REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije

(Politika SIMoD-PKI)

Verzija 3.0

Zgodovina sprememb in dopolnitev Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije:

Izdaja:	Spremembe glede na prejšnjo izdajo:
Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, 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 omejitev ponovne izdaje digitalnih potrdil brez preverjanja istovetnosti maksimalno dvakrat (2x) zaporedoma.
Pravila o spremembah pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, verzija 2.0, številka: 386-11/2014-20, datum: 07.02.2014	Prenehanje uporabe algoritma SHA-1 in začetek uporabe algoritma SHA256.
Pravila o dopolnitvah Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, verzija 2.0, številka: 386-6/2011-304, datum: 14.11.2011	Uvedena je možnost, da overitelj s svojimi pravili delovanja lahko določi načine preverjanja istovetnosti in postopke obdelave zahtevka za ponovno izdajo digitalnih potrdil v izjemnih primerih, ki so različni od načinov oziroma postopkov predpisanih s Pravili delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije.
Pravila o spremembah Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, verzija 2.0, številka: 386-6/2011-229, datum: 08.09.2011	• odstranjene so vrednosti parametrov v povezavi z digitalnimi potrdili (dolžine in obdobje veljavnosti ključev) in • poenostavljen je postopek oddaje vloge za preklic digitalnega potrdila.

Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, verzija 2.0, številka: 382-5/2006-109, datum: 24.08.2010	• pristojnost sprejemanja pravil delovanja posameznih overiteljev je prenesena na Svet za upravljanje z infrastrukturo javnih ključev na MO, • spremenjeno je pravilo za določanje identifikacijskih oznak politik digitalnih potrdil, • 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 prve registracije za digitalna potrdila NIZKE stopnje zaupanja.
Spremembe in dopolnitve Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije (Politika SIMoD-PKI), številka: 382-5/2006-42, datum: 27.12.2007	• spremenjena so polja v digitalnih potrdilih, • spremenjeno je pravilo za določanje identifikacijskih oznak politik digitalnih potrdil.
Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije (Politika SIMoD-PKI), šifra: 382-5/2006-11, datum: 17.7.2006	Vpeljan je hiearalhični model infrastrukture javnih ključev.
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 INFRASTRUKTURE JAVNIH KLJUČEV NA MINISTRSTVU ZA OBRAMBO REPUBLIKE SLOVENIJE

(Politika SIMoD-PKI)

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**loveni**i**an **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, podrejeni izdajatelji digitalnih potrdil in izdajatelji časovnih žigov, v nadaljevanju izdajatelji SIMoD-PKI.

Ta dokument, Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, imenujemo tudi Politika SIMoD-PKI.

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

Politika SIMoD-PKI predpisuje izdajanje in upravljanje digitalnih potrdil 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.

Digitalna potrdila se med seboj ločijo glede na stopnjo zaupanja v digitalno potrdilo, namen uporabe, zahtevnost postopka preverjanja istovetnosti bodočega imetnika digitalnega potrdila in način hranjenja zasebnih ključev.

Izdajatelji SIMoD-PKI izdajajo nekvalificirana in kvalificirana digitalna potrdila. Kvalificirana so digitalna potrdila, za katera sta poleg splošnih zahtev po Politiki SIMoD-PKI izpolnjena naslednja pogoja:

- zasebni ključ se hrani samo pri imetniku oziroma je vedno pod njegovim nadzorom in
- ob prvi registraciji se preverja istovetnost bodočega imetnika v prijavni službi.

Politika SIMoD-PKI zagotavlja, da so kvalificirana digitalna potrdila skladna z [1] ZEPEP, [3] eIDAS in standardi ETSI ([4], [5], [6], [7], [8], [9], [10], [11], [12], [13] in [14]).

Izdajatelji SIMoD-PKI so dolžni objaviti pravila delovanja, ki morajo biti v skladu s Politiko SIMoD-PKI.

Izdajatelji SIMoD-PKI delujejo v zasebnem komunikacijsko informacijskem sistemu MO in SV (v nadaljnjem besedilu: KIS MO in SV).

SIMoD-PKI deluje po priporočilih zveze NATO, Evropske skupnosti in v skladu s predpisi, ki urejajo področje elektronskega podpisa v Republiki Sloveniji.

1.2. Identifikacijske oznake politik delovanja

Identifikacijske oznake politik delovanja izdajateljev SIMoD-PKI (ang. Policy Object Identifiers; Policy OIDs) se tvorijo po naslednjem pravilu: *osnova.p1.p2.p3.p4.p5.p6*

Del identifikacijske oznake	Vrednost	
Osnova OID	1.3.6.1.4.1.22295.10	
Klasifikacija KIS (p1)	1	brez stopnje tajnosti, javna omrežja + INTERNO
	2	TAJNO
	…	
Ob prvi registraciji obvezno preverjanje istovetnosti v prijavni službi (p2)	1	DA
	2	NE
Obvezna uporaba sredstva za varno elektronsko podpisovanje[1] (p3)	1	DA
	2	NE
	…	
Imetnik digitalnega potrdila (p4)	1	fizična oseba
	2	funkcijska ali organizacijska vloga – izvzeto iz uporabe
	3	splošni naziv; vključuje organizacijske enote MO ali institucije, ki opravljajo naloge povezane z obrambo in funkcijske ter organizacijske vloge oziroma njihove splošne nazive
	4	strežnik ali druga strojna oziroma programska oprema
	5	izdajatelj varnih časovnih žigov
	6	sistemi za sprotno preverjanje veljavnosti digitalnih potrdil (ang. Online Certificate Status Protocol, OCSP)
		…
Namen uporabe ključev (p5)	1	preverjanje digitalnega podpisa
	2	šifriranje s hranjenjem kopije zasebnega ključa pri izdajatelju
	3	preverjanje digitalnega podpisa in šifriranje
	4	časovno žigosanje
	5	podpisovanje zahtevkov za sprotno preverjanje veljavnosti potrdil
		…
Verzija (p6)	zaporedna številka izdaje politike	

Izdajatelji označijo, pod katero politiko izdajajo digitalna potrdila, v razširitvenih poljih, kot je določeno v poglavju 7.1.2 Razširitvena polja.

