REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Pravila delovanja izdajatelja SIMoD-CA-Restricted, javni del

(Javna pravila SIMoD-CA-Restricted)

Verzija 3.0

NEURADNO PREČIŠČENO BESEDILO

marec 2018

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

Izdaja:	Spremembe glede na prejšnjo izdajo:
Neuradno prečiščeno besedilo Pravil delovanja izdajatelja SIMoD-CA-Restricted, javni del, verzija 3.0, marec 2018	Združena sta dokumenta Pravila delovanja izdajatelja SIMoD-CA-Restricted, javni del, verzija 3.0, številka: 382-12/2017-41 in Pravila o spremembi in dopolnitvah Pravil delovanja izdajatelja SIMoD-CA-Restricted, javni del, verzija 3.0, številka: 386-12/2018-16.
Pravila o spremembi in dopolnitvah Pravil delovanja izdajatelja SIMoD-CA-Restricted, javni del, verzija 3.0, številka: 386-12/2018-16: datum: 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, predvsem glede okoliščin in načina obveščanja nadzornega organa. Dodana je obveza rednega pregledovanja Pravil delovanja izdajatelja SIMoD-CA-Restricted in ostalih dokumentov, povezanih z delovanjem izdajatelja SIMoD-CA-Restricted. Dodana je tehnična varnostna kontrola oziroma obveza rednega izvajanja vdornih testov in testov ranljivosti. Dodane so določbe glede preverjanja skladnosti oziroma nadzora izdajatelja SIMoD-CA-Restricted kot ponudnika storitev zaupanja v skladu z Uredbo eIDAS.
Pravila delovanja izdajatelja SIMoD-CA-Restricted, javni del, verzija 3.0	Uskladitev z Uredbo (EU) št. 910/2014 Evropskega parlamenta in sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES. Uskladitev s spremembami ETSI priporočil. Uskladitev izrazov; konsistentna uporaba izrazov »overitelj« in »izdajatelj«. Ukinjena je možnost izdaje digitalnega potrdila po preklicu v izjemnih primerih brez identifikacije v prijavni službi in na osnovi zahtevka brez podpisa vodje organizacijske enote. Ukinjena omejitev ponovne izdaje digitalnih potrdil brez preverjanja istovetnosti maksimalno dvakrat (2x) zaporedoma. Veljavnost digitalnega potrdila in ključev izdajatelja SIMoD-CA-Restricted je povečana na dvajset (20) let. Podaljšanje obdobja veljavnosti digitalnih potrdil in ključev.

Pravila o spremembah in dopolnitvah Pravil delovanja overitelja SIMoD-CA-Restricted, javni del, verzija 2.0, številka: 386-11/2014-23, datum: 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.
Neuradno prečiščeno besedilo Pravil delovanja overitelja SIMoD-CA-Restricted, javni del, verzija 2.0	Združena sta dokumenta Pravila delovanja overitelja SIMoD-CA-Restricted, javni del, verzija 2.0, številka: 382-5/2006-121 in Pravila o dopolnitvah in spremembah Pravil delovanja overitelja SIMoD-CA-Restricted, javni del, verzija 2.0, številka: 386-6/2011-336.
Pravila o dopolnitvah in spremembah Pravil delovanja overitelja SIMoD-CA-Restricted, javni del, verzija 2.0, številka: 386-6/2011-336, datum: 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; predpisan je postopek preverjanja istovetnosti in obdelave zahtevka za ponovno izdajo digitalnega potrdila v izjemnem primeru, • odstranjena so določila, ki se nanašajo na korenskega overitelja SIMoD-CA-Root.
Pravila delovanja overitelja SIMoD-CA-Restricted, javni del, verzija 2.0, številka: 382-5/2006-121, datum: 23.11.2010	• Pristojnost sprejemanja Pravil delovanja overitelja SIMoD-CA-Restricted je prenesena 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 ZEPEP in priporočili ETSI, • podrobneje so definirane zahteve za kvalificirana digitalna potrdila, • dodana so polja v kvalificiranih digitalnih potrdilih, • 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, • poenostavljen je postopek pridobitve digitalnih potrdil NIZKE stopnje zaupanja.

Spremembe in dopolnitve Pravil delovanja overitelja SIMoD-CA-Restricted, javni del, številka: 382-5/2006-44, datum: 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, datum: 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, datum: 29.07.2005.	

KAZALO

PRAVILA DELOVANJA IZDAJATELJA SIMoD-CA-Restricted
JAVNI DEL

(JAVNA PRAVILA SIMoD-CA-Restricted)

Verzija 3.0

1. UVOD

1.1. Pregled

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

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

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

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 okviru SIMOD-PKI, katere delovanje predpisuje [16] Politika SIMoD-PKI. [16] Politika SIMoD-PKI predpisuje splošne zahteve za digitalna potrdila, minimalne zahteve za tehnične lastnosti in raven varnosti infrastrukture izdajateljev, postopke za upravljanje z digitalnimi potrdili, obveznosti in odgovornosti, ki jih morajo izpolnjevati izdajatelji, imetniki ter tretje osebe, ki se zanašajo na digitalna potrdila ter drugi izdajatelji, ki se želijo povezovati z infrastrukturo javnih ključev na MO.

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

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

Javna pravila SIMoD-CA-Restricted, podajajo opis izdajateljeve infrastrukture, postopkov izdajatelja in izpolnjevanje zahtev Politike SIMoD-PKI. Za oceno zaupanja v SIMoD-PKI kot celoto je potrebno poleg tega dokumenta upoštevati še dokumenta [16] Politika SIMoD-PKI in [17] 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 datotek, sporočil in elektronskih obrazcev,
- prepoznavanje in preverjanje istovetnosti oseb in gradnikov informacijske infrastrukture kot so strežniki, usmerjevalniki, požarne pregrade in imeniki,
- nezanikanje oddaje ali sprejema sporočil in
- ustvarjanje časovnih žigov.

Izdajatelj SIMoD-CA-Restricted loči dva tipa digitalnih potrdil glede na možnost njihovega upravljanja na:

- upravljana digitalna potrdila, imenovana tudi *Entrust ID*[1],
- neupravljana digitalna potrdila, imenovana tudi spletna[2] ali WEB[3] digitalna potrdila.

Izdajatelj SIMoD-CA-Restricted glede na namen uporabe zasebnega ključa izdaja naslednja digitalna potrdila za:

- preverjanje digitalnega podpisa,
- šifriranje,
- preverjanje digitalnega podpisa in šifriranje (z dvojno uporabo, ang. dual usage),
- izdajatelje varnih časovnih žigov in
- sisteme za sprotno preverjanje statusa digitalnih potrdil (ang. Online Certficate Status Protocol, OCSP)

Izdajatelj SIMoD-CA-Restricted izdaja digitalna potrdila v naslednjih kombinacijah:

upravljana digitalna potrdila (*Entrust ID*)	
skupek dveh (2) digitalnih potrdil	digitalno potrdilo za preverjanje digitalnega podpisa
	digitalno potrdilo za šifriranje
eno (1) digitalno potrdilo	digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje (z dvojno uporabo)
neupravljana digitalna potrdila (spletna, *WEB*)	
eno (1) digitalno potrdilo	digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje (z dvojno uporabo)

Dokument je skladen z [18] 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] Poimenovanje upravljanih digitalnih potrdil v okviru uporabljene tehnološke rešitve.

[2] Ime spletno digitalno potrdilo izhaja iz zgodovine oziroma prvotnega namena uporabe neupravljanih potrdil; tovrstna digitalna potrdila se pretežno uporabljajo v spletnem okolju.

[3] Namesto spletna digitalna potrdila se pogosto uporablja angleški izraz WEB digitalna potrdila.

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	Stopnja zaupanja	Identifikacijske oznake politik	Identifikacija ETSI EN 319 411-2
Fizične osebe	Digitalno potrdilo za preverjanje digitalnega podpisa	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.1.2, 0.4.0.194112.1.2	QCP-n-qscd
	Digitalno potrdilo za šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.2.2	
	Digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.1.3.2, 0.4.0.194112.1.2	QCP-n-qscd
	Digitalno potrdilo za preverjanje digitalnega podpisa	SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.1.1.2, 0.4.0.194112.1.0	QCP-n
	Digitalno potrdilo za šifriranje	SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.1.2.2	
	Digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje	SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.1.3.2, 0.4.0.194112.1.0	QCP-n
	Digitalno potrdilo za preverjanje digitalnega podpisa	NIZKA	1.3.6.1.4.1.22295.10.1.2.2.1.1.2	
	Digitalno potrdilo za šifriranje	NIZKA	1.3.6.1.4.1.22295.10.1.2.2.1.2.2	
	Digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje	NIZKA	1.3.6.1.4.1.22295.10.1.2.2.1.3.2	
Splošni nazivi (org. enote MO, funkcijske ter organizacijske vloge	Digitalno potrdilo za preverjanje elektronskega žiga in šifriranje	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.3.3.2, 0.4.0.194112.1.3	QCP-l-qscd
		SREDNJA	1.3.6.1.4.1.22295.10.1.1.2.3.3.2, 0.4.0.194112.1.1	QCP-l
		NIZKA	1.3.6.1.4.1.22295.10.1.2.2.3.3.2	
Strežniki, druga strojna in programska oprema.	Digitalno potrdilo za preverjanje digitalnega 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 varnih časovnih žigov	Digitalno potrdilo za overjanje varnih časovnih žigov	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.5.4.2	
Sistemi za preverjanje veljavnosti digitalnih potrdil (OCSP)	Digitalno potrdilo overjanje odzivov OCSP	VISOKA	1.3.6.1.4.1.22295.10.1.1.1.6.5.2	
Sistemi za podpis programske kode	Digitalno potrdilo za preverjanje digitalnega 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

Izdajatelj SIMoD-CA-Restricted je podrejeni izdajatelj korenskega izdajatelja SIMoD-CA-Root in izdaja digitalna potrdila za potrebe uporabnikov in aplikacij v omrežju KIS MO in SV, klasificiranem za prenos podatkov stopnje tajnosti INTERNO.

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

1.3.1.1. Svet za upravljanje z infrastrukturo javnih ključev na MO

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

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

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

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

- obvesti nadzorni organ, kot ga določa [2] Uredba o izvajanju eIDAS, o vseh dejstvih, okoliščinah in spremembah, vezanih na status izdajatelja SIMoD-CA-Restricted kot ponudnika kvalificiranih storitev zaupanja,
- brez nepotrebnega odlašanja, v vsakem primeru pa v 24 urah po ugotovitvi, uradno obvesti nadzorni organ, po potrebi pa tudi druge pristojne organe, kot je pristojni nacionalni organ za varnost informacij ali organ za varstvo podatkov, o kršitvah varnosti ali izgubi celovitosti, ki znatno vpliva na storitev zaupanja ali na osebne podatke, vsebovane v njej.

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

1.3.1.2. Operativno osebje izdajatelja SIMoD-CA-Restricted

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

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. Osebje prijavne službe imenuje vodja organizacijske enote MO, pristojne za kadrovske zadeve.

1.3.3. Imetniki digitalnih potrdil

Imetniki digitalnih potrdil izdajatelja SIMoD-CA-Restricted so:

- fizične osebe - zaposleni v MO,

- organizacijske enote in organi v sestavi MO (v nadaljevanju organizacijske enote MO),
- funkcijske in organizacijske vloge, povezane z opravljanjem vojaških ali drugih nalog s področja obrambe,
- strežniki in druga strojna ter programska oprema,
- izdajatelji varnih časovnih žigov in
- sistemi za sprotno preverjanje veljavnosti digitalnih potrdil (OCSP).

Odgovorna oseba za digitalno potrdilo za organizacijske enote MO je njen vodja.

Odgovorna oseba za digitalno potrdilo za funkcijsko ali organizacijsko vlogo je nosilec, skrbnik ali administrator vloge.

Odgovorna oseba za digitalno potrdilo za strežnike in drugo strojno ter programsko opremo je skrbnik strežnika, druge strojne ali programske opreme.

Odgovorna oseba za digitalno potrdilo za izdajatelje varnih časovnih žigov in druge ponudnike storitev overjanja je vodja organizacijske enote MO, ki upravlja z izdajateljem varnega časovnega žiga ali drugim ponudnikom storitev overjanja.

Odgovorne osebe imajo glede digitalnega potrdila enake obveznosti kot fizične osebe.

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 digitalno potrdilo izdajatelja SIMoD-CA-Restricted in korenskega izdajatelja SIMoD-CA-Root.

1.3.5. Posredno odgovorni organi

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

1.4. Namen uporabe digitalnih potrdil

1.4.1. Dovoljena uporaba digitalnih potrdil

Namen uporabe digitalnih potrdil izdajatelja SIMoD-CA-Restricted je določen z namenom uporabe pripadajočih ključev, glej tudi poglavje 6.1.7 Namen uporabe ključev:

Vrsta digitalnega potrdila	Namen uporabe zasebnega ključa	Namen uporabe javnega ključa oziroma digitalnega potrdila
za preverjanje digitalnega podpisa / elektronskega žiga	digitalno podpisovanje / kreiranje elektronskega žiga	preverjanje digitalnega podpisa / elektronskega žiga
za šifriranje	dešifriranje[4]	šifriranje[5]
za preverjanje digitalnega podpisa / elektronskega žiga in šifriranje	digitalno podpisovanje / kreiranje elektronskega žiga in dešifriranje	preverjanje digitalnega podpisa / elektronskega žiga in šifriranje
za izdajatelja varnih časovnih žigov	digitalno podpisovanje varnih časovnih žigov	preverjanje varnih časovnih žigov
za sisteme OSCP	digitalno podpisovanje odzivov OCSP	preverjanje odzivov OCSP
za sisteme za podpis programske kode	digitalno podpisovanje programske kode	preverjanje digitalnega podpisa programske kode

[4] Zasebni ključ se uporablja za dešifriranje dejanskih simetričnih šifrirnih ključev.

