni uporabljeno	samo za potrdila za strežnike *serverAuth,* *clientAurh*
Private Key Usage Period / veljavnost zasebnega ključa	Ni uporabljeno	V skladu s 6.3.2; *Not Before*: *Not After*:	Ni uporabljeno
Certificate Policies / oznaka politike potrdila	*[1]Certificate Policy:*		
Policy Identifier / enolična oznaka politike	Skladno s 1.2. *Policy Identifier=*		
Policy Qualifier / podatki o politiki	*[1,1]Policy Qualifier Info:* *Policy Qualifier Id=CPS* *Qualifier: http:/www.simod-pki.mors.si*		
CRL Distribution Points / naslovi registra preklicanih potrdil	DN: *cn=CRLn (n* = številka delnega registra), *cn=simod-ca-restricted* *ou=simod-pki,* *o=mors,* *c=si* URL: *ldap://imenik.simod-pki.mors.si/cn=CRLn,cn=simod-ca-restricted,ou=simod-pki,o=mors,c=si?certificateRevocationList* *ldap://imenik.simod-pki.mors.si/cn=WinCombinedN,cn=simod-ca-restricted,ou=simod-pki,o=mors,c=si?certificateRevocationList* *http://www.simod-pki.mors.si/crl/simod-ca-restrictedN.crl*		
Subject Alternative Name / alternativno ime imetnika	• *rfc822Name* – naslov elektronske pošte in/ali • *OtherName, Permanent Identifier* in/ali • *DNS Name* in/ali • druga standardna polja		
Basic Constraints / osnovne omejitve	**Kritično** CA =: False		
Authority Info Access / dostop do informacij o izdajatelju	*Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)* *Access Location: URL=http://www.simod-pki.mors.si/certs/simod-ca-restricted.p7b* *Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)* *Access Location: URL=http://ocsp.simod-pki.mors.si/simod-ca-restricted*		

7.1.3. Identifikacijske oznake algoritmov

Identifikacijski oznaki kriptografskih algoritmov, uporabljena v digitalnih potrdilih, 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

Kot v poglavju 3.1.1 Oblika imen.

7.1.5. Omejitve imen

Uporaba in način uporabe polja *Name Constraints* nista predpisana.

7.1.6. Identifikacijska oznaka politik

Digitalno potrdilo, ki ga izda izdajatelj SIMoD-CA-Restricted, vsebuje v polju *Certificate Policy* vsaj eno identifikacijsko oznako politike.

7.1.7. Način uporabe razširitvenega polja za omejitev uporabe politik

Izdajatelj SIMoD-CA-Restricted ne predpisuje uporabe in načina uporabe polja *Policy Constrains*.

7.1.8. Specifični podatki o politiki

V razširitvenem polju za specifične podatke o politiki *certificatePolicies, policyQualifier* je objavljen spletni naslov, kjer so objavljena Pravila delovanja izdajatelja (ang. CPS Pointer).

Razširitveno polje za specifične podatke o politiki *certificatePolicies, policyQualifier* se ne uporablja za objavo obvestila uporabnikom (ang. User Notice).

7.1.9. Procesiranje oznake kritičnosti razširitvenih polj

Uporabniške aplikacije morajo procesirati razširitvena polja digitalnega potrdila, označena kot kritična, v skladu s priporočili [16] RFC 5280.

7.2. Profil registrov preklicanih potrdil

7.2.1. Verzija registrov preklicanih potrdil

Izdajatelj SIMoD-CA-Restricted izdaja registre preklicanih potrdil verzije 2 v skladu s priporočilom [16] RFC 5280, ki vsebujejo naslednja osnovna polja:

Ime osnovnega polja		Prevod ali opis	Vrednost
version		verzija	v2
signature		algoritem za podpis registra	*Sha256WithRSAEncryption*, podpis
Issuer		izdajatelj	razločevalno ime SIMoD-CA-Restricted
thisUpdate		čas izdaje registra	čas izdaje po GMT
nextUpdate		čas izdaje naslednjega registra	čas naslednje izdaje po GMT
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

Izdajatelj SIMoD-CA-Restricted izdaja registre preklicanih potrdil verzije 2 v skladu s priporočilom [16] RFC 5280, 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 izdajatelja, ki podpisuje register preklicanih potrdil	SHA256 odtis javnega ključa izdajatelja SIMoD-CA-Restricted

7.3. Profil sprotnega preverjanja statusa potrdil

7.3.1. Verzija sprotnega preverjanja statusa potrdil

Sprotno preverjanja statusa digitalnih potrdil OCSP je v skladu s priporočilom [19] RFC 6960.

7.3.2. Razširitve sprotnega preverjanja statusa digitalnih potrdil

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

8. PREVERJANJE SKLADNOSTI IN OSTALE OBLIKE NADZORA

8.1. Pogostost 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-Restricted

Izdajatelj SIMoD-CA-Restricted jamči, da upravlja z digitalnimi potrdili v skladu s politiko SIMoD-PKI in pravili SIMoD-CA-Restricted.