[1] Primera sredstev za varno elektronsko podpisovanje: strojni kriptografski modul in pametna kartica

Izdajatelji SIMoD-PKI lahko izdajajo eno ali več vrst digitalnih potrdil, kar morajo jasno označiti v svojih pravilih delovanja in digitalnih potrdilih z navedbo identifikacijske oznake politike v razširitvenem polju *Certificate Policies*. Izdajatelji lahko digitalnim potrdilom, ki jih izdajajo po eni od politik SIMoD-PKI, dodelijo svojo identifikacijsko oznako. V tem primeru mora biti v razširitvenem polju *Certificate Policies* identifikacijska oznaka po politiki SIMoD-PKI in izdajateljeva identifikacijska oznaka.

Izdajatelji SIMoD-PKI lahko poleg digitalnih potrdil po Politiki SIMoD-PKI izdajajo tudi druga digitalna potrdila, kar morajo jasno označiti v svojih pravilih delovanja in digitalnih potrdilih z navedbo identifikacijske oznake politike v razširitvenem polju C*ertificate Policies*. Digitalna potrdila, ki niso skladna s Politiko SIMoD-PKI, ne smejo vsebovati identifikacijske oznake politike SIMoD-PKI.

Kvalificirana digitalna potrdila morajo v skladu z [1] ZEPEP vsebovati navedbo, da so kvalificirana potrdila.

Kvalificirana digitalna potrdila skladna z [7] ETSI EN 319 411-2 morajo v razširitvenem polju *Certificate Policies* vsebovati poleg oznake politike po Politiki SIMoD-PKI še oznako politike, ki označuje skladnost z eno izmed ETSI politik za kvalificirana potrdila:

Opis politike:	Skrajšan opis politike (ang.)	Oznaka politike (Policy OID)
politika za EU kvalificirana potrdila izdana fizičnim osebam	QCP-n	0.4.0.194112.1.0
politika za EU kvalificirana potrdila izdana pravnim osebam	QCP-l	0.4.0.194112.1.1
politika za EU kvalificirana potrdila izdana fizičnim osebam z obvezno uporabo naprave za ustvarjanje kvalificiranega elektronskega podpisa	QCP-n-qscd	0.4.0.194112.1.2
politika za EU kvalificirana potrdila izdana pravnim osebam z obvezno uporabo naprave za ustvarjanje kvalificiranega elektronskega podpisa	QCP-l-qscd	0.4.0.194112.1.3
politika za EU kvalificirana potrdila za avtentikacijo spletišč	QCP-w	0.4.0.194112.1.4

Kvalificirana digitalna potrdila skladna z [7] ETSI EN 319 411-2 morajo vsebovati razširitveno polje *qcStatement* kot predpisano v [14] ETSI EN 319 412-5.

1.3. Udeleženci infrastrukture javnih ključev

1.3.1. Overitelj na Ministrstvu za obrambo

Overitelj na Ministrstvu za obrambo (v nadaljevanju overitelj na MO) združuje korenskega izdajatelja digitalnih potrdil, podrejene izdajatelje digitalnih potrdil in izdajatelje časovnih žigov, ki delujejo v okviru SIMoD-PKI.

Overitelj na MO s svojimi izdajatelji je ponudnik naslednjih storitev zaupanja:

- izdajanje kvalificiranih digitalnih potrdil,
- izdajanje varnih časovnih žigov.

Izdajatelji posedujejo strojno in programsko opremo, zaposlujejo osebje in izvajajo predpisane postopke ter ukrepe, ki zagotavljajo varno in zanesljivo poslovanje SIMoD-PKI.

Overitelja na MO oziroma izdajatelje, ki delujejo v okviru SIMoD-PKI, zastopa Svet za upravljanje z infrastrukturo javnih ključev na MO.

1.3.1.1. Svet za upravljanje z infrastrukturo javnih ključev na MO

Svet za upravljanje z infrastrukturo javnih ključev na MO upravlja z infrastrukturo javnih ključev na MO, zastopa overitelja na MO in ima v zvezi s tem naslednje obveznosti:

- pripravlja spremembe, dopolnitve in nove verzije Politike SIMoD-PKI,
- ocenjuje in potrjuje skladnost pravil delovanja posameznega izdajatelja s Politiko SIMoD-PKI,
- sprejema pravila delovanja izdajateljev SIMoD-PKI,
- imenuje operativno osebje izdajateljev SIMoD-PKI,
- operativnemu osebju daje usmeritve za odpravljanje pomanjkljivosti, ugotovljenih ob inšpekcijskem in drugih oblikah nadzora ter uveljavlja druge ukrepe, kot je npr. preklic izdajateljevega digitalnega potrdila,
- ocenjuje ustreznost politik digitalnih potrdil 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 sestavlja 7 članov:

- vodja organizacijske enote MO pristojne za informatiko in telekomunikacije, ki je vodja sveta,
- vodja organizacijske enote MO pristojne za obveščevalno varnostne zadeve,
- vodja organizacijske enote MO pristojne za pravne zadeve,
- prvi varnostni inženir iz skupine za upravljanje z digitalnimi potrdili korenskega izdajatelja,
- prvi administrator iz skupine za upravljanje z informacijskim sistemom korenskega izdajatelja,
- dva člana Sveta sta strokovna sodelavca iz organizacijske enote MO pristojne za informatiko in telekomunikacije, ki ju predlaga vodja sveta.