[5] Javni ključ se uporablja za šifriranje dejanskih simetričnih šifrirnih ključev.

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 in elektronsko podpisovanje oz. naprave za ustvarjanje elektronskega podpisa, za končne uporabnike je to običajno pametna kartica	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 izdajatelja SIMoD-CA-Restricted se morajo uporabljati v skladu s Politiko SIMoD-PKI in Pravili delovanja izdajatelja SIMoD-CA-Restricted. Namenjena so izključno službeni uporabi v MO, v drugih institucijah pa je namen omejen na opravljanje nalog povezanih z obrambo države.

1.4.2. Nedovoljena uporaba digitalnih potrdil

Ni relevantno.

1.5. Upravljanje s Pravili delovanja SIMoD-CA-Restricted

1.5.1. Organ, ki upravlja s tem dokumentom

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

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

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

1.5.2. Kontaktna oseba

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

1.5.3. Odgovorni organ za odobritev skladnosti Pravil delovanja izdajatelja SIMoD-CA-Restricted s Politiko SIMoD-PKI

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

1.5.4. Postopek odobritve Pravil delovanja izdajatelja SIMoD-CA-Restricted

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

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

1.6. Pojmi in kratice

Pojem	Definicija
Časovni žig	Elektronsko podpisano potrdilo, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času.
Digitalni podpis	Dodan podatek ali kriptografsko preoblikovanje, ki omogoča, da prejemnik podatkov preveri njihov izvor in integriteto, ter s tem prepreči poneverbo.
Digitalno potrdilo	Potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto. V tem dokumentu uporabljen kot ekvivalenten izraz za »potrdilo za elektronski podpis« po [3] eIDAS.
Digitalno potrdilo 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 digitalnega podpisa, preverjanje istovetnosti uporabnikov in preverjanje celovitosti podatkov v elektronski obliki.
Digitalno potrdilo za šifriranje	Digitalno potrdilo, ki se uporablja za izmenjavo simetričnih šifrirnih ključev pri zagotavljanju tajnosti podatkov v elektronski obliki.
Elektronski podpis	Niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika.
Elektronsko sporočilo	Niz podatkov, ki so poslani ali prejeti na elektronski način, kar vključuje predvsem elektronsko izmenjavo podatkov in elektronsko pošto.
Elektronski žig	Po definiciji 27. odstavka 3. člena [3] eIDAS 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 običajno v skladu s standardom X.500 oziroma razširjenim standardom X.509 ver.3.
Imetnik potrdila	Fizična oseba, navedena v digitalnem potrdilu v polju »Subject«. Lastnik zasebnega ključa, ki ustreza javnemu ključu, vsebovanem v digitalnem potrdilu oziroma odgovorna oseba za uporabo digitalnega potrdila.

Informacijski sistem	Skupek naprav in postopkov, ki omogočajo obdelavo informacij oziroma nudijo informacijske storitve. Združuje računalniško strojno in programsko opremo, računalniške nosilce podatkov, podatkovne zbirke in druge naprave ter identifikacijske, avtorizacijske, upravljavske in nadzorne postopke v funkcionalno celoto.
Javni ključ	Ključ iz para ključev, ki je lahko javno objavljen.
Javni komunikacijsko informacijski sistem	Komunikacijsko informacijski sistem, katerega storitve so namenjene javni uporabi.
Komunikacijski sistem	Skupek naprav in postopkov, ki omogočajo prenos informacij. Primeri takih sistemov so telekomunikacijski sistemi in računalniška omrežja.
Komunikacijsko informacijski sistem	Skupen izraz za komunikacijski in informacijski sistem.
Kvalificirano digitalno potrdilo	Digitalno potrdilo, ki izpolnjuje zahteve iz 28. člena ZEPEP. Izda ga overitelj, ki deluje v skladu z zahtevami iz 28. do 36. člena ZEPEP.
Naprava	V tem dokumentu izraz uporabljen za strežnik, drugo strojno ali programsko opremo, izdajatelja varnih časovnih žigov, sistem za preverjanje veljavnosti digitalnih potrdil ali drugega ponudnika storitev overjanja.
Naprava za ustvarjanje elektronskega podpisa	Po definiciji 22. odstavka 3. člena [3] 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 [3] eIDAS naprava za ustvarjanje elektronskega podpisa, ki izpolnjuje zahteve iz Priloge II [3] eIDAS.
Naročnik potrdila	Fizična ali pravna oseba, ki z zahtevkom zaprosi za izdajo digitalnega potrdila.
Oprema za elektronsko podpisovanje	Strojna ali programska oprema ali njune specifične sestavine, ki jo izdajatelj uporablja za storitve v zvezi z elektronskim podpisovanjem ali ki se uporabljajo za oblikovanje ali preverjanje elektronskih podpisov.
Overitelj	Fizična ali pravna oseba, ki izdaja digitalna potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi.
Par ključev	Par asimetričnih kriptografskih ključev, ki ga sestavljata zasebni in javni ključ.
Podatki v elektronski obliki	Podatki, ki so oblikovani, shranjeni, poslani, prejeti ali izmenljivi na elektronski način.
Podatki za elektronsko podpisovanje	Edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa.
Podatki za preverjanje elektronskega podpisa	Edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa.
Podpisnik	Oseba, ki ustvari ali je v njenem imenu in v skladu z njeno voljo ustvarjen elektronski podpis.
Ponudnik storitev zaupanja	Po definiciji 19. odstavka 3. člena [3] eIDAS: fizična ali pravna oseba, ki zagotavlja eno ali več storitev zaupanja.
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.
Pošiljatelj elektronskega sporočila	Oseba, ki je sama poslala elektronsko sporočilo ali pa je bilo sporočilo poslano v njenem imenu in v skladu z njeno voljo; posrednik elektronskega sporočila se ne šteje za pošiljatelja tega elektronskega sporočila.
Potrdilo za elektronski podpis	Po definiciji 14. odstavka 3. člena [3] eIDAS: elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega podpisa s fizično osebo in potrjuje vsaj ime ali psevdonim te osebe. V tem dokumentu se namesto izraza »potrdilo za elektronski podpis« uporablja izraz »digitalno potrdilo«.

Potrdilo za elektronski žig	Po definiciji 29. odstavka 3. člena [3] eIDAS: elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega žiga s pravno osebo in potrjuje ime te osebe.
Prejemnik elektronskega sporočila	Oseba, ki je prejela elektronsko sporočilo; posrednik elektronskega sporočila se ne šteje za prejemnika tega elektronskega sporočila.
Prijavna služba	Služba oziroma organizacija, ki po pooblastilu izdajatelja sprejema zahtevke in preverja istovetnosti bodočih imetnikov.
Selektivno omejevanje dostopa	Ločevanje dostopa glede na upravičen interes.
Sredstvo za elektronsko podpisovanje	Nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa.
Sredstvo za varno elektronsko podpisovanje	Sredstvo za elektronsko podpisovanje, ki izpolnjuje zahteve iz 37. člena ZEPEP.
Storitev zaupanja	Elektronska storitev po definiciji 16. odstavka 3. člena [3] eIDAS: a) ustvarjanje, preverjanje in potrjevanje veljavnosti elektronskih podpisov, elektronskih žigov ali elektronskih časovnih žigov, storitev elektronske priporočene dostave in potrdil, povezanih s temi storitvami, ali b) ustvarjanje, preverjanje in potrjevanje veljavnosti potrdil za avtentikacijo spletišč ali c) hrambo elektronskih podpisov, žigov ali potrdil, povezanih s temi storitvami.
Šifrirni (kriptografski) ključ	Niz znakov uporabljen za kriptografsko preoblikovanje (npr. šifriranje, dešifriranje, podpisovanje, ali preverjanje podpisa).
Tajni podatek	Dejstvo ali sredstvo iz delovnega področja organa, ki se nanaša na javno varnost, obrambne zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov določenih v [25] ZTP določiti in označiti kot tajno ter zaščititi pred nepooblaščenimi osebami.
Tretja oseba	Subjekt, ki ni aktivno udeležen v storitev, vendar zaupa izvajalcu in rezultatu storitve.
Uporabnik	Naročnik ali imetnik digitalnega potrdila.
Varen časovni žig	Elektronsko podpisano potrdilo, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času (2. člen ZEPEP). Varen časovni žig mora vsebovati nedvoumne in pravilne podatke o datumu, točnem času najmanj na sekundo natančno in izdajatelju, ki je varni časovni žig ustvaril. Varni časovni žig je lahko dokumentu dodan ali priložen in z njim povezan, vendar morajo biti pri tem vedno izpolnjene enake zahteve kot za varen elektronski podpis s kvalificiranim digitalnim potrdilom.
Varen elektronski podpis	Elektronski podpis, ki izpolnjuje naslednje zahteve: • povezan je izključno s podpisnikom, • iz njega je mogoče zanesljivo ugotoviti podpisnika, • ustvarjen je s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom, • povezan je s podatki, na katere se nanaša, tako, da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi.
Zasebni komunikacijsko informacijski sistem	Komunikacijsko informacijski sistem, ki ni javen in je v lasti, upravljanju in pod nadzorom neke privatne, vladne ali nevladne organizacije.
Zasebni ključ	Ključ iz para ključev, ki mora ostati skriven, da se zagotovi zaupnost in celovitost podatkov v elektronski obliki.
Zloraba	Razkritje tajnega podatka, izguba celovitosti ali razpoložljivosti podatka.

Kratica	Opis
CN	Splošno ime objekta v imeniku (ang. Common Name).
CRL	Register preklicanih potrdil (ang. Certificate Revocation List).
DN	Razločevalno ime objekta v imeniku, tudi polno ime objekta v imeniku (ang. Distinguished Name).
eIDAS	Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (eIDAS; Uradni list EU, št. L 257/73).
ETSI	Evropski inštitut za standardizacijo na področju telekomunikacij; izdaja serijo standardov s področja elektronskega podpisa in delovanja overiteljev (ang. European Telecommunications Standards Institute).
FIPS	Standardi za informacijske tehnologije, ki so v uporabi v ameriških zveznih institucijah. Izdaja jih ameriški nacionalni inštitut za standarde in tehnologijo (ang. Federal Information Processing Standards).
FIPS 140-2	Serija standardov FIPS za kriptografske module.
FQDN	Popolno ime naprave v domenskem sistemu (ang. Fully Qualified Domain Name).
HTTP	Protokol za prenos podatkov v spletnem okolju (ang. Hypertext Transfer Protocol).
IETF	Združenje strokovnjakov s področja Internetnih tehnologij. Izdelujejo serije priporočil (ang. Internet Engineering Task Force).
ISO	Mednarodna organizacija za standardizacijo (ang. International Standardization Organization).
ITU-T	Mednarodna organizacija za standardizacijo na področju telekomunikacij (ang. International Telecommunications Union - Telecommunication Standardization Sector).
KIS MO in SV	Komunikacijsko informacijski sistem MO in SV.
LDAP	Protokol, ki določa dostop do imenika in je specificiran po IETF (ang. Internet Engineering Task Force) priporočilu RFC 1777 (LDAP, ang. Leightweight Directory Access Protocol).
MO	Ministrstvo za obrambo.
PKCS	Priporočila podjetja RSA Security za uporabo asimetričnih kriptografskih algoritmov (ang. Public Key Cryptographic Standards).
PKCS#1	Osnovna pravila za formatiranje podatkov ob implementaciji RSA funkcij. Predpisuje, kako se izračuna digitalni podpis, kako se formatirajo podatki, ki se podpisujejo in format podpisa. Predpisuje tudi sintakso javnega in zasebnega RSA ključa.
PKCS#10	Sintaksa zahtevka za digitalno potrdilo. Zahtevek za digitalno potrdilo vsebuje razločevalno ime, javni ključ in nabor drugih atributov, ki jih podpiše subjekt, ki zahteva potrditev. Daljše ime: PKCS#10 Certification Request Syntax Standard.
PKCS#7	Sintaksa za kriptografsko obdelane podatke, kot digitalni podpisi in digitalne ovojnice.
PKI	Infrastruktura javnih ključev; strojna in programska oprema ter varnostni mehanizmi za zaupanja vredno implementacijo varnostnih storitev, ki temeljijo na nesimetrični kriptografiji (ang. Public Key Infrastructure).
PKIX	Delovna skupina za področje infrastrukture javnih ključev v okviru IETF (ang. Internet Engineering Task Force). Izdala serijo priporočil za digitalna potrdila in registre preklicanih potrdil (ang. Public Key Infrastrukture X.509).
PKIX- CMP	Postopek izmenjave podatkov, ki se nanašajo na digitalna potrdila med subjekti infrastrukture overitelja (ang. PKIX Certificate Management Protocol). Vključuje PKCS#7 in PKCS#10.
QCP	oznaka ETSI politike za kvalificirana potrdila (ang. Qualified Certificate Policy); [7] ETSI EN 319 411-2

QSCD	Naprava za ustvarjanje kvalificiranega elektronskega podpisa (ang. Qualified Signature/Seal Creation Device); [7] ETSI EN 319 411-2
RDN	Kratko razločevalno ime objekta v imeniku, praviloma sestavljeno in splošnega imena (ang. Common Name, CN) in serijske številke (ang. serialNumber)
RFC	Priporočila, ki jih izdaja IETF.
RFC 5280	Priporočilo, ki določa elemente potrdil in registra preklicanih potrdil.
RFC 3647	Priporočilo, ki določa elemente, ki naj bodo zajeti v politiki overitelja (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework).
RFC 4043	Priporočilo, ki definira posebno polje *Permanent Identifier* v razširitvi *subjectAltName* v digitalnih potrdilih.
RFC 4210	Priporočilo, ki določa postopke za izmenjavo podatkov, ki se nanašajo na digitalna potrdila. Vsebuje PKIX-CMP.
RSA	Eden prvih nesimetričnih kriptografskih sistemov, patentiran leta 1983, imenovan po odkriteljih: Rivest, Shamir in Adelman.
SIMoD-PKI	Infrastruktura javnih ključev Ministrstva za obrambo Republike Slovenije (ang. **S**loven**i**an **M**inistry **o**f **D**efence **P**ublic **K**ey **I**nfrastructure - SIMoD-PKI)
SV	Slovenska vojska
X.501	Standard organizacij ITU-T in ISO, ki definira poimenovanje objektov v imeniku. Tudi del serije PKIX Part1.
X.509	Standard organizacij ITU-T in ISO, ki definira strukturo digitalnih potrdil. Eden izmed serije standardov ITU-ISO s področja imenikov. Tudi del RFC 5280.