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

9.6.2. Odgovornost in jamstva prijavne službe

Prijavna služba je odgovorna za skladnost identifikacijskih postopkov s politiko SIMoD-PKI in pravili SIMoD-CA-Restricted ter za točnost podatkov v zahtevkih.

9.6.3. Odgovornost in jamstva imetnikov digitalnih potrdil

Imetnik digitalnega potrdila jamči, da:

- je bil seznanjen s politiko SIMoD PKI in pravili SIMoD-CA-Restricted pred podpisom zahtevka za izdajo digitalnega potrdila,
- ravna v skladu s politiko SIMoD-PKI, pravili SIMoD-CA-Restricted in drugimi pravnimi akti,
- spremlja obvestila izdajatelja SIMoD-CA-Restricted in ravna v skladu z njimi,
- je prijavni službi ali operativnemu osebju posredoval popolne in točne podatke,
- se strinja z javno objavo svojega digitalnega potrdila.

Obveznosti imetnikov glede uporabe zasebnih ključev in digitalnih potrdil so določene v podpoglavju 4.5.1 Uporaba ključev in digitalnih potrdil imetnikov.

9.6.4. Odgovornost in jamstva tretjih oseb

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

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

9.6.5. Odgovornost in jamstva drugih udeležencev

Ni predpisano.

9.7. Zanikanje odgovornosti

Izdajatelj SIMoD-CA-Restricted ni odgovoren za škodo, ki izhaja iz uporabe digitalnih potrdil in z njimi povezanih ključev, če:

- je bilo digitalno potrdilo izdano kot rezultat napake ali neverodostojnosti podatkov v zahtevku,
- je bilo digitalno potrdilo spremenjeno,
- 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 in pravili SIMoD-CA-Restricted,
- imetnik ali tretja oseba ni postopala v skladu s predpisanimi postopki v politiki SIMoD-PKI ali pravilih SIMoD-CA-Restricted,
- je nastala škoda zaradi napake v delovanju strojne ali programske opreme,
- je do ravnanja v nasprotju s politiko SIMoD-PKI ali pravili SIMoD-CA-Restricted prišlo zaradi višje sile.

9.8. Omejitve odgovornosti

Skladno s predpisi.

9.9. Zavarovanje pred škodo zaradi neizpolnjevanja obveznosti

Skladno s predpisi.

9.10. Začetek in prenehanje veljavnosti

9.10.1. Začetek veljavnosti

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

Pravil SIMoD-SIMoD-CA-Restricted začnejo veljati in se uporabljati naslednji dan po podpisu.

9.10.2. Prenehanje veljavnosti

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

9.10.3. Posledice prenehanja veljavnosti

Po prenehanju veljavnosti pravil SIMoD-CA-Restricted zaradi objave nove verzije imetniki praviloma uporabljajo obstoječa potrdila v skladu z določili pravil SIMoD-CA-Restricted, po kateri so bila izdana.

9.11. Obvestila in komuniciranje z udeleženci

Izdajatelj SIMoD-CA-Restricted 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-Restricted.

9.12.2. Postopek obveščanja in rok za pripombe

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

9.12.3. Spremembe, ki zahtevajo novo identifikacijsko oznako politike

Kolegij organizacijske enote, pristojne za informatiko odloči, ali so spremembe pravil SIMoD-CA-Restricted take, da zahtevajo objavo novih pravil in spremembo identifikacijskih oznak politik delovanja.

9.13. Reševanje sporov

V skladu s predpisi.

9.14. Predpisi in priporočila

Izdajatelj SIMoD-CA-Restricted 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]	ETSI EN 319 412	Electronic Signatures and Infrastructures (ESI); Certificate Profiles:
[7]	ETSI EN 319 412-1	Part 1: Overview and common data structures
[8]	ETSI EN 319 412-2	Part 2: Certificate profile for certificates issued to natural persons
[9]	ETSI EN 319 412-3	Part 3: Certificate profile for certificates issued to legal persons
[10]	ETSI EN 319 412-4	Part 4: Certificate profile for web site certificates
[11]	ETSI EN 319 412-5	Part 5: QCStatements
[12]	CC EAL5+ / PP QSCD	Certification based on Common Criteria Protection Profiles EN 419211 part 1 to 6, as mandated by eIDAS
[13]	politika SIMoD-PKI	Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, Verzija 3.1
[14]	pravila SIMoD-CA-Root	Pravila delovanja izdajatelja SIMoD-CA-Root, ver. 3.1
[15]	RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[16]	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[17]	RFC 4210	Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
[18]	PKCS#10	Certification Request Syntax Standard

[19] RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OSCP

[20] ZObr Zakon o obrambi (Uradni list RS, št. 103/04 – UPB1, 95/15)

[21] ZTP Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – UPB2, 9/10, 60/11)

[22] ZVOP-1 Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – UPB1)

Delovanje izdajatelja SIMoD-CA-Restricted opredeljujejo še naslednji dokumenti:

A.1. Načrt varovanja tajnih podatkov v prostorih izdajatelja SIMoD-CA-Restricted

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

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

A.4. Postopek obnove ključev overitelja SIMoD-CA-Restricted

A.5. Postopkovnik o tehnični arhitekturi infrastrukture SIMoD-PKI

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

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