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

1.3.1.2. Operativno osebje izdajateljev SIMoD-PKI

Operativno osebje izdajateljev SIMoD-PKI 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.

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 so:

- fizične osebe - zaposleni v MO in v institucijah, ki opravljajo naloge povezane z obrambo,
- organizacijske enote in organi v sestavi MO (v nadaljevanju organizacijske enote MO),
- institucije, ki opravljajo naloge povezane z obrambo,
- funkcijske in organizacijske vloge, povezane z opravljanjem vojaških nalog ali drugih nalog s področja obrambe,
- strežniki in druga strojna ter programska oprema,
- izdajatelji varnih časovnih žigov,
- sistemi za preverjanje veljavnosti digitalnih potrdil ter drugi ponudniki storitev overjanja.

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

Odgovorna oseba za digitalno potrdilo za institucije, ki opravljajo naloge povezane z obrambo, je predstojnik institucije.

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 časovnih žigov in druge ponudnike storitev overjanja je vodja notranje organizacijske enote MO, ki upravlja z izdajateljem časovnega žiga ali drugim ponudnikom storitev overjanja.

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

Izdajatelj ali medsebojno priznani drugi izdajatelj je s tehničnega stališča tudi imetnik digitalnega potrdila, vendar se v tem dokumentu oznaka “imetnik” uporablja za tiste lastnike digitalnih potrdil, ki uporabljajo digitalna potrdila za namene, različne od podpisovanja in izdajanja digitalnih potrdil ter podpisovanja registra preklicanih potrdil.

1.3.4. Tretje osebe

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

1.3.5. Posredno odgovorni organi

Izdajatelji SIMoD-PKI delujejo v KIS MO in SV in obratujejo v skladu s predpisi MO za področje KIS MO in SV. Posredno odgovorni organi so tudi organizacijske enote MO, ki so pristojne za področje varovanja ter nadzora KIS MO in SV.

1.4. Namen uporabe digitalnih potrdil

Namen uporabe digitalnih potrdil je določen z namenom uporabe pripadajočih ključev, glej tudi poglavje 6.1.7 Namen uporabe ključev:

Digitalno potrdilo	Namen uporabe zasebnega ključa	Namen uporabe javnega ključa oz. digitalnega potrdila
korenskega izdajatelja	digitalno podpisovanje potrdil podrejenih izdajateljev in medsebojno priznanih izdajateljev ter registrov preklicanih izdajateljev	preverjanje digitalnega podpisa na potrdilih podrejenih izdajateljev in medsebojno priznanih izdajateljev ter registrih preklicanih izdajateljev
podrejenega izdajatelja	digitalno podpisovanje digitalnih potrdil in registrov preklicanih potrdil	preverjanje digitalnega podpisa na digitalnih potrdilih in registrih preklicanih potrdil
za preverjanje digitalnega podpisa	digitalno podpisovanje	preverjanje digitalnega podpisa
za šifriranje	dešifriranje[2]	šifriranje[3]
za preverjanje digitalnega podpisa in šifriranje	digitalno podpisovanje in dešifriranje	preverjanje digitalnega podpisa in šifriranje
izdajatelja varnih časovnih žigov	digitalno podpisovanje varnih časovnih žigov	preverjanje varnih časovnih žigov
ponudnika storitev overjanja	digitalno podpisovanje podatkov ponudnika storitev overjanja	preverjanje podatkov ponudnika storitev overjanja

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

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

Digitalna potrdila izdajateljev SIMoD-PKI se morajo uporabljati v skladu s Politiko SIMoD-PKI in pravili delovanja izdajatelja. Namenjena so izključno službeni uporabi v MO, v drugih institucijah pa je namen omejen na opravljanje nalog povezanih z obrambo države.

Infrastruktura javnih ključev na MO omogoča pet osnovnih varnostnih storitev:

- **zaupnost**, lastnost podatkov v elektronski obliki, da so nerazumljivi ali nerazpoložljivi neavtoriziranim osebam,
- **celovitost**, lastnost podatkov v elektronski obliki, da se niso spremenili na način, ki ga ne bi bilo moč ugotoviti,
- **nezanikanje**, lastnost oz. mehanizem, ki onemogoča zanikanje izvršenega dejanja (npr. elektronske transakcije) oz. lastništva podatkov v elektronski obliki,
- **preverjanje istovetnosti**, mehanizem za preverjanje identitete v elektronski obliki in
- **selektivno omejevanje dostopa**, lastnost podatkov v elektronski obliki, da so kot šifrirani podatki nerazumljivi ali nerazpoložljivi neavtoriziranim osebam.

Infrastruktura javnih ključev na MO zagotavlja zgoraj navedene varnostne storitve prepoznavanja oziroma preverjanja istovetnosti, celovitosti in nezanikanja z varnostnim mehanizmom digitalnega podpisa, zaupnost in omejevanje dostopa pa z mehanizmi izmenjave ključev kot podporo simetričnim šifrirnim algoritmom. Te osnovne varnostne storitve omogočajo dolgoročno celovitost podatkov, vendar same zase včasih ne zagotavljajo celovitosti v vseh primerih. Če obstaja zahteva po zagotavljanju verodostojnosti podpisa v časovnem obdobju, ki presega veljavnost potrdila za preverjanje podpisa, je zahtevana dodatna storitev časovnega žigosanja. Ta storitev mora biti predpisana z ustreznimi politikami delovanja izdajateljev varnih časovnih žigov.