2. ODGOVORNOST ZA OBJAVE IN IMENIK

2.1. Repozitoriji

Podatki o 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 računalniških omrežjih, ki med seboj niso povezana. Vsi imajo naslov imenik.simod-pki.mors.si.

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

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

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

2.2. Objave informacij o digitalnih potrdilih

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

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

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

- digitalno potrdilo izdajatelja SIMoD-CA-Restricted,
- kombinirani register preklicanih potrdil izdajatelja SIMoD-CA-Restricted,
- Javna pravila SIMoD-CA-Restricted in
- druge javne objave.

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 – zaposleni v MO in zaposleni v institucijah, ki opravljajo naloge povezane z obrambo
ou=cert-splosno-<X>, organizationIdentifier =VATSI-47978457, o=Ministrstvo za obrambo, c=SI	• organizacijske enote MO, • splošni nazivi • institucije, ki opravljajo naloge povezane z obrambo
ou=cert-naprave-<X>, organizationIdentifier =VATSI-47978457, o=Ministrstvo za obrambo, c=SI	• strežniki in druga strojna ter programska oprema • izdajatelji varnih 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 opravljenem preklicu. Pogostost objav registrov preklicanih potrdil je opisana v poglavju 4.9.7 Pogostost objav registrov preklicanih potrdil.

2.4. Dostop do podatkov v repozitorijih

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

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

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

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

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 [19] RFC 5280, [11] ETSI EN 319 412-2, [12] ETSI EN 319 412-3 ter [13] ETSI EN 319 412-4.

Razločevalno ime izdajatelja je cn=SIMoD-CA-Restricted,ou=simod-pki,o=mors,c=si in je shranjeno v polju Issuer digitalnega potrdila.

Razločevalno ime imetnika je shranjeno v polju Subject digitalnega potrdila. V tabeli so različne oblike razločevalnega imena, glede na vrsto imetnika:

Fizične osebe	cn=<splošno ime> + givenName=<ime> + sn=<priimek>, ou=cert-osebe-<X>, organizationIdentifier=VATSI-47978457, o=Ministrstvo za obrambo, c=SI
Splošni nazivi	cn=<splošno ime> + description=<opis>, ou=cert-splosno-<X>, organizationIdentifier=VATSI-47978457, o=Ministrstvo za obrambo, c=SI
Naprave	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.

Imetnik ima lahko tudi eno ali več alternativnih imen, ki so zapisana v razširitvenem polju digitalnega potrdila *subjectAltName* v skladu z [19] RFC 5280. Tip alternativnega imena je običajno:

- *rfc822Name*; vrednost polja je naslov elektronske pošte v skladu z [19] RFC 5280 ali
- *DNS Name*; vrednost je domensko ime strežnika ali naprave.

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 izdajatelja si pridržujejo pravico za zavrnitev imena, če je neprimerno oziroma žaljivo, zavajajoče za tretje osebe, oziroma pripada drugi pravni ali fizični osebi ali je v nasprotju z veljavnimi predpisi. V teh primerih prijavna služba in operativno osebje izdajatelja predlagata drugačno ime.

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

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

Splošno ime v digitalnih potrdilih za strežnike, drugo strojno ali programsko opremo praviloma vsebuje polno domensko ime naprave (ang. fully qualified domain name, FQDN), oziroma mora enolično in nedvoumno označevati storitev.

3.1.3. Anonimnost imetnikov in uporaba psevdonimov

Uporaba psevdonimov ni dovoljena. Izdaja digitalnih potrdil z zakrito identiteto imetnika oziroma mehanizmi zagotavljanja anonimnosti niso predvideni.

3.1.4. Pravila za interpretacijo različnih oblik imen

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

3.1.5. Edinstvenost imen

Razločevalno ime enolično označuje imetnika potrdila.

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

Pri digitalnih potrdilih za organizacijske enote in splošne nazive je v splošnem imenu praviloma tudi serijska številka entitete v imeniškem sistemu MO.

Pri digitalnih potrdilih za strežnike je že polno domensko ime naprave oziroma storitve, ki je v splošnem imenu, enolično.

3.1.6. Priznavanje, preverjanje istovetnosti in vloga zaščitenih znamk

Uporaba zaščitenih znamk v imenih je dovoljena samo nosilcem zaščitenih znamk. Izdajatelj SIMoD-CA-Restricted ne sme zavestno izdati digitalnega potrdila z imenom, ki vsebuje zaščiteno znamko naročniku, ki ni nosilec zaščitene znamke. Prijavna služba in operativno osebje niso dolžni preverjati pravic do uporabe zaščitenih znamk niti razčiščevati sporov glede zaščitenih znamk.

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

3.2. Preverjanje istovetnosti imetnikov ob prvi registraciji

3.2.1. Metode dokazovanja lastništva zasebnega ključa

Izdajatelj SIMoD-CA-Restricted preverja lastništvo zasebnega ključa, ki odgovarja javnemu ključu, vsebovanem v zahtevku. V ta namen morajo prosilci za izdajo digitalnega potrdila posredovati izdajatelju javni ključ:

- kot [22] PKCS#10 zahtevek ali
- po PKIX-CMP protokolu v skladu z [21] RFC 4210.

3.2.2. Preverjanje istovetnosti za imetnike, ki niso fizične osebe

3.2.2.1. Digitalna potrdila za splošne nazive

Zahtevek za pridobitev digitalnega potrdila za splošni naziv za organizacijsko enoto MO mora vsebovati njen uradni naziv, naslov in ime odgovorne osebe, ki je praviloma vodja organizacijske enote MO. Za pravilnost podatkov jamči odgovorna oseba s podpisom na zahtevku. Za zahtevke za pridobitev digitalnih potrdil SREDNJE in VISOKE stopnje zaupanja prijavna služba preveri podatke o odgovorni osebi v kadrovski evidenci in izvede osebno identifikacijo odgovorne osebe na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list ali vozniško dovoljenje).

Zahtevek za pridobitev digitalnega potrdila za splošne nazive za organizacijsko ali funkcijsko vlogo podpišeta nosilec, skrbnik ali administrator vloge in njegov nadrejeni poveljnik oziroma

vodja ustrezne organizacijske enote MO. Za pravilnost podatkov jamči poveljnik oziroma vodja s podpisom na zahtevku. Za zahtevke za pridobitev digitalnih potrdil SREDNJE in VISOKE stopnje zaupanja, prijavna služba preveri pristnost podatkov nosilca, skrbnika ali administratorja vloge v kadrovski evidenci in izvede njegovo osebno identifikacijo na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list, ali vozniško dovoljenje).

Za zahtevke za pridobitev digitalnih potrdil NIZKE stopnje zaupanja preverjanje podatkov in osebna identifikacija ni obvezna. Zahtevke prejme in obdela operativno osebje izdajatelja.

3.2.2.2. Digitalna potrdila za naprave

Zahtevek za pridobitev digitalnega potrdila naprave (strežnike, drugo strojno in programsko opremo, izdajatelje varnih časovnih žigov, sisteme za preverjanje veljavnosti digitalnih potrdil ter druge ponudnike storitev overjanja) izpolnita in podpišeta skrbnik naprave in vodja organizacijske enote MO.

Za zahtevke za pridobitev digitalnih potrdil SREDNJE in VISOKE stopnje zaupanja prijavna služba preveri podatke skrbnika v kadrovski evidenci in izvede osebno identifikacijo na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list, ali vozniško dovoljenje).

Za zahtevke za pridobitev digitalnih potrdil NIZKE stopnje zaupanja preverjanje podatkov in osebna identifikacija ni obvezna. Zahtevke prejme in obdela operativno osebje izdajatelja SIMoD-CA-Restricted.

3.2.3. Preverjanje istovetnosti za fizične osebe

Zahtevek za pridobitev digitalnega potrdila za zaposlene v MO izpolnita in podpišeta bodoči imetnik in vodja njegove organizacijske enote. Za pravilnost podatkov jamči vodja organizacijske enote s podpisom na zahtevku.

Za zahtevek za pridobitev digitalnih potrdil SREDNJE in VISOKE stopnje zaupanja prijavna služba preveri podatke o bodočem imetniku v kadrovski evidenci in izvede osebno identifikacijo na podlagi uradnega dokumenta s fotografijo (osebna izkaznica, potni list ali vozniško dovoljenje).

Za zahtevke za pridobitev digitalnih potrdil NIZKE stopnje zaupanja preverjanje podatkov in osebna identifikacija ni obvezna. Zahtevke prejme in obdela operativno osebje izdajatelja SIMoD-CA-Restricted.

3.2.4. Podatki o naročniku, ki se ne preverjajo

Prijavna služba ne preverja naslednjih podatkov, ki bodo vsebovani v digitalnem potrdilu:

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

Za pravilnost zgoraj navedenih podatkov jamči vodja organizacijske enote oziroma poveljnik enote SV.

3.2.5. Preverjanje pooblastil

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

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[6], ki so bila izdana po protokolu PKIX-CMP, imetnik izkaže svojo istovetnost s posedovanjem še veljavnega zasebnega ključa.

Rutinska ponovna izdaja neupravljanih digitalnih potrdil[7], izdanih z uporabo PKCS#10 protokola, ni možna. 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 še veljavnega zasebnega ključa.

3.3.2. Preverjanje istovetnosti za ponovno izdajo digitalnega potrdila po preklicu

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

3.4. Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila

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 izbrala ob oddaji zahtevka za izdajo digitalnega potrdila.

Osebna identifikacija ni obvezna.

[6] Imenovana tudi *Entrust ID.*

[7] Imenovana tudi spletna ali WEB digitalna 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 za fizične osebe lahko oddajo zaposleni v MO.

Zahtevek za pridobitev digitalnega potrdila za organizacijske enote MO oddajo predstojniki organizacijske enote vsaj na ravni vodje sektorja.

Zahtevek za pridobitev digitalnih potrdil za naprave oddajo skrbniki naprave.

4.1.2. Postopek bodočega imetnika 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.

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

Naročnik posreduje izpolnjen in podpisan 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.

V primeru pomanjkljivih podatkov, neupravičenosti do digitalnega potrdila ali neuspešnega preverjanja istovetnosti prijavna služba zavrne izdajo digitalnega potrdila SREDNJE ali VISOKE stopnje zaupanja.

V primeru pomanjkljivih podatkov 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 odgovornost in pravica prijavne službe. Obvestilo o zavrnitvi pošlje prijavna služba naročniku po elektronski pošti, odobritev zahtevka pa prijavna služba na varen način (v zapečateni kuverti) posreduje operativnemu osebju izdajatelja SIMoD-CA-Restricted.

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

Naročnik 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

Največji dopusten čas od sprejema zahtevka za pridobitev digitalnega potrdila in izdajo aktivacijskih podatkov, ki jih bodoči imetnik potrebuje za generiranje ključev, je enaindvajset (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 s postopki izdajanja digitalnega potrdila SREDNJE in VISOKE stopnje zaupanja po prejemu odobrenega zahtevka od prijavne službe.

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

Operativno osebje izdajatelja SIMoD-CA-Restricted zvede 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; referenčno številko po elektronski pošti, avtorizacijsko kodo pa v kuverti, zaščiteni pred nepooblaščenim pregledovanjem, po pošti s potrdilom o prevzemu.

Za digitalna potrdila z obvezno uporabo pametne kartice, kjer 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 dostavi imetniku na varen način.

4.3.1.1. Dostava zasebnega ključa imetniku

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

Ko izdajatelj generira zasebne ključe, kot je to v primeru dešifrirnih ključev s podporo za povrnitev zgodovine ključev, poteka prenos zasebnega ključa z uporabo protokola PKIX-CMP in je integralni del postopka za prevzem digitalnega potrdila.