1.4.1. Dovoljena uporaba digitalnih potrdil

1.4.1.1. Stopnja zaupanja v digitalno potrdilo

Digitalno potrdilo nedvoumno povezuje imetnika digitalnega potrdila z njegovim javnim ključem. Celovitost in varnost povezave med imetnikom in njegovim javnim ključem je ocenjena s stopnjo zaupanja v digitalno potrdilo. Stopnja zaupanja je odvisna od strogosti registracijskih postopkov, postopkov pri upravljanju z digitalnimi potrdili in pripadajočimi zasebnimi ključi, zahtev glede osebja, fizičnega in tehničnega varovanja infrastrukture javnih ključev ter varovanja zasebnih ključev.

Stopnje zaupanja v digitalna potrdila izdajateljev SIMoD-PKI so določene z izpolnjevanjem naslednjih pogojev:

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 (v strojni obliki, npr. pametna kartica)	DA	NE	NE
Stopnja zaupanja:	VISOKA	SREDNJA	NIZKA

V nadaljevanju so podane smernice za uporabo digitalnih potrdil različnih stopenj zaupanja Odločitev o uporabi digitalnega potrdila ustrezne stopnje zaupanja mora biti rezultat konkretne študije, ki upošteva konkretno okolje uporabe in vključuje obvladovanje tveganj. Študija upošteva dejstvo ali gre za tajne, osebne ali druge podatke, ki glede na pomembnost, zahtevo po celovitosti in razpoložljivosti, zahtevajo uporabo digitalnih potrdil določene stopnje zaupanja. Ustreznost odločitve potrdi odgovorni organ, ki izda dovoljenje za obratovanje informacijske rešitve.

Uporaba digitalnih potrdil oziroma varnostnih storitev infrastrukture javnih ključev MO ne povečuje ravni zaščite KIS MO in SV, povečuje pa varnost konkretne aplikacije oziroma informacijske rešitve. Izjemoma je dopustna uporaba digitalnih potrdil za zagotavljanje tajnosti, kjer se omrežje z nizko ravnjo zaščite uporablja samo kot prenosni medij (npr.

podatki stopnje tajnosti INTERNO se prenašajo preko javnega Internet omrežja). Digitalna potrdila se uporabljajo v okviru KIS MO in SV za implementacijo varnostnih storitev, ki jih KIS MO in SV sam ne nudi.

1.4.1.2. Uporaba digitalnih potrdil VISOKE in SREDNJE stopnje zaupanja

Uporaba digitalnih potrdil VISOKE in SREDNJE stopnje zaupanja zagotavlja:

- celovitost, preverjanje istovetnosti in nezanikanje podatkov vseh stopenj tajnosti,
- zaupnost podatkov do stopnje tajnosti vključno INTERNO,
- selektivno omejevanje dostopa do podatkov do stopnje tajnosti vključno TAJNO,
- upravljanje z varnostnimi parametri v KIS; upravljanje s šifrirnimi ključi naprav v KIS (usmerjevalniki, šifrirne naprave), daljinski nadzor in upravljanje z napravami in
- preverjanje istovetnosti naprav v KIS.

Pri prenosu podatkov stopnje tajnosti ZAUPNO in višje v nevarovanem KIS ni dovoljeno uporabljati digitalnih potrdil za šifriranje kot edinega varnostnega mehanizma za zagotavljanje zaupnosti teh podatkov.

1.4.1.3. Uporaba digitalnih potrdil NIZKE stopnje zaupanja

V vseh primerih, kjer se uporabljajo potrdila z NIZKO stopnjo zaupanja, se lahko uporabljajo tudi potrdila SREDNJE in VISOKE stopnje zaupanja.

Uporaba digitalnih potrdil NIZKE stopnje zaupanja zagotavlja:

- celovitost, preverjanje istovetnosti, selektivno omejevanje dostopa, zaupnost in nezanikanje za podatke brez stopnje tajnosti (npr. spletni dostop po protokolu SSL),
- zaupnost podatkov, ki niso tajni podatki po [20] ZTP, npr. osebni podatki,
- upravljanje z varnostnimi parametri v KIS; upravljanje s šifrirnimi ključi naprav v KIS (usmerjevalniki, šifrirne naprave), daljinski nadzor in upravljanje z napravami; predpogoj je ustrezno fizično varovanje naprav, da je možnost zlorabe digitalnih potrdil majhna in
- preverjanje istovetnosti naprav v KIS, če so naprave fizično varovane, da je možnost zlorabe potrdil majhna.

1.4.2. Nedovoljena uporaba digitalnih potrdil

Ni relevantno.

1.5. Upravljanje s Politiko SIMoD-PKI

1.5.1. Organ, ki upravlja s tem dokumentom

Svet za upravljanje z infrastrukturo javnih ključev na MO nadzira izdelavo, vodi postopek potrditve in ocenjuje, predlaga ter načrtuje uveljavitev sprememb in dopolnitev Politike SIMoD-PKI.

Spremembe in dopolnitve oziroma novo Politiko SIMoD-PKI potrdi minister.

1.5.2. Kontaktna oseba

Naslov:	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
Faks:	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 s Politiko SIMoD-PKI

Odgovorni organ za odobritev skladnosti pravil delovanja izdajatelja SIMoD-PKI s Politiko SIMoD-PKI je Svet za upravljanje z infrastrukturo javnih ključev na MO.

1.5.4. Postopek odobritve Pravil delovanja izdajatelja

Svet za upravljanje z infrastrukturo javnih ključev na MO:

- preveri skladnost pravil delovanja izdajatelja SIMoD-PKI s Politiko SIMoD-PKI in
- vodi postopek potrditve pravil delovanja izdajatelja SIMoD-PKI.

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.
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 oz. razširjenim standardom X.509 ver.3.
Imetnik potrdila	Fizična oseba, navedena v digitalnem potrdilu v polju »Subject«. Lastnik zasebnega ključa, ki ustreza javnemu ključu, vsebovanem v digitalnem potrdilu oziroma odgovorna oseba za uporabo digitalnega potrdila.
Informacijski sistem	Skupek naprav in postopkov, ki omogočajo obdelavo informacij oz. nudijo informacijske storitve. Združuje računalniško strojno in programsko opremo, nosilce podatkov, podatkovne zbirke in druge naprave ter identifikacijske, avtorizacijske, upravljavske in nadzorne postopke v funkcionalno celoto.
Infrastruktura javnih ključev	Nabor pravil, postopkov, vlog in informacijski sistem za implementacijo varnostnih storitev na osnovi kriptografije javnih ključev oziroma za upravljanje digitalnih potrdil.
Izdajatelj	Izdajatelj digitalnih potrdil, ki deluje v okviru overitelja.
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.
Politika digitalnih potrdil	Nabor pravil, ki posledično definira uporabnost digitalnih potrdil v določeni skupini uporabnikov in/ali za določen nabor aplikacij s skupnimi varnostnimi zahtevami.
Ponudnik storitev zaupanja	Po definiciji 19. odstavka 3. člena [3] eIDAS: fizična ali pravna oseba, ki zagotavlja eno ali več storitev zaupanja.
Pošiljatelj elektronskega sporočila	Oseba, ki je sama poslala elektronsko sporočilo ali pa je bilo sporočilo poslano v njenem imenu in v skladu z njeno voljo; posrednik elektronskega sporočila se ne šteje za pošiljatelja tega elektronskega sporočila.
Potrdilo za elektronski podpis	Po definiciji 14. odstavka 3. člena [3] eIDAS: elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega podpisa s fizično osebo in potrjuje vsaj ime ali psevdonim te osebe. V tem dokumentu se namesto izraza »potrdilo za elektronski podpis« uporablja izraz »digitalno potrdilo«.
Prejemnik elektronskega sporočila	Oseba, ki je prejela elektronsko sporočilo; posrednik elektronskega sporočila se ne šteje za prejemnika tega elektronskega sporočila.
Prijavna služba	Služba oziroma organizacija, ki po pooblastilu izdajatelja sprejema zahtevke in preverja istovetnosti bodočih imetnikov.
Razločevalno ime	(Ang. distinguished name) je oblika zapisa podatkov o imetniku digitalnega potrdila. Razločevalno ime se tvori v skladu s priporočilom IETF RFC 5280 in standardom X.501.
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 [20] 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).
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 (ang. Leightweight Directory Access Protocol).
MO	Ministrstvo za obrambo
OCSP	Protokol za sprotno preverjanje veljavnosti digitalnih potrdil in je specificiran po priporočilu IETF RFC 2560 (ang. Online Certificate Status Protocol)
PKCS	Priporočila podjetja RSA Security za uporabo asimetričnih kriptografskih algoritmov (ang. Public Key Cryptographic Standards).
PKCS#1	Osnovna pravila za formatiranje podatkov ob implementaciji RSA funkcij. Predpisuje, kako se izračuna digitalni podpis, kako se formatirajo podatki, ki se podpisujejo in format podpisa. Predpisuje tudi sintakso javnega in zasebnega RSA ključa.
PKCS#10	Sintaksa zahtevka za digitalno potrdilo. Zahtevek za digitalno potrdilo vsebuje razločevalno ime, javni ključ in nabor drugih atributov, ki jih podpiše subjekt, ki zahteva potrditev. Daljše ime: PKCS#10 Certification Request Syntax Standard.

PKCS#7	Sintaksa za kriptografsko obdelane podatke, kot digitalni podpisi in digitalne ovojnice.
PKI	Infrastruktura javnih ključev; strojna in programska oprema ter varnostni mehanizmi za zaupanja vredno implementacijo varnostnih storitev, ki temeljijo na nesimetrični kriptografiji (ang. Public Key Infrastructure).
PKIX	Delovna skupina za področje infrastrukture javnih ključev v okviru IETF (ang. Internet Engineering Task Force). Izdala serijo priporočil za digitalna potrdila in registre preklicanih potrdil (ang. Public Key Infrastrukture X.509).
PKIX- CMP	Postopek izmenjave podatkov, ki se nanašajo na digitalna potrdila med subjekti infrastrukture izdajatelja (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
RFC	Priporočila, ki jih izdaja IETF.
RFC 5280	Priporočilo, ki določa elemente potrdil in registra preklicanih potrdil.
RFC 3647	Priporočilo, ki določa elemente, ki naj bodo zajeti v politiki overitelja (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework).
RFC 4210	Priporočilo, ki določa postopke za izmenjavo podatkov, ki se nanašajo na digitalna potrdila. Vsebuje PKIX-CMP.
RSA	Eden prvih nesimetričnih kriptografskih sistemov, patentiran leta 1983, imenovan po odkriteljih: Rivest, Shamir in Adelman.
SIMoD-PKI	Infrastruktura javnih ključev Ministrstva za obrambo Republike Slovenije (ang. **S**loveni**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 na naslovu imenik.simod-pki.mors.si in
- na spletni strani http://www.simod-pki.mors.si.