Za digitalna potrdila z obvezno uporabo pametne kartice, kjer izdajatelj SIMoD-CA-Restricted ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, generira ključe operativno osebje. Izdajatelj SIMoD-CA-Restricted na varen način dostavi zasebni ključ imetniku skupaj s pametno kartico z digitalnim potrdilom.

4.3.1.2. Dostava izdajateljevega javnega ključa imetniku

Javni ključ izdajatelja SIMoD-CA-Restricted oziroma izdajateljevo digitalno potrdilo, ki vsebuje izdajateljev javni ključ, se pošlje bodočim imetnikom digitalnih potrdil, ki se prevzemajo po PKIX-CMP protokolu, v sklopu PKIX-CMP protokola kot integralni del postopka za prevzem digitalnega potrdila.

Javni ključ izdajatelja SIMoD-CA-Restricted oziroma izdajateljevo digitalno potrdilo, ki vsebuje izdajateljev javni ključ, se pošlje bodočim imetnikom digitalnih potrdil, ki se izdajajo na osnovi PKCS#10 zahtevka, po protokolu PKCS#7 kot integralni del postopka za prevzem digitalnega potrdila.

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

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 pošilja referenčno številko, in z obvestilom po pošti, s katerim mu pošilja avtorizacijsko kodo.

Za digitalna potrdila z obvezno uporabo pametne kartice, kjer izdajatelja 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.

Digitalno potrdilo je izdano, ko ga izdajatelj SIMoD-CA-Restricted objavi v imeniku iz poglavja 2.2. Objave informacij o digitalnih potrdilih.

4.4. Prevzem digitalnega potrdila

4.4.1. Postopek prevzema digitalnega potrdila

Izdaja digitalnega potrdila je neločljivo povezana s prevzemom digitalnega potrdila. Bodoči imetnik praviloma prevzame digitalno potrdilo z aktivacijskimi podatki: referenčno številko in avtorizacijsko kodo.

Veljavnost aktivacijskih podatkov je šestdeset (60) dni od izdaje.

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

Prevzem upravljanih digitalnih potrdil[8] se izvaja s programsko opremo Entrust Entelligence Security Provider. Navodila za namestitev in uporabo programske opreme se nahajajo na spletni strani http://www.simod-pki.mors.si.

Prevzem neupravljanih digitalnih potrdil[9] se izvaja preko spletnega vmesnika. Spletni naslov vmesnika in navodila za prevzem so dostopna na spletnem naslovu http://www.simod-pki.mors.si.

Za digitalna potrdila z obvezno uporabo pametne kartice, kjer izdajatelj SIMoD-CA-restricted ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, opravi prevzem digitalnega potrdila operativno osebje. Izdajatelj SIMoD-CA-Restricted nato pametno kartico s prevzetim digitalnim potrdilom na varen način posreduje imetniku.

Ob prevzemu digitalnega potrdila je imetnik dolžan preveriti vsebino digitalnega potrdila in polno pot digitalnih podpisov do korenskega izdajatelja SIMoD-CA-Root. S prvo uporabo oziroma če imetnik osem (8) dni od prevzema digitalnega potrdila izdajatelja ne obvesti o morebitnih napakah, velja, da je imetnik potrdil točnost podatkov v digitalnem potrdilu in da prevzema vse obveznosti in jamstva iz poglavja 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 poglavja 2.1. Repozitoriji. Izdajatelj SIMoD-CA-Restricted praviloma ne objavlja digitalnih potrdil z javnimi ključi za preverjanje podpisa.

4.4.3. Obveščanje drugih udeležencev o izdaji digitalnega potrdila

Ni predvideno.

[8] Imenovana tudi *Entrust ID.*

[9] Imenovana tudi spletna ali WEB potrdila digitalna potrdila.

4.5. Uporaba ključev in digitalnih potrdil

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

4.5.1. Uporaba ključev in digitalnih potrdil imetnikov

4.5.1.1. Zasebni ključi in digitalna potrdila izdajateljev

Izdajatelj SIMoD-CA-Restricted uporablja svoje zasebne ključe samo za podpisovanje digitalnih potrdil imetnikom, ki so določeni v poglavju 1.3.3 Imetniki digitalnih potrdil in svojemu operativnemu osebju ter za podpisovanje registrov preklicanih potrdil.

Operativno osebje izdajatelja SIMoD-CA-Restricted uporablja digitalna potrdila in pripadajoče ključe izključno za izvajanje nalog upravljanja z infrastrukturo izdajatelja SIMoD-CA-Restricted. V primeru, da izdajateljevi zaposleni potrebujejo ključe oziroma digitalna potrdila kot uporabniki oziroma za druge namene, kot je upravljanje z izdajateljevo infrastrukturo, morajo zaprositi za izdajo uporabniških digitalnih potrdil.

4.5.1.2. Zasebni ključi in digitalna potrdila prijavne službe

Osebje prijavne službe za izvajanje nalog prijavne službe ne potrebuje namenskih digitalnih potrdil.

4.5.1.3. Uporabniški zasebni ključi in digitalna potrdila

Imetnik digitalnega potrdila izdajatelja SIMoD-CA-Restricted je dolžan:

- uporabljati ključe in digitalna potrdila samo za namene, ki so definirani v Politiki SIMoD-PKI in Pravilih delovanja izdajatelja SIMoD-CA-Restricted,
- po prevzemu digitalnega potrdila preveriti podatke v digitalnem potrdilu in ob morebitnih napakah in problemih takoj obvestiti operativno osebje izdajatelja SIMoD-CA-Restricted oziroma zahtevati preklic digitalnega potrdila,
- vse spremembe, ki so povezane s digitalnimi potrdili, v osmih (8) dneh sporočiti prijavni službi ali operativnemu osebju izdajatelja SIMoD-CA-Restricted,
- uporabljati zasebne ključe in digitalna potrdila samo v obdobju njihove veljavnosti,
- digitalno podpisovati in/ali šifrirati le podatke, katerih veljavnost je krajša od veljavnosti digitalnega potrdila oziroma pred potekom veljavnosti digitalnega potrdila ponovno podpisati in/ali šifrirati podatke, če to ni rešeno na drug način (z aplikacijo),
- varovati svoje zasebne ključe in pametne kartice ali drugačne nosilce zasebnih ključev in upoštevati vse ukrepe, da se prepreči izguba, razkritje, sprememba ali nepooblaščena uporaba in
- ob sumu zlorabe svojega zasebnega ključa ukrepati po postopku, ki je opisan v poglavju 4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila.

4.5.2. Uporaba digitalnih potrdil s strani tretjih oseb

Tretja oseba je dolžna:

- pred uporabo digitalnega potrdila preveriti, ali je ustrezno za predvideno uporabo,
- uporabiti digitalno potrdilo le za namene, določene v Politiki SIMoD-PKI, Pravilih delovanja izdajatelja SIMoD-CA-Restricted oziroma pogodbi o medsebojnem priznavanju,
- ob domnevni zlorabi zasebnega ključa ali če so spremenjeni podatki iz digitalnega potrdila, na katerega se zanaša, obvestiti operativno osebje izdajatelja SIMoD-CA-Restricted,
- preveriti, če je bil digitalni podpis kreiran v času veljavnosti digitalnega potrdila,
- za vsako uporabljeno digitalno potrdilo izvesti popoln postopek preverjanja poti zaupanja,
- preveriti status digitalnega potrdila v veljavnem registru preklicanih potrdil in
- skrbeti za arhiv dokumentov.

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[10]

4.7.1. Razlogi za ponovno izdajo digitalnega potrdila

Ponovna izdaja digitalnega potrdila se izvede:

- po preklicu,
- po preteku veljavnosti,
- pred pretekom veljavnosti ali
- če je imetnik v obdobju veljavnosti digitalnega potrdila:
    - pozabil geslo za dostop do zasebnih ključev ali
    - izgubil ali poškodoval pametno kartico ali drugačen nosilec zasebnih ključev.

4.7.2. Kdo lahko zahteva ponovno izdajo digitalnega potrdila

Ponovno izdajo digitalnega potrdila lahko zaprosijo imetniki, oziroma isti subjekti, kot za prvo izdajo, skladno s poglavjem 4.1.1 Kdo lahko zaprosi za izdajo digitalnega potrdila.

4.7.3. Obdelava zahtevkov za ponovno izdajo digitalnega potrdila

Za ponovno izdajo digitalnega potrdila po preklicu ali preteku veljavnosti oddajo uporabniki enak zahtevek, kot za prvo pridobitev digitalnega potrdila. Zahtevek se obdeluje smiselno enako kot zahtevek za prvo pridobitev digitalnega potrdila skladu s poglavji 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[11], izdana po protokolu PKIX-CMP, izvede samodejno ob prvi uporabi digitalnega potrdila ob dostopu do izdajatelja SIMoD-CA-Restricted v obdobju stotih (100) dni pred zadnjim dnem veljavnosti zasebnega ključa. Generiranje novih parov ključev je možno samo v primeru, da je digitalno potrdilo, ki ga trenutno poseduje imetnik, veljavno. Postopek imenujemo tudi rutinska ponovna izdaja digitalnih potrdil.

Ponovna izdaja digitalnih potrdil pred pretekom veljavnosti se za neupravljana digitalna potrdila[12] po protokolu PKCS#10 izvede na osnovi ustreznega elektronskega zahtevka, ki je podpisan z veljavnim digitalnim potrdilom.

Ponovna izdaja digitalnega potrdila izdajatelja SIMoD-CA-Restricted in izdajateljev varnih časovnih žigov mora biti pod kontrolo operativnega osebja.

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.

---

[10] Ponovna izdaja digitalnega potrdila za preverjanje digitalnega podpisa in digitalnega potrdila za preverjanje digitalnega podpisa in 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 poglavjem 4.12.1 Povrnitev zgodovine ključev za dešifriranje.

[11] Imenovana tudi *Entrust ID.*

[12] Imenovana tudi spletna ali WEB digitalna 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 digitalnega potrdila ni možna. Ob spremembah podatkov, vsebovanih v digitalnem potrdilu, je potrebno digitalno potrdilo preklicati.

4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila

4.9.1. Okoliščine preklica

4.9.1.1. Okoliščine preklica imetniških digitalnih potrdil

Razlogi za preklic digitalnih potrdil imetnikov so:

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

4.9.1.2. Okoliščine preklica digitalnega potrdila korenskega izdajatelja

Ni relevantno.

4.9.1.3. Okoliščine preklica digitalnega potrdila o priznavanju drugega izdajatelja

Ni relevantno.

4.9.1.4. Okoliščine preklica digitalnega potrdila izdajatelja SIMoD-CA-Restricted

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

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

4.9.2. Kdo lahko zahteva preklic

4.9.2.1. Kdo lahko zahteva preklic digitalnega potrdila imetnika

Zahtevo za preklic digitalnega potrdila imetnika lahko poda:

- imetnik za svoje digitalno potrdilo,
- vodja organizacijske enote MO,
- skrbnik strežnika, druge strojne ali programske opreme, izdajatelja varnih časovnih žigov, ponudnika storitev overjanja,
- operativno osebje izdajatelja SIMoD-CA-Restricted, ki opravlja naloge prvega ali drugega varnostnega inženirja, če sumi, da imetnik krši pravila varnega ravnanja z digitalnim potrdilom ali
- tretja oseba, če utemeljeno sumi, da je pri določenemu imetniku prišlo do zlorabe zasebnih ključev.

4.9.2.2. Kdo lahko zahteva preklic digitalnega potrdila korenskega izdajatelja

Ni relevantno.

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

Ni relevantno.

4.9.2.4. Kdo lahko zahteva preklic digitalnega potrdila izdajatelja SIMoD-CA-Restricted

Preklic digitalnega potrdila izdajatelja SIMoD-CA-Restricted lahko zahteva:

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

4.9.3. Postopki za preklic

4.9.3.1. Postopki preklica digitalnih potrdil imetnikov

Načini posredovanja zahtevkov za preklic:

- poslati digitalno podpisano elektronsko sporočilo operativni osebi izdajatelja ali na skupinski elektronski naslov izdajatelja,
- kot zahtevek v elektronskem dokumentacijskem sistemu, podpisan z veljavnim digitalnim potrdilom, posredovan operativnemu osebju izdajatelja,
- kot lastnoročno podpisani zahtevek za preklic posredovan operativnemu osebju izdajatelja ali
- po telefonu na dežurno številko za preklic.

V primeru telefonsko posredovanega zahtevka dežurna oseba posreduje zahtevek za preklic operativnemu osebju izdajatelja SIMoD-CA-Restricted.

Preklic izvrši operativno osebje izdajatelja SIMoD-CA-Restricted.

Preklic lahko po lastni presoji izvede prvi ali drugi varnostni inženir na podlagi ocene o domnevni ali dejanski zlorabi zasebnega ključa. Odločitev mora biti utemeljena in zabeležena.

Po preklicu mora izdajatelj SIMoD-CA-Restricted objaviti preklicano digitalno potrdilo v registru preklicanih potrdil.

Operativno osebje izdajatelja SIMoD-CA-Restricted o preklicu digitalnega potrdila po elektronski pošti ali pismeno obvesti imetnika ali odgovorno osebo.