2.2. Objave informacij o digitalnih potrdilih

Na spletni strani http://www.simod-pki.mors.si so objavljeni naslednji podatki:

- Politika SIMoD-PKI in pravila delovanja izdajateljev,
- digitalno potrdilo korenskega izdajatelja,
- digitalna potrdila podrejenih izdajateljev,
- registri preklicih potrdil in
- druge javne objave izdajateljev.

Izdajatelji v imeniku objavljajo naslednje podatke:

- digitalna potrdila imetnikov in
- registre preklicanih potrdil:
    - delne registre ter
    - kombinirani register.

Imenik je dostopen po protokolu LDAP.

Kombinirani register preklicanih potrdil je dostopen tudi po protokolu HTTP na spletnem naslovu, ki je naveden v razširitvenem polju digitalnega potrdila, kot je navedeno v poglavju 7.1.2 Razširitvena polja.

Izdajatelji SIMoD-PKI objavljajo navodila uporabnikom za varno uporabo digitalnih potrdil in zahtevke za pridobitev, preklic ter druge storitve v zvezi z digitalnimi potrdili. V pravilih delovanja posameznega izdajatelja SIMoD-PKI je naveden spletni naslov, na katerem so dokumenti dostopni.

Izdajatelji SIMoD-PKI si lahko pridržijo pravico, da nekaterih podatkov v javno dostopnih kopijah repozitorijev ne objavijo.

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. Objava registrov preklicanih potrdil je v skladu s poglavji 4.9.7 Pogostost objav registrov preklicanih potrdil in 4.9.8 Dovoljene zakasnitve pri objavi registrov preklicanih potrdil.

2.4. Dostop do podatkov v repozitorijih

Vpogled v podatke iz poglavja 2.2. Objave informacij o digitalnih potrdilih je brez omejitev.

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

Razločevalno ime imetnika je v digitalnem potrdilu shranjeno v polju Subject, razločevalno ime izdajatelja pa v polju Issuer.

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 neki drugi pravni ali fizični osebi ali je v nasprotju z veljavnimi predpisi. V teh primerih prijavna služba in operativno osebje izdajatelja predlaga drugačno ime.

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

Splošno ime v digitalnih potrdilih za 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

V skladu s poglavji 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 splošne nazive za organizacijske enote 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. Izdajatelji SIMoD-PKI ne smejo 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 se v okviru SIMoD-PKI tega ne preverja niti ne bo Svet za upravljanje z infrastrukturo javnih ključev na MO posredoval v takšnih sporih. Prijavna služba in operativno osebje izdajatelja 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

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

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

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 ali institucijo, ki opravlja naloge povezane z obrambo države, mora vsebovati uradni naziv organizacijske enote MO ali institucije, naslov in ime odgovorne osebe, ki je praviloma vodja organizacijske enote MO oziroma predstojnik institucije. 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; če je bodoči imetnik institucija, ki opravlja naloge povezane z obrambo države, lahko prijavna služba zahteva dodatna dokazila. Nato 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 za 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.

3.2.3. Preverjanje istovetnosti za fizične osebe

Zahtevek za pridobitev digitalnega potrdila za zaposlene v MO in v institucijah, ki opravljajo naloge povezane z obrambo države, izpolnita in podpišeta bodoči imetnik in vodja njegove organizacijske enote oziroma predstojnik institucije. Za pravilnost podatkov jamči vodja organizacijske enote oziroma predstojnik institucije 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; če je bodoči imetnik zaposlen v instituciji, ki opravlja naloge povezane z obrambo države, lahko prijavna služba zahteva dodatna dokazila, da je bodoči imetnik zaposlen v instituciji. Nato 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.

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 ali institucije,
- 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, predstojnik institucije oziroma poveljnik enote SV.

3.2.5. Preverjanje pooblastil

Vodja organizacijske enote MO ali predstojnik institucije, ki opravlja naloge povezane z obrambo, oziroma poveljnik enote 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, institucijo, funkcijsko ali organizacijsko vlogo, ali napravo.

3.2.6. Merila za medsebojno povezovanje

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

3.3. Preverjanje imetnikov za ponovno izdajo digitalnega potrdila

3.3.1. Preverjanje istovetnosti pri rutinski ponovni izdaji digitalnih potrdil

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

Rutinska ponovna izdaja digitalnih potrdil, 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.

S pravili delovanja posameznega izdajatelja so lahko določeni drugačni načini preverjanja istovetnosti za ponovno izdajo digitalnega potrdila v izjemnih primerih.

3.4. Preverjanje istovetnosti ob zahtevi za preklic digitalnega potrdila

Oseba, ki želi preklicati digitalno potrdilo, se identificira:

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

Osebna identifikacija ni obvezna.

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 in v institucijah, ki opravljajo naloge povezane z obrambo.

Zahtevek za pridobitev digitalnega potrdila za splošne nazive za organizacijske enote MO ali institucije, ki opravljajo naloge povezane z obrambo države, oddajo predstojniki organizacijske enote vsaj na ravni vodje sektorja za organizacijske enote MO oziroma predstojniki institucij.

Zahtevek za pridobitev digitalnega potrdila za splošne nazive za funkcijske ali organizacijske vloge lahko oddajo nosilci, skrbniki ali administratorji vloge.

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 ustreznega izdajatelja SIMoD-PKI.

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 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 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 ustreznega izdajatelja.

Odobritev ali zavrnitev izdaje digitalnega potrdila NIZKE stopnje zaupanja je odgovornost in pravica operativnega osebja izdajatelja. Obvestilo o zavrnitvi pošlje operativno osebje izdajatelja 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 izdajateljev SIMoD-PKI ob izdaji potrdil

Operativno osebje izdajatelja začne s postopki izdajanja digitalnega potrdila SREDNJE in VISOKE stopnje zaupanja po prejemu odobrenega zahtevka od prijavne službe.