Za izdajo novega digitalnega potrdila po preklicu je potrebno ponoviti postopek kot za prvo pridobitev digitalnega potrdila.

4.9.3.2. Postopki preklica digitalnega potrdila korenskega izdajatelja

Ni relevantno.

4.9.3.3. Postopki preklica digitalnega potrdila o priznavanju drugega izdajatelja

Ni relevantno.

4.9.3.4. Postopki preklica digitalnega potrdila izdajatelja SIMoD-CA-Restricted

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

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

- prekliče vsa digitalna potrdila,
- zagotavlja razpoložljivost registrov preklicanih potrdil vsaj še devetdeset (90) dni od preklica svojega digitalnega potrdila,
- ustvari nove ključe,
- izda imetnikom nova digitalna potrdila in
- objavi obvestilo o preklicu svojega potrdila na spletni strani http://www.simod-pki.mors.si.

4.9.4. Čas za posredovanje zahtevka za preklic

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

4.9.5. Čas od prejema zahtevka za preklic do preklica

4.9.5.1. Čas za preklic digitalnega potrdila imetnika

Operativno osebje izdajatelja SIMoD-CA-Restricted izvede preklic v osmih (8) urah po prejemu zahtevka za preklic v primeru:

- dejanske ali domnevne zlorabe zasebnih ključev ali
- neizpolnjevanja obveznosti po Politiki SIMoD-PKI ali Pravilih delovanja izdajatelja SIMoD-CA-Restricted.

Operativno osebje izdajatelja SIMoD-CA-Restricted izvede preklic v štiriindvajsetih (24) urah po prejemu zahtevka za preklic v primeru:

- spremembe podatkov v digitalnem potrdilu,
- prenehanja delovnega razmerja imetnika,
- prenehanja obstoja organizacijske enote MO in
- prenehanja delovanja strežnika, druge strojne ali programske opreme, izdajatelja varnih časovnih žigov ali ponudnika storitev overjanja.

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

4.9.5.2. Čas za preklic digitalnega potrdila korenskega izdajatelja

Ni relevantno.

4.9.5.3. Čas za preklic digitalnega potrdila o priznavanju drugega izdajatelja

Ni relevantno.

4.9.5.4. Čas za preklic digitalnega potrdila izdajatelja SIMoD-CA-Restricted

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

4.9.6. Obveza preverjanja registra preklicanih potrdil

Tretje osebe, ki se zanašajo na digitalno potrdilo, so pred uporabo dolžne preveriti najnovejši register preklicanih potrdil. Kot del postopka preverjanja morajo preveriti tudi veljavnost in verodostojnost registra preklicanih potrdil. Tretja oseba mora za vsako uporabljeno digitalno potrdilo izvesti popoln postopek preverjanja poti zaupanja v skladu z [19] RFC 5280.

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

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

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

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

4.9.7. Pogostost objav registrov preklicanih potrdil

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

- vsaj na petindvajset (25) ur in
- 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 sto dvajset (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 le ta objavlja, še pred iztekom veljavnosti starega registra.

4.9.9. Sprotno preverjanje statusa digitalnih potrdil

Podprt je protokol za sprotno preverjanje statusa digitalnih potrdil (ang. On-line Certificate Status Protocol, OCSP) v skladu s priporočilom [23] RFC 6960.

4.9.10. Obveza sprotnega preverjanja statusa preklicanih potrdil

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

4.9.11. Ostale oblike objavljanja preklicanih digitalnih potrdil

Niso podprte.

4.9.12. Posebne zahteve glede zlorabe ključa

Ni predpisano.

4.9.13. Okoliščine za začasno ukinitev veljavnosti

Ni podprto.

4.9.14. Kdo lahko zahteva začasno ukinitev veljavnosti

Ni 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 kot opisano v poglavju 2.2. Objave informacij o digitalnih potrdilih. Storitev sprotnega preverjanja statusa digitalnih potrdil (ang. On-Line Certificate Status Protocol, OCSP) je dostopna na naslovu http://ocsp.simod-pki.mors.si.

Registri preklicanih potrdil so v skladu z [19] RFC 5280.

Sprotno preverjanje statusa potrdil je v skladu z [23] RFC 6960.

4.10.2.Razpoložljivost storitve

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

4.10.3.Dodatne možnosti

Niso na voljo.

4.11. Predčasna prekinitev veljavnosti digitalnih potrdil

Predčasno se prekine veljavnost digitalnega potrdila iz naslednjih razlogov:

- prenehanje delovnega razmerja imetnika,
- prenehanje delovanja organizacijske enote MO,
- ukinitev organizacijske ali funkcijske vloge,
- prenehanje potrebe po varnostni storitvi strežnika, strojne ali programske opreme in
- prenehanje potrebe po storitvi izdajanja varnih časovnih žigov ali drugi storitvi overjanja.

Prekinitev veljavnosti digitalnega potrdila pred iztekom obdobja veljavnosti se izvede kot preklic potrdila v skladu s poglavjem 4.9. Začasna ukinitev veljavnosti in preklic digitalnega potrdila.

4.12. Varnostno kopiranje in odkrivanje zasebnega ključa

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

Dovoljeno je varnostno kopiranje (ang. Key Backup) in posledično povrnitev zgodovine ključev (ang. Key Recovery) ter odkrivanje ključev samo za zasebne ključe za dešifriranje v povezavi z digitalnimi potrdili za šifriranje po protokolu PKIX-CMP.

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

Varnostno kopiranje zasebnih ključev izdajatelja SIMoD-CA-Restricted se zagotavlja v skladu s poglavjem 6.2.4 Varnostno kopiranje zasebnih ključev.

4.12.1.Povrnitev zgodovine ključev za dešifriranje

Izdajatelj SIMoD-CA-Restricted omogoča povrnitev zgodovine ključev za dešifriranje samo za upravljana digitalna potrdila za šifriranje, izdana po protokolu PKIX-CMP.

Povrnitev zgodovine ključev za dešifriranje se izvede:

- na osnovi zahtevka za povrnitev zgodovine ključev – imetnik vloži zahtevek, če je pred pretekom veljavnosti digitalnega potrdila izgubil geslo za dostop do zasebnih ključev, izgubil ali poškodoval pametno kartico ali drug nosilec zasebnih ključev in
- praviloma ob ponovni izdaji digitalnega potrdila.

4.12.2.Odkrivanje kopije ključev za dešifriranje

Izdajatelj SIMoD-CA-Restricted omogoča odkrivanje kopije ključev za dešifriranje samo za upravljana digitalna potrdila za šifriranje, izdana po protokolu PKIX-CMP.

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

- imetnikovemu predstojniku na podlagi zahtevka za odkrivanje kopije ključev za dešifriranje ali
- če to odredi pristojno sodišče, sodnik za prekrške ali upravni organ.

O odobritvi zahtevka za odkrivanje kopije ključa za dešifriranje odloči Svet za upravljanje z infrastrukturo javnih ključev na MO.

Izdajatelj SIMoD-CA-Restricted pred odkrivanjem kopije ključev za dešifriranje:

- po elektronski pošti obvesti imetnika digitalnega potrdila o datumu ter vlagatelju zahtevka za odkrivanje kopije njegovih ključev za dešifriranje in
- prekliče digitalno potrdilo za šifriranje in o preklicu obvesti imetnika v skladu s poglavjem 4.9.3 Postopki za preklic.

Če je v zahtevku zahtevano takojšnje odkritje kopije, mora izdajatelj SIMoD-CA-Restricted v roku štiriindvajset (24) ur od prejetja zahtevka odkriti kopijo zasebnega ključa za dešifriranje in jo posredovati predstojniku ali subjektu, ki je naveden v odločbi sodišča ali upravnega organa.

4.12.3.Zaščita odkritega zasebnega ključa in postopek prenosa

Postopek prenosa odkritega zasebnega ključa za dešifriranje je enak kot postopek prenosa zasebnega ključa za dešifriranje ob ponovnem generiranju digitalnega potrdila v skladu s protokolom PKIX-CMP.

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 posebnih in ločenih prostorih, ki so varovani z več nivojskim sistemom fizičnega in tehničnega varovanja.

Komunikacijska in informacijska oprema izdajatelja SIMoD-CA-Restricted je v prostorih, ki so varnostno območje II. stopnje po [25] ZTP.

5.1.2. Fizični dostop

Nadzor fizičnega dostopa izvaja pristojna služba MO.

Nadzor nad vstopom se izvaja z uporabo tehničnih sredstev, ki preprečujejo nepooblaščen vstop. Vstop je dovoljen samo operativnemu osebju 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 in
- klimatsko napravo za kontrolo 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 zelo 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 arhiv podatkov se hranijo v protivlomnih omarah.

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

5.1.7. Odstranjevanje odpadkov

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

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

5.1.8. Hranjenje na oddaljeni lokaciji

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

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

5.2. Organizacijski varnostni ukrepi

5.2.1. Organizacija izdajatelja SIMoD-CA-Restricted

5.2.1.1. Operativno osebje

Naloge upravljanja z izdajateljem SIMoD-CA-Restricted izvaja operativno osebje, ki je glede na vsebinska področja razdeljeno na zaključene organizacijske skupine:

- upravljanje z digitalnimi potrdili,
- upravljanje s programsko in strojno opremo ter
- varovanje in nadzor komunikacijskega sistema.

Operativni osebi izdajatelja SIMoD-CA-Restricted je dovoljeno opravljanje nalog samo znotraj ene skupine.

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

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

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

- prvi administrator izdajatelja in
- administratorji izdajatelja.

V organizacijski skupini za varovanje in nadzor komunikacijskega sistema izdajatelja SIMoD-CA-Restricted so:

- prvi administrator komunikacijskega sistema in
- administratorji komunikacijskega sistema.

Podrobnejša razdelitev nalog je del zaupnega dela Pravil delovanja izdajatelja SIMoD-CA-Restricted.

5.2.1.2. Prijavna služba

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

- sprejemanje zahtevkov za izdajo digitalnega potrdila,
- preverjanje istovetnosti naročnikov oziroma imetnikov in točnosti podatkov v zahtevkih za izdajo digitalnega potrdila,
- posredovanje zahtevkov operativnemu osebju izdajatelja SIMoD-CA-Restricted, ki upravlja z digitalnimi potrdili in
- obveščanje operativnega osebje izdajatelja SIMoD-CA-Restricted, ki upravlja z digitalnimi potrdili, o spremembi podatkov imetnika digitalnega potrdila (npr. prekinitev delovnega razmerja, premestitev v drugo organizacijsko enoto).

5.2.1.3. Druge funkcije

Pristojne organizacijske enote v MO skrbijo za:

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

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

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

5.2.2. Število oseb, potrebnih za izvedbo postopkov

V organizacijski skupini za upravljane z digitalnimi potrdili izdajatelja SIMoD-CA-Restricted so najmanj tri (3) osebe, v organizacijski skupini za upravljane s programsko in strojno opremo

izdajatelja SIMoD-CA-Restricted sta najmanj dve osebi (2), v organizacijski skupini za zavarovanje in nadzor komunikacijskega sta najmanj dve (2) osebi.

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

5.2.3. Preverjanje istovetnosti operativnega osebja

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

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

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

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

5.3. Zahteve za osebje izdajatelja SIMoD-CA-Restricted

5.3.1. Kvalifikacije, izkušnje in varnostno preverjanje

Operativno osebje izdajatelja SIMoD-CA-Restricted:

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

5.3.2. Dovoljenja za dostop do tajnih podatkov

V skladu z [25] ZTP.

5.3.3. Usposabljanje osebja

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

5.3.4. Pogostost dodatnih usposabljanj

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

5.3.5. Kroženje med delovnimi mesti

Ni predpisano.

5.3.6. Ukrepi ob kršitvah pooblastil

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

5.3.7. Zunanji izvajalci

Zunanji izvajalci morajo za izvajanje posegov izpolnjevati vse pogoje, določene v [25] ZTP in vse varnostne zahteve izdajatelja SIMoD-CA-Restricted.

5.3.8. Dokumentacija za operativno osebje

Operativnemu osebju izdajatelja SIMoD-CA-Restricted, skupini za pomoč uporabnikom in skupini za nastavitev uporabniškega okolja 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 svojem operacijskem sistemu, programski in strojni opremi,
- na operacijskih sistemih, programski in strojni opremi elementov komunikacijskega sistema,
- v zvezi s svojimi ključi,
- v zvezi z imetniškimi ključi in digitalnimi potrdili - izdaja, prevzem, ponovna izdaja in preklic, povrnitev zgodovine ključev za dešifriranje in odkrivanje kopije ključev za dešifriranje,
- v zvezi z varnostno politiko in upravljanjem informacijskega sistema in
- v zvezi z varnostno politiko in upravljanjem komunikacijskega sistema.

V elektronski ali pisni obliki se beležijo tudi dogodki, ki niso vezani direktno na komunikacijsko informacijskega sistem izdajatelja SIMoD-CA-Restricted, a vplivajo na njegovo varnsot:

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

5.4.2. Pogostost pregleda dnevnikov beleženih dogodkov

Operativno osebje 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 (7) let v arhivu.

5.4.4. Zaščita dnevnikov beleženih dogodkov

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

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

Dostop do dnevnikov beleženih dogodkov je dovoljen samo pooblaščenim osebam:

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

5.4.5. Varnostne kopije dnevnikov beleženih dogodkov

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

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

5.4.6. Način zbiranja beleženih dogodkov

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

5.4.7. Obveščanje povzročitelja dogodka

Povzročitelja dogodka o dogodku ni treba obvestiti.