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

Operativno osebje izdajatelja 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 ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, operativno osebje izdajatelja bodočemu imetniku ne pošilja aktivacijskih podatkov. Ključe in digitalna potrdila generira operativno osebje izdajatelja. 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 oziroma mora biti vedno pod kontrolo imetnika. Izdajatelj 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 ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, generira ključe izdajatelj. Izdajatelj 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 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 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.

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, generira ključe in digitalno potrdilo izdajatelj. Izdajatelj dostavi javni ključ imetniku z digitalnim potrdilom na pametni kartici.

Izdajateljevo digitalno potrdilo 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 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 izdajatelj 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 objavi v imeniku iz poglavja 2.2. Objave informacij o digitalnih potrdilih.

4.4. Prevzem digitalnega potrdila

4.4.1. Postopek prevzema digitalnega potrdila

V okviru SIMoD-PKI sta izdaja in prevzem digitalnega potrdila neločljivo povezana. Bodoči imetnik praviloma prevzame digitalno potrdilo samo z ustreznimi aktivacijskimi podatki: referenčno številko in avtorizacijsko kodo.

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

Postopek prevzema je odvisen od strojne in programske opreme na strani uporabnika in posameznega izdajatelja. Izdajatelji morajo v svojih pravilih delovanja opisati postopek prevzema oziroma objaviti uporabniška navodila za prevzem digitalnih potrdil.

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, opravi prevzem digitalnega potrdila izdajatelj. Izdajatelj nato pametno kartico s prevzetim digitalnim potrdilom na varen način posreduje imetniku.

Ob prevzemu digitalnega potrdila je imetnik dolžan preveriti vsebino digitalnega potrdila, ali je digitalno potrdilo podpisal pravi izdajatelj ter polno pot digitalnih podpisov do korenskega izdajatelja. 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 tudi 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 2.2. Objave informacij o digitalnih potrdilih. Izdajatelji lahko v imenikih objavijo tudi digitalna potrdila z javnim ključem za preverjanje digitalnega podpisa.

4.4.3. Obveščanje drugih udeležencev o izdaji digitalnega potrdila

Ni predvideno.

4.5. Uporaba ključev in digitalnih potrdil

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

4.5.1. Uporaba ključev in digitalnih potrdil imetnikov

4.5.1.1. Zasebni ključi in digitalna potrdila izdajateljev

Korenski izdajatelj lahko uporablja svoj zasebni ključ samo za podpisovanje digitalnih potrdil podrejenih in medsebojno priznanih izdajateljev, registrov preklicanih izdajateljev in digitalnih potrdil svojega operativnega osebja. Korenski izdajatelj ne izdaja uporabniških digitalnih potrdil.

Podrejeni izdajatelji SIMoD-PKI lahko uporabljajo svoje zasebne ključe samo za podpisovanje digitalnih potrdil in registrov preklicanih potrdil. Podrejeni izdajatelji podpisujejo digitalna potrdila za uporabnike storitev infrastrukture javnih ključev na MO, ki so določeni v poglavju 1.3.3 Imetniki digitalnih potrdil, operativno osebje posameznega izdajatelja in osebje prijavne službe.

Operativno osebje izdajateljev SIMoD-PKI uporablja digitalna potrdila in pripadajoče ključe izključno za izvajanje nalog operativnega osebja izdajatelja. V primeru, da izdajateljevi zaposleni potrebujejo ključe oziroma digitalna potrdila kot uporabniki oziroma za druge namene, kot je opravljanje nalog operativnega osebja izdajatelja, morajo zaprositi za izdajo uporabniških digitalnih potrdil.

4.5.1.2. Zasebni ključi in digitalna potrdila prijavne službe

Osebje prijavne službe lahko uporablja digitalna potrdila, izdana za izvajanje nalog prijavne službe, samo za te namene. V primeru, da zaposleni prijavne službe potrebujejo ključe oziroma digitalna potrdila kot uporabniki oziroma za druge namene kot je delo v prijavni službi, morajo zaprositi za izdajo uporabniških digitalnih potrdil.

4.5.1.3. Uporabniški zasebni ključi in digitalna potrdila

Imetnik digitalnega potrdila je dolžan:

- uporabljati ključe in digitalna potrdila samo za namene, ki so definirani v Politiki SIMoD-PKI in pravilih delovanja izdajatelja,
- po prevzemu digitalnega potrdila preveriti podatke v digitalnem potrdilu in ob morebitnih napakah in problemih takoj obvestiti operativno osebje izdajatelja oziroma zahtevati preklic digitalnega potrdila,
- vse spremembe, ki so povezane s digitalnimi potrdili, v osmih (8) dneh sporočiti prijavni službi ali operativnemu osebju izdajatelja,
- 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 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,
- 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[4]

4.7.1. Razlogi za ponovno izdajo digitalnega potrdila

Ponovna izdaja digitalnega potrdilo 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 in 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.

S pravili delovanja izdajatelja so lahko določeni drugačni postopki obdelave zahtevka za ponovno izdajo digitalnega potrdila v izjemnih primerih.

Ponovna izdaja digitalnih potrdil pred pretekom veljavnosti se za digitalna potrdila po protokolu PKCS#10 izvede na osnovi ustreznega elektronskega zahtevka, ki je podpisan z veljavnim digitalnim potrdilom. Zahtevek se obdeluje smiselno enako kot zahtevek za prvo

4 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.