5.4.8. Ocena in odprava ranljivosti

Dnevnike beleženih dogodkov pregleduje operativno osebje izdajatelja SIMoD-CA-Restricted z namenom odkrivanja in odprave ranljivosti. Ugotovljeno ranljivost se oceni s stališča verjetnosti povzročitve škode in predvidi ukrepe za zmanjšanje grožnje.

5.5. Arhiviranje podatkov

5.5.1. Vrste arhiviranih podatkov

Izdajatelj SIMoD-CA-Restricted hrani naslednje podatke:

- dnevnike beleženih dogodkov iz poglavja 5.4.1 Vrste beleženih dogodkov,
- zahtevke imetnikov digitalnih potrdil,
- dokumentacijo o izvedbi postopka izdaje digitalnih potrdil,
- korespondenco in pogodbe imetnikov digitalnih potrdil z izdajateljem SIMoD-CA-Restricted,
- digitalna potrdila in liste preklicanih potrdil,
- verzije Pravil delovanja izdajatelja SIMoD-CA-Restricted, javnih in zaupnih delov ter
- zasebne dešifrirne ključe v skladu s poglavjem 6.2.4 Varnostno kopiranje zasebnih ključev.

5.5.2. Obdobje hranjenja arhiva

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

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

5.5.3. Zaščita arhiva

Podatki, ki sodijo v dokumentarno gradivo (zahtevki za izdajo digitalnih potrdil in spremljajoči dokumenti, dokumentacija o izvedbi postopka izdaje digitalnih potrdil, korespondenca in pogodbe z imetniki digitalnih potrdil, verzije pravil delovanja izdajatelja SIMoD-CA-Restricted in dnevniki beleženih dogodkov v pisni obliki) se hranijo in arhivirajo v skladu s predpisi za delo z dokumentarnim gradivom.

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

5.5.4. Varnostna kopija arhiva

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

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

5.5.5. Časovno žigosanje zapisov

Ni predpisano.

5.5.6. Način arhiviranja

Način zbiranja arhivskih podatkov je del zaupnega dela pravil delovanja.

5.5.7. Postopek vpogleda v arhiv in njegova verifikacija

Dostop do arhiva je omogočen samo:

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

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 kateregakoli digitalnega potrdila imetnika, podpisanega s pripadajočim zasebnim ključem.

Za podpisovanje digitalnih potrdil se vedno uporablja najnovejši izdajateljev zasebni ključ. Za preverjanje veljavnosti digitalnih potrdil pa se uporablja predhodno izdajateljevo digitalno potrdilo vse dokler ne poteče veljavnost zadnjega digitalnega potrdila, podpisanega s starim zasebnim izdajateljevim 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 se izvede po predpisanem in nadzorovanem postopku. Posamezne korake postopka izvaja 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 v primeru okvar in zlorab

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

5.7.2. Uničenje programske, strojne opreme ali podatkov izdajatelja

V primeru okvare strojne ali programske opreme oziroma podatkov, pri kateri zasebni ključ izdajatelja SIMoD-CA-Restricted ni bil uničen, bodo storitve izdajatelja SIMoD-CA-Restricted vzpostavljene nazaj v najkrajšem možnem času. Izdajatelj SIMoD-CA-Restricted bo v najkrajšem možnem času vzpostavil vsaj funkcionalnost preklica digitalnih potrdil in objavljanja registra preklicanih potrdil. Skrajni rok za vzpostavitev storitve preklica digitalnih potrdil in objavljanja registra preklicanih potrdil je sedem (7) dni. Po tem roku bo izdajatelj SIMoD-CA-Restricted objavil preklic svojega potrdila in ukrepal v skladu s poglavjem 4.9.3.4 Postopki preklica digitalnega potrdila izdajatelja SIMoD-CA-Restricted.

V primeru okvare, kjer pride do uničenja izdajateljevega zasebnega ključa in vseh njegovih kopij, se postopa, kot da je prišlo do zlorabe ključa v skladu s poglavjem 4.9.3.4 Postopki preklica digitalnega potrdila izdajatelja SIMoD-CA-Restricted.

5.7.3. Zloraba zasebnega ključa izdajatelja SIMoD-CA-Restricted

Postopki ob zlorabi zasebnega ključa izdajatelja SIMoD-CA-Restricted so predpisani v poglavju 4.9.3.4 Postopki preklica digitalnega potrdila izdajatelja SIMoD-CA-Restricted.

5.7.4. Zagotavljanje kontinuitete delovanja po nesrečah

Postopki v primeru naravnih in drugih nesreč, ki imajo za posledico fizično uničenje ali varnostno vprašljivo delovanje programske ali strojne opreme ali ogroženo celovitost

podatkov izdajatelja SIMoD-CA-Restricted oziroma uničenje in poškodovanje varovanih prostorov izdajatelja SIMoD-CA-Restricted, so del okrevalnega načrta, ki je predpisan v zaupnem delu pravil delovanja.

5.8. Prenehanje delovanja izdajatelja SIMoD-CA-Restricted

Vzroki za prenehanje delovanja izdajatelja SIMoD-CA-Restricted so podani v poglavju 4.9.1.4 Okoliščine preklica digitalnega potrdila izdajatelja SIMoD-CA-Restricted.

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

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

- operativno osebje,
- vse imetnike digitalnih potrdil oziroma odgovorne osebe.

Izdajatelj SIMoD-CA-Restricted bo po prenehanju delovanja izvedel postopke predpisane v poglavju 4.9.3.4 Postopki preklica digitalnega potrdila izdajatelja SIMoD-CA-Restricted.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev para ključev

6.1.1. Generiranje para ključev

Generiranje ključev izdajatelja SIMoD-CA-Restricted izvede operativno osebje. Izvedba postopka je dokumentirana v zapisniku. Generiranje para ključev je izvedeno znotraj varnostnega kriptografskega modula.

Par ključev izdajateljev časovnih žigov in za storitev OCSP se vedno generira pri izdajatelju časovnih žigov v varnostnem kriptografskem modulu in pod njegovo kontrolo.

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 (minimalna zahteva)	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	VISOKA	pri izdajatelju	na uporabnikovi pametni kartici	digitalno potrdilo za šifriranje
zasebni ključ za dešifriranje	SREDNJA	pri izdajatelju	v programski opremi pri uporabniku	šifrirana v bazi izdajatelja
javni ključ za šifriranje	SREDNJA	pri izdajatelju	v programski opremi pri uporabniku	digitalno potrdilo za šifriranje
zasebni ključ za dešifriranje	NIZKA	pri izdajatelju	v programski opremi pri uporabniku	šifrirana v bazi izdajatelja
javni ključ za šifriranje	NIZKA	pri izdajatelju	v programski opremi pri uporabniku	digitalno potrdilo za šifriranje
Digitalno potrdilo za preverjanje digitalnega podpisa, vedno upravljano digitalno potrdilo (*Entrust ID*)				
zasebni ključ za digitalni podpis	VISOKA	na uporabnikovi pametni kartici	na uporabnikovi pametni kartici	ne obstaja
javni ključ za preverjanje digitalnega podpisa	VISOKA	na uporabnikovi pametni kartici	na uporabnikovi pametni kartici	digitalno potrdilo za preverjanje digitalnega podpisa
zasebni ključ za digitalni podpis	SREDNJA	v programski opremi pri uporabniku	v programski opremi pri uporabniku	ne obstaja
javni ključ za preverjanje digitalnega podpisa	SREDNJA	v programski opremi pri uporabniku	v programski opremi pri uporabniku	digitalno potrdilo za preverjanje digitalnega podpisa
zasebni ključ za digitalni podpis	NIZKA	v programski opremi pri uporabniku	v programski opremi pri uporabniku	ne obstaja
javni ključ za preverjanje digitalnega podpisa	NIZKA	v programski opremi pri uporabniku	v programski opremi pri uporabniku	digitalno potrdilo za preverjanje digitalnega podpisa

Namen uporabe ključa	Stopnja zaupanja	Kje se ključ generira	Kje se ključ hrani (minimalna zahteva)	Kje se hrani kopija ključa
digitalno potrdilo za preverjanje digitalnega podpis in šifriranje; lahko je upravljano (*Entrust ID*) ali neupravljano (spletno, *WEB*) digitalno potrdilo				
zasebni ključ za digitalni podpis in dešifriranje	VISOKA	na uporabnikovi pametni kartici	na uporabnikovi pametni kartici	ne obstaja
javni ključ za preverjanje digitalnega podpisa in šifriranje	VISOKA	na uporabnikovi pametni kartici	na uporabnikovi pametni kartici	digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje
zasebni ključ za digitalni podpis in dešifriranje	SREDNJA	v programski opremi pri uporabniku	v programski opremi pri uporabniku	ne obstaja
javni ključ za preverjanje digitalnega podpisa in šifriranje	SREDNJA	v programski opremi pri uporabniku	v programski opremi pri uporabniku	digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje
zasebni ključ za digitalni podpis in dešifriranje	NIZKA	v programski opremi pri uporabniku	v programski opremi pri uporabniku	ne obstaja
javni ključ za preverjanje digitalnega podpisa in šifriranje	NIZKA	v programski opremi pri uporabniku	v programski opremi pri uporabniku	digitalno potrdilo za preverjanje digitalnega podpisa in šifriranje

Za digitalna potrdila z obvezno uporabo pametne kartice, kjer izdajatelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, to je za neupravljana (spletna, *WEB*) digitalna potrdila za preverjanje digitalnega podpisa in šifriranje VISOKE stopnje zaupanja, se zasebni ključ za oba namena uporabe (podpisovanje in dešifriranje) generira na pametni kartici pri izdajatelju.

6.1.2. 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 na strojni ali programski opremi izdajatelja.

V primeru digitalnih potrdil z obvezno uporabo pametne kartice, kjer izdajatelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, to je za neupravljana (spletna, *WEB*) digitalna potrdila za preverjanje digitalnega podpisa in šifriranje VISOKE stopnje zaupanja, izvede generiranje zasebnega ključa za digitalni podpis in dešifriranje na uporabnikovi pametni kartici operativno osebje izdajatelja SIMoD-CA-Restricted. Pametna kartica se nato varno dostavi imetniku.

6.1.3. Dostava imetnikovega javnega ključa izdajatelju

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

6.1.4. Dostava izdajateljevega javnega ključa uporabnikom

Javni ključ izdajatelja SIMoD-CA-Restricted oziroma izdajateljevo digitalno potrdilo, ki vsebuje javni ključ, se pošlje bodočemu imetniku digitalnega potrdila kot integralni del postopka za prevzem potrdila.

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

6.1.5. Dolžina ključev

Ob uveljavitvi teh Pravil delovanja izdajatelja SIMoD-CA-Restrcited se ponovna izdaja digitalnega potrdila izdajatelja SIMoD-CA-Restricted ni izvedla. Dolžina RSA zasebnega ključa izdajatelja SIMoD-CA-Restricted je bila 2048 bitov.

Ob naslednji zamenjavi ključev izdajatelja SIMoD-CA-Restricted po uveljavitvi teh Pravil delovanja izdajatelja SIMoD-CA-Restricted mora biti dolžina RSA zasebnega ključa izdajatelja SIMoD-CA-Restricted vsaj 3072 bitov.

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

6.1.6. Parametri za generiranje javnih ključev in preverjanje parametrov

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

6.1.7. Namen uporabe ključev

Namen uporabe ključev je določen v razširitvenem polju *keyUsage* in *extKeyUsage* po priporočilu [19] RFC 5280.

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

Digitalno potrdilo za:		*keyUsage*	*extKeyUsage*
izdajatelj SIMoD-CA-Restricted		*keyCertSign, cRLSign*	
končni imetniki:			
preverjanje digitalnega podpisa / e-žiga		*digitalSignature, nonRepudiation*	
šifriranje		*keyEncipherment*	
preverjanje digitalnega podpisa / e-žiga in šifriranje	fizične osebe	*digitalSignature, keyEncipherment, nonRepudiation*	
	splošni nazivi	*digitalSignature, keyEncipherment*	
	strežniki	*digitalSignature, keyEncipherment*	*serverAuth, clientAurh*
izdajatelji varnih 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 [6] ETSI EN 319 411-1, poglavje 6.5.2..

Imetniki digitalnih potrdil VISOKE stopnje zaupanja morajo uporabljati pametne kartice ali podobne nosilce ključev stopnje varnosti vsaj FIPS 140-2 level 2 ali primerljive.

Imetniki kvalificiranih digitalnih potrdil VISOKE stopnje zaupanja morajo uporabljati pametne kartice ali podobne nosilce ključev, ki ustrezajo kriterijem za napravo za ustvarjanje kvalificiranega elektronskega podpisa,QSCD (ang. Qualified Signature/Seal Creation Device), ref. [7] ETSI EN 319 411-2 oziroma ustreza standardu [15] CC EAL5+ / PP QSCD.

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

6.2.2. Nadzor zasebnega ključa z več pooblaščenimi osebami

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

6.2.3. Odkrivanje zasebnega ključa

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

Odkrivanje zasebnega ključa izdajateljev časovnih žigov ni dovoljeno.

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

6.2.4. Varnostno kopiranje zasebnih ključev

Varnostna kopija zasebnega ključa izdajatelja SIMoD-CA-Restricted se zagotavlja z mehanizmi varnostnega kriptografskega modula. Varnostna kopija se pred izvozom iz varnostnega kriptografskega modula šifrira. Dešifrirni ključ je porazdeljen na N[13] od M[14] administratorskih pametnih karticah.

Kopije zasebnih ključev za dešifriranje digitalnih potrdil, za katera izdajatelj SIMoD-CA-Restricted zagotavlja storitev povrnitve zgodovine ključev, se hranijo pri izdajatelju v šifrirani obliki.

6.2.5. Arhiviranje zasebnega ključa

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

Arhivira se samo zasebne dešifrirne ključe imetniških digitalnih potrdil, za katera izdajatelj SIMoD-CA-Restricted zagotavlja povrnitev zgodovine in odkrivanje kopije ključev za dešifriranje.

6.2.6. Zapis zasebnega ključa v kriptografski modul in iz njega

Zasebni ključ izdajatelja SIMoD-CA-Restricted in izdajateljev varnih časovnih žigov se generira v varnostnem kriptografskem modulu.

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

Zasebni ključi se v primeru digitalnih potrdil SREDNJE in NIZKE stopnje varnosti generirajo v programskem modulu pri bodočem imetniku.

Zasebni ključi za dešifriranje se v primeru digitalnih potrdil, za katera izdajatelj SIMoD-CA-Restricted zagotavlja storitev povrnitve zgodovine in odkrivanja kopije ključev za dešifriranje, generirajo v izdajateljevem kriptografskem modulu in se prenesejo bodočemu imetniku z uporabo protokola PKIX-CMP.

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

[13] N mora biti enako ali večje od 2.

[14] M mora biti eneko ali večje od 5.

6.2.7. Hranjenje zasebnega ključev v kriptografskem modulu

Zasebni ključi izdajatelja SIMoD-CA-Restricted in izdajateljev časovnih žigov se hranijo v varnostnem kriptografskem modulu in v varnostni kopiji na disku v šifrirani obliki in se nikdar ne pojavijo izven modula v nešifrirani obliki.

6.2.8. Postopek za aktiviranje zasebnega ključa

Zasebni ključi izdajatelja SIMoD-CA-Restricted in izdajateljev varnih časovnih žigov se aktivirajo ob zagonu aplikativne programske opreme. Za aktiviranje je potrebno predložiti operatersko pametno kartico varnostnega kriptografskega modula ter administratorsko geslo.

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 ključi izdajatelja SIMoD-CA-Restricted in izdajateljev varnih časovnih žigov se deaktivirajo z zaustavitvijo 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 oziroma izdajatelja varnih časovnih žigov se uničijo vsi ključi, ki se nahajajo v delovnem pomnilniku varnostnega kriptografskega modula. Zasebni ključi se nikoli ne nahajajo v sistemskem pomnilniku, temveč samo v strojni opremi varnostnega kriptografskega modula.

Zasebni ključi pri digitalnih potrdilih VISOKE stopnje zaupanja se nikoli ne nahajajo v sistemskem pomnilniku, vedno samo v strojni opremi pametne kartice.

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

6.2.10.Postopek za uničenje zasebnega ključa

Operativno osebje uniči zasebne ključe izdajatelja SIMoD-CA-Restricted, izdajateljev časovnih žigov in sistemov OCSP, ko jim poteče obdobje uporabe, oziroma se ne uporabljajo več iz drugih razlogov. Ob uničenju ključev se uničitjo aktivne kopije v varnostnem kriptografskem modulu in vse varnostne kopije.

6.2.11.Stopnja varnosti kriptografskih modulov

Opisano v poglavju 6.2.1 Standardi za kriptografski modul.

6.3. Ostali vidiki upravljanja s pari ključev

6.3.1. Arhiviranje javnega ključa

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 (glej poglavje 5.5. Arhiviranje podatkov). Javni ključi v povezavi s šifrirnimi digitalnimi potrdili se ne arhivirajo.

6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil

Veljavnost digitalnega potrdila oziroma javnega in zasebnega ključa izdajatelja SIMoD-CA-Restricted je največ dvajset (20) let oziroma do poteka veljavnosti digitalnega potrdila korenskega izdajatelja SIMoD-CA-Restricted.

Veljavnost imetniških digitalnih potrdil oziroma javnih in zasebnih ključev je:

Digitalno potrdilo za:	Ključ	Veljavnost
preverjanje digitalnega podpisa / e-žiga	zasebni	štiri (4) leta
	javni	pet (5) let
šifriranje	zasebni	neomejeno
	javni	pet (5) let
preverjanje digitalnega podpisa / e-žiga in šifriranje	zasebni	pet (5) let
	javni	pet (5) let
izdajatelja varnih časovnih žigov	zasebni	tri (3) leta
	javni	pet (5) let
sistemi OCSP	zasebni	tri (3) leta
	javni	tri (3) leta
sistemi za podpis programske kode	zasebni	pet (5) let
	javni	pet (5) let

6.4. Gesla za dostop do zasebnih ključev

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

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

Razen v primerih iz naslednjega odstavka določijo geslo za pametne kartice imetniki v postopku inicializacije pametne kartice pred prvim prevzemom digitalnega potrdila.

Za digitalna potrdila z obvezno uporabo pametne kartice, kjer izdajatelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, se geslo določi ob prevzemu digitalnega potrdila pri izdajatelju. To geslo mora imetnik spremeniti pred prvo uporabo digitalnega potrdila.

Za dostop do zasebnih ključev, ki se hranijo v programski obliki (npr. Microsoft Cryptographic Store) morajo uporabniki uporabljati visoko stopnjo zaščite, ki jo nudi programska oprema. Geslo za dostop do zasebnih ključev, ki se hranijo v programski obliki, določijo imetniki ob prevzemu digitalnega potrdila.

6.4.2. Zaščita gesel

Gesla se morajo hraniti na način, ki zagotavlja njihovo zaupnost. Če je bilo geslo za dostop do pametne kartice določeno pri izdajatelju, ga izdajatelj dostavi imetniku na varen način.

6.4.3. Druge zahteve za gesla

Geslo za dostop do pametne kartice oziroma za aktivacijo pametne kartice mora biti dolgo najmanj 9 znakov in mora vsebovati velike in male črke, številke ter posebne znake in ne sme biti beseda iz slovarja.

Odstopanje od zahteve je dovoljeno le, če tehnična izvedba pametne kartice ne omogoča določitve tako varnega gesla. V tem primeru morajo imetniki pametne kartice določiti najbolj varno geslo, kot ga pametna kartica omogoča.

6.5. Varnostne zahteve za računalnike

6.5.1. Specifične tehnične varnostne zahteve za računalnike

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

- kontrolo 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 varnostno relevantnih dogodkov,
- varen arhiv informacijskega sistema izdajatelja, kopij ključev imetnikov in varnostnih beležk,
- mehanizme restavriranja sistema, ključev ter baze podatkov izdajatelja in
- redno izvajanje vdornih testov in testov ranljivosti.

6.5.2. Raven varnostne zaščite računalnikov

Elementi informacijskega sistem izdajatelja SIMoD-CA-Restricted za upravljanje z digitalnimi potrdili dosegajo raven varnostne zaščite računalnikov vsaj CC EAL 4+.

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

Izdajatelj SIMoD-CA-Restricted evidentira postopke inštalacije, sprememb konfiguracije in nadgradenj za vse svoje informacijske in komunikacijske komponente.

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

6.6.3. Upravljanje varnosti čez življenjski cikel

Nadgradnje, nove verzije in popravki delov informacijskih in komunikacijskih sistemov izdajatelja SIMoD-CA-Restricted oziroma upravljanje varnosti skozi celoten življenjski je v skladu z 6.6.2 Upravljanje varnosti.

6.7. Varnostne kontrole na ravni računalniškega omrežja

Komunikacijsko informacijski sistemi izdajatelja SIMoD-CA-Restricted deluje v izoliranem omrežju, ki je z drugimi omrežji KIS MO in SV povezan preko varnostnih pregrad. Varnostna pravila na varnostnih pregradah dovoljujejo prehod samo protokolom, potrebnim za dostop do storitev izdajatelja SIMoD-CA-Restricted.

6.8. Časovno žigosanje

Ni predpisano.

7. PROFIL DIGITALNIH POTRDIL IN REGISTROV PREKLICANIH POTRDIL

7.1. Profil digitalnih potrdil

7.1.1. Verzija digitalnih potrdil

Izdajatelj SIMoD-CA-Restricted izdaja digitalna potrdila X.509 verzije 3 v skladu s priporočilom [19] RFC 5280, ki vsebujejo naslednja osnovna polja:

Ime osnovnega polja / prevod ali opis	Vrednost
Version / X.509 verzija	*v3*
Serial Number / enolična serijska številka	enolična serijska številka
Signature Algorithm / algoritem za podpis	*sha256WithRSAEncryption*
Issuer / razločevalno ime izdajatelja	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 imetnika v skladu s poglavjem 3.1. Določanje imen
Subject Public Key Info / podatki o imetnikovem javnem ključu	*rsaEncryption*, modul, eksponent, vrednost javnega ključa

7.1.2. Razširitvena polja

Standardna razširitvena polja po priporočilu [19] RFC 5280 uporabljena v digitalnih potrdilih izdajatelja SIMoD-CA-Restricted, izdajateljev časovnega žiga, sistemov OCSP in sistemov za podpis programske kode so:

Ime razširitvenega polja / prevod ali opis	Digitalno potrdilo SIMoD-CA-Restricted	Digitalna potrdila za izdajatelje varnih časovnih žigov	Digitalna potrdila OCSP
Authority Key Identifier / odtis javnega ključa izdajatelja	SHA256 odtis javnega ključa izdajatelja SIMoD-CA-Root, s katerim je podpisano potrdilo	SHA256 odtis javnega ključa izdajatelja SIMoD-CA-Restricted, s katerim je podpisano potrdilo	SHA256 odtis javnega ključa izdajatelja SIMoD-CA-Restricted, s katerim je podpisano potrdilo
Subject Key Identifier / odtis imetnikovega javnega ključa	SHA256 odtis javnega ključa izdajatelja SIMoD-CA-Restricted	SHA256 odtis javnega ključa izdajatelja časovnega žiga	SHA256 odtis javnega ključa sistema OCSP
Key Usage / namen uporabe ključa	**Kritično** keyCertSign, cRLSign	**Kritično** digitalSignature	**Kritično** digitalSignature
Extended Key Usage / razširjen namen uporabe	Ni uporabljeno	**Kritično** *timeStamping*	**Kritično** OCSP Signing
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	Ni uporabljeno	*Certificate Policy*	*Certificate Policy*
Policy Identifier / enolična oznaka politike		Skladno s 1.2. ,*OID: 1.3.6.1.4.1.22295.10.1.1.1.5.4.2*	Skladno s 1.2. ,*OID: 1.3.6.1.4.1.22295.10.1.1.1.6.5.2*
Policy Qualifier / podatki o politiki		*Qualifiers OID* *Qualifier: http:/www.simod-pki.mors.si*	*Qualifiers OID* *Qualifier: http:/www.simod-pki.mors.si*
CRL Distribution Point / naslovi registra preklicanih potrdil	LDAP in http URL naslov registra preklicanih potrdil SIMoD-CA-Root	LDAP in http URL naslov registra preklicanih potrdil SIMoD-CA-Restricted	LDAP in http URL naslov registra preklicanih potrdil SIMoD-CA-Restricted
subject Alternative Name / alternativno ime imetnika	Ni uporabljeno	Ni uporabljeno	Ni uporabljeno
Basic Constraints / osnovne omejitve	**Kritično** CA =: True pathLenConstraint = 0	**Kritično** CA =: False	**Kritično** CA =: False
Authority Info Access / dostop do informacij o izdajatelju	URL naslov izdajatelja	URL naslov izdajatelja	URL naslov izdajatelja

Ime razširitvenega polja / prevod ali opis	Digitalna potrdila za sisteme za podpis programske kode
Authority Key Identifier / odtis javnega ključa izdajatelja	SHA256 odtis javnega ključa izdajatelja SIMoD-CA-Restricted
Subject Key Identifier / odtis imetnikovega javnega ključa	SHA256 odtis javnega ključa sistema za podpis programske kode
Key Usage / namen uporabe ključa	**Kritično** digitalSignature
Extended Key Usage / razširjen namen uporabe	codeSigning
Private Key Usage Period / veljavnost zasebnega ključa	Ni uporabljeno
Certificate Policies / oznaka politike potrdila	*Certificate Policy*
Policy Identifier / enolična oznaka politike	Skladno s poglavjem 1.2. , *OID:* *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*
Policy Qualifier / podatki o politiki	*Qualifiers OID* *Qualifier: http:/www.simod-pki.mors.si*
CRL Distribution Point / naslovi registra preklicanih potrdil	LDAP in http URL naslov registra preklicanih potrdil SIMoD-CA-Restricted
subject Alternative Name / alternativno ime imetnika	DNS ime sistema
Basic Constraints / osnovne omejitve	**Kritično** CA =: False
Authority Info Access / dostop do informacij o izdajatelju	URL naslov izdajatelja

Imetniška digitalna potrdila, ki jih izdaja izdajatelj SIMoD-CA-Restricted, vsebujejo naslednja razširitvena polja po priporočilu [19] RFC 5280:

Ime razširitvenega polja / prevod ali opis	Potrdilo za preverjanje digitalnega podpisa	Potrdilo za šifriranje	Potrdilo za preverjanje digitalnega 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* za potrdila za 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. in 7.1.6 *Policy Identifier=*		
Policy Qualifier / podatki o politiki	*[1,1]Policy Qualifier Info:* *Policy Qualifier Id=CPS* *Qualifier: http:/www.simod-pki.mors.si*		
	samo za kvalificirana digitalna potrdila še dodatno polje: *[2]Certificate Policy:* *Policy Identifier=oznaka EU kvalificirane politike*		
CRL Distribution Points / naslovi registra preklicanih potrdil	LDAP in http URL naslov registra preklicanih potrdil SIMoD-CA-Restricted		
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	*Authority Info Access* *Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)* *Alternative Name: URL=http://www.simod-pki.mors.si/certs/simod-ca-restricted.p7b* *[2]Authority Info Access* *Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)* *Alternative Name: URL=http://ocsp.simod-pki.mors.si/simod-ca-restricted*		

Kvalificirana digitalna potrdila skladna z [7] ETSI EN 319 411-2 morajo vsebovati izjavo, da ustrezajo profilu kvalificiranih potrdil po priporočilu v [14] ETSI EN 319 412-5. V ta namen vsebujejo dodatno razširitveno polje:

qcStatement 1.3.6.1.5.5.7.1.3 / izjava, da je potrdilo kvalificirano	• *etsi-qcs-QcCompliance*, ob uporabi naprave za ustvarjanje kvalificiranega elektronskega podpisa, QSCD še: • *etsi-qcs-QcSSCD*

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

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

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

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.

Kvalificirano digitalno potrdilo ima skladno s priporočilom [7] ETSI EN 319 411-2 poleg oznake politike izdajatelja SIMoD-CA-Restricted še vrednost, ki ga označuje kot EU kvalificirano digitalno potrdilo.

7.1.7. Način uporabe razširitvenega polja za omejitev uporabe politik

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

7.1.8. Specifični podatki o politiki

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 [19] 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 [19] 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 [19] 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

Storitev sprotnega preverjanja statusa digitalnih potrdil (OCSP) je v skladu s priporočilom [23] RFC 6960.

7.3.2. Razširitve sprotnega preverjanja statusa digitalnih potrdil

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

8. PREVERJANJE SKLADNOSTI IN OSTALE OBLIKE NADZORA

8.1. Pogostost inšpekcije

Pogostost inšpekcijskega nadzora je določena z veljavno zakonodajo..

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

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

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

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

8.2. Pogoji za inšpektorja

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

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

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

8.3. Relacija med inšpektorjem in izdajateljem SIMoD-CA-Restricted

Inšpektor mora biti neodvisen od infrastrukture javnih ključev na MO.

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

8.4. Področja inšpekcije

Inšpekcijski nadzor preverja skladnost delovanja izdajatelja SIMoD-CA-Restricted z veljavno zakonodajo, Politiko SIMoD-PKI in Pravili delovanja izdajatelja SIMoD-CA-Restricted.

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

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

8.5. Postopki po opravljeni inšpekciji

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

Če izdajatelj SIMoD-CA-Restricted pomanjkljivosti ne odpravi, je Svet za upravljanje z infrastrukturo javnih ključev na MO dolžan ukrepati v okviru naslednjih možnosti:

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

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

8.6. Prejemniki ugotovitev o inšpekciji

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

Izdajatelj SIMoD-CA-Restricted se na osnovi ugotovitev inšpektorja odloči ali je potrebno obvestiti imetnike digitalnih potrdil in ostale udeležence. Obvestilo imetnikom in ostalim udeležencem objavi v skladu s poglavjem 9.11. Obvestila in komuniciranje z udeleženci.

V skladu s prvim odstavkom 20. člena [3] Uredbe eIDAS mora ponudnik kvalificiranih storitev zaupanja poročilo o ugotovitvi skladnosti predložiti nadzornemu organu, ki je določen v 3. členu [2] Uredbe o izvajanju eIDAS, v treh (3) dneh po njegovem prejemu.

9. OSTALE POSLOVNE IN PRAVNE ZADEVE

9.1. Cenik

9.1.1. Cena prve in ponovne izdaje digitalnega potrdila

Ni predpisano.

9.1.2. Cena dostopa do digitalnega potrdila

Ni predpisano.

9.1.3. Cena dostopa do podatka o statusu in preklicu potrdila

Ni predpisano.

9.1.4. Cene drugih storitev

Ni predpisano.

9.1.5. Povračilo stroškov

Ni predpisano.

9.2. Finančna odgovornost

9.2.1. Višina zavarovanja

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

9.2.2. Druge oblike zavarovanja

Ni predpisano.

9.2.3. Zavarovanje ali jamstva za končne uporabnike

Ni predpisano.

9.3. Zaupnost poslovnih informacij

9.3.1. Obseg zaupnih poslovnih informacij

Ni predpisano.

9.3.2. Informacije izven obsega zaupnih poslovnih informacij

Ni predpisano.

9.3.3. Odgovornost za zagotavljanje zaupnosti poslovnih informacij

Ni predpisano.

9.4. Zaupnost osebnih podatkov

9.4.1. Načrt zagotavljanja zaupnosti osebnih podatkov

Izdajatelj SIMoD-CA-Restricted pridobi osebne podatke od bodočih imetnikov z zahtevkom za izdajo digitalnega potrdila. Pridobljeni podatki se uporabljajo izključno za potrebe izdaje in

upravljanja digitalnih potrdil. Osebni podatki imetnikov se obdelujejo v skladu s predpisi o varstvu osebnih podatkov.

9.4.2. Obseg osebnih podatkov, ki se obravnavajo kot zaupni

Osebni podatki so določeni s predpisi o varstvu osebnih podatkov.

9.4.3. Osebni podatki, ki se ne obravnavajo kot zaupni

Podatki, objavljeni v digitalnih potrdilih, imenikih in registrih preklicanih potrdil, niso osebni podatki, ki bi jih bilo potrebno varovati v skladu s predpisi o varstvu osebnih podatkov.

9.4.4. Odgovornost glede varovanja osebnih podatkov

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

9.4.5. Dovoljenje za uporabo osebnih podatkov

Prijavna služba mora od bodočih imetnikov pridobiti dovoljenje za uporabo osebnih podatkov v postopku preverjanja istovetnosti in v postopkih upravljanja digitalnih potrdil.

9.4.6. Posredovanje osebnih podatkov v sodnih in upravnih postopkih

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

9.4.7. Druge okoliščine posredovanja osebnih podatkov

Ni predpisano.

9.5. Zaščita intelektualne lastnine

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

Na zasebnem ključu za podpisovanje pripadajo vse pravice imetniku digitalnega potrdila za podpisovanje.

Ob pogojih iz poglavja 4.12.2 Odkrivanje kopije ključev za dešifriranje se lahko prenese lastništvo zasebnega ključa za dešifriranje drugemu subjektu kot je imetnik digitalnega potrdila.

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 delovanja izdajatelja SIMoD-CA-Restricted. Svet za upravljanje z infrastrukturo javnih ključev na MO predstavlja izdajatelja SIMoD-CA-Restricted in jamči za izpolnjevanje njegovih obveznosti.

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

9.6.2. Odgovornost in jamstva prijavne službe

Prijavna služba je odgovorna za skladnost identifikacijskih postopkov s Politiko SIMoD-PKI in Pravili delovanja izdajatelja SIMoD-CA-Restricted ter za točnost podatkov v zahtevkih. Za pravilnost delovanja prijavne službe jamči Svet za upravljanje z infrastrukturo javnih ključev na MO.

9.6.3. Odgovornost in jamstva imetnikov digitalnih potrdil

Imetnik digitalnega potrdila jamči, da:

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

Obveznosti imetnikov digitalnih potrdil glede uporabe zasebnih ključev in digitalnih potrdil so opisane v poglavju 4.5.1.3 Uporabniški zasebni ključi in digitalna potrdila.

9.6.4. Odgovornost in jamstva tretje osebe

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 Javnih pravilih SIMoD-CA-Restricted ter v pogodbi o medsebojnem priznavanju.

Obveznosti tretjih oseb glede uporabe zasebnih ključev in 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 relevantno.

9.7. Zanikanje odgovornosti

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

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

9.8. Omejitve odgovornosti

Izdajatelj SIMoD-CA-Restricted jamči za vrednost posameznega pravnega posla do vrednosti glede na vrsto digitalnega potrdila:

- za digitalna potrdila VISOKE stopnje zaupanja do 5.000 EUR in
- za digitalna potrdila SREDNJE stopnje zaupanja do 1.000 EUR.

Za digitalna potrdila NIZKE stopnje zaupanja izdajatelj SIMoD-CA-Restricted ne prevzema jamstva.

9.9. Zavarovanje pred škodo zaradi neizpolnjevanja obveznosti

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

9.10. Začetek in prenehanje veljavnosti

9.10.1.Začetek veljavnosti

Nova verzija Javnih pravil SIMoD-CA-Restricted se objavi na spletnih straneh http://www.simod-pki.mors.si.

Določbe Pravil SIMoD-SIMoD-CA-Restricted za nekvalificirana digitalna potrdila začnejo veljati in se uporabljati naslednji dan po podpisu.

Določbe Pravil SIMoD-SIMoD-CA-Restricted za kvalificirana digitalna potrdila začnejo veljati in se uporabljati z datumom, ko pristojni organ za izvajanje nadzornih nalog v skladu s 17. členom [3] eIDAS izda zagotovilo, da ponudnik storitev zaupanja na Ministrstvu za obrambo izpolnjuje zahteve [3] eIDAS.

9.10.2.Prenehanje veljavnosti

Veljavnost dokumenta ni časovna omejena. Javna pravila SIMoD-CA-Restricted veljajo do uveljavitve nove verzije.

9.10.3.Posledice prenehanja veljavnosti

Po prenehanju veljavnosti Javnih pravil SIMoD-CA-Restricted zaradi objave nove verzije imetniki praviloma uporabljajo obstoječa potrdila v skladu Javnimi pravili 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

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

9.12.2.Postopek obveščanja in rok za pripombe

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

9.12.3.Spremembe, ki zahtevajo novo identifikacijsko oznako politike

Svet za upravljanje z infrastrukturo javnih ključev na MO odloči, ali so spremembe vsebine Javnih pravil SIMoD-CA-Restricted tolikšne, da zahtevajo objavo novih Javnih pravil SIMoD-CA- Restricted in spremembe identifikacijskih oznak politik delovanja.

9.13. Reševanje sporov

Stranke si bodo prizadevale za sporazumno reševanje sporov, če pa to ne bo mogoče, je za reševanje sporov pristojno sodišče v Ljubljani. Stranke za reševanje sporov dogovorijo izključno uporabo predpisov Republike Slovenije.

9.14. Veljavna zakonodaja

Izdajatelj SIMoD-CA-Restricted deluje v skladu z predpisi in priporočili:

[1]	ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 – UPB1, 61/06)
[2]	Uredba o izvajanju eIDAS	Uredba o izvajanju Uredbe (EU) o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 199/93/ES (Uradni list RS, št. 46/16)
[3]	eIDAS	Uredba (EU) št. 910/2014 Evropskega parlamenta in sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (Uradni list EU, št. L 257/83 z dne 28.8.2014)
[4]	ETSI ES 319 401	v2.1.1 Electronic Signatures and Infrastructures (ESI); General Policy requirements for Trust Service Providers
[5]	ETSI EN 319 411	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Provider issuing certificates
[6]	ETSI EN 319 411-1	v1.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Provider issuing certificates, Part 1: General requirements
[7]	ETSI EN 319 411-2	v2.1.1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Provider issuing certificates, Part 2: Requirements for trust service providers issuing EU qualified certificates
[8]	ETSI EN 319 421	v1.1.1 Policy and Security Requirements for Trust Services Providers issuing Electronic Time-Stamps
[9]	ETSI EN 319 412	Electronic Signatures and Infrastructures (ESI); Certificate Profiles
[10]	ETSI EN 319 412-1	v1.1.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
[11]	ETSI EN 319 412-2	V2.1.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
[12]	ETSI EN 319 412-3	v1.1.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
[13]	ETSI EN 319 412-4	v1.1.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates
[14]	ETSI EN 319 412-5	v2.1.1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[15]	CC EAL5+ / PP QSCD	Certification based on Common Criteria Protection Profiles EN 419211 part 1 to 6, as mandated by eIDAS
[16]	Politika SIMoD-PKI	Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, Verzija 3.0
[17]	Pravila SIMoD-CA-Root	Pravila delovanja izdajatelja SIMoD-CA-Root, ver. 3.0
[18]	RFC 3647	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[19]	RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[20]	RFC 4043	Internet X.509 Public Key Infrastructure Permanent Identifier

[21] RFC 4210 Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)

[22] PKCS#10 Certification Request Syntax Standard

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

9.15. Ostala relevantna zakonodaja

Izdajatelji SIMoD-PKI delujejo morajo pri svojem delovanju upoštevati tudi:

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

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

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

9.16. Razne določbe

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

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

A.2. Načrt varovanja tajnih podatkov v prostorih izdajatelja SIMoD-CA-Restricted

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

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

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

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

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

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

9.17. Končne določbe

Ni ostalih določb.