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 digitalna potrdila, izdana po protokolu PKIX-CMP, izvede samodejno ob prvi uporabi digitalnega potrdila z neposrednim dostopom do izdajatelja v predefiniranem časovnem obdobju pred pretekom 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 izdajateljev in izdajateljev varnih časovnih žigov mora biti pod kontrolo operativnega osebja SIMoD-PKI.

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 digitalnega potrdila po protokolu PKIX-CMP namenska programska oprema imetnika obvesti o uspešnem prevzemu digitalnega potrdila.

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

4.7.5. Postopek potrditve prevzema novega digitalnega potrdila

Enako kot 4.4.1 Postopek prevzema digitalnega potrdila.

4.7.6. Objava novega digitalnega potrdila

Enako kot 4.4.2 Objava digitalnega potrdila.

4.7.7. Obveščanje drugih udeležencev o izdaji digitalnega potrdila

Enako kot 4.4.3 Obveščanje drugih udeležencev o izdaji digitalnega potrdila.

4.8. Sprememba digitalnega potrdila

Sprememba 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,
- sprememba podatkov, ki so vsebovani v digitalnem potrdilu in
- razlogi, navedeni v poglavju 4.11. Predčasna prekinitev veljavnosti digitalnih potrdil.

4.9.1.2. Okoliščine preklica digitalnega potrdila korenskega izdajatelja

Razlogi za preklic digitalnega potrdila korenskega izdajatelja so:

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

4.9.1.3. Okoliščine preklica digitalnega potrdila o priznavanju drugega izdajatelja

Korenski izdajatelja prekliče digitalno potrdilo o priznavanju drugega izdajatelja iz naslednjih razlogov:

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

4.9.1.4. Okoliščine preklica digitalnega potrdila podrejenega izdajatelja

Razlogi za preklic digitalnega potrdila podrejenega izdajatelja so:

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

4.9.2. Kdo lahko zahteva preklic

4.9.2.1. Kdo lahko zahteva preklic digitalnega potrdila imetnika

Zahtevo za preklic digitalnega potrdila imetnika lahko poda:

- imetnik za svoje digitalno potrdilo,
- vodja organizacijske enote MO oziroma predstojnik institucije, ki je povezana z obrambo države,
- nosilec, skrbnik oziroma administrator funkcijske ali organizacijske vloge ali njegov nadrejeni oziroma predstojnik ustrezne organizacijske enote MO,
- skrbnik strežnika, druge strojne ali programske opreme, izdajatelja varnih časovnih žigov, ponudnika storitev overjanja,
- operativno osebje izdajatelja, 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

Preklic digitalnega potrdila korenskega izdajatelja lahko zahteva:

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

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

Preklic digitalnega potrdila o priznavanju drugega izdajatelja lahko zahteva:

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

4.9.2.4. Kdo lahko zahteva preklic digitalnega potrdila podrejenega izdajatelja

Preklic digitalnega potrdila izdajatelja lahko zahteva:

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

4.9.3. Postopki za preklic

4.9.3.1. Postopki preklica imetniških digitalnih potrdil

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.

Preklic izvrši operativno osebje izdajatelja.

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 objaviti preklicano digitalno potrdilo v registru preklicanih potrdil.

Operativno osebje izdajatelja 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 v skladu s poglavji 4.1. Pridobitev digitalnega potrdila do 4.4. Prevzem digitalnega potrdila.

4.9.3.2. Postopki preklica digitalnega potrdila korenskega izdajatelja

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

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

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

4.9.3.3. Postopki preklica digitalnega potrdila o priznavanju drugega izdajatelja

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

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

Preklicano digitalno potrdilo mora biti objavljeno v registru preklicanih izdajateljev.

4.9.3.4. Postopki preklica digitalnega potrdila podrejenega izdajatelja

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

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

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

Korenski izdajatelj mora ob preklicu digitalnega potrdila podrejenega izdajatelja izvesti naslednje postopke:

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

4.9.4. Čas za posredovanje zahtevka za preklic

Osebe, ki lahko zahtevajo preklic (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 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.

Operativno osebje izvede preklic v štiriindvajsetih (24) urah po prejemu zahtevka za preklic v primeru:

- spremembe podatkov v digitalnem potrdilu,
- prenehanja delovnega razmerja imetnika,
- prenehanja delovanja organizacijske enote MO ali institucije, ki je povezana z obrambo države, organizacijske ali funkcijske vloge,
- spremembe statusa imetnika, zaposlenega v instituciji, ki je povezana z obrambo države, ki ima za posledico dejstvo, da imetnik ne opravlja več nalog povezanih z obrambo države ali
- spremembe statusa institucije, ki je povezana z obrambo države, ki ima za posledico dejstvo, da institucija ne opravlja več nalog povezanih z obrambo države.

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

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

4.9.5.3. Čas za preklic digitalnega potrdila o priznavanju drugega izdajatelja

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

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

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

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

4.9.5.4. Čas za preklic digitalnega potrdila podrejenega izdajatelja

Korenski izdajatelj prekliče digitalno potrdilo podrejenega izdajatelja takoj, ko prejme zahtevek, ali v roku, ki ga določi Svet za upravljanje z infrastrukturo javnih ključev na MO.

4.9.6. Obveza preverjanja registra preklicanih potrdil

Tretje osebe, ki se zanašajo na digitalno potrdilo, so pred uporabo dolžne preveriti najnovejši register preklicanih potrdil. Kot del postopka preverjanja je potrebno preveriti tudi veljavnost in verodostojnost registra preklicanih potrdil. Tretja oseba mora za vsako uporabljeno digitalno potrdilo izvesti popoln postopek preverjanja poti zaupanja v skladu z [17] 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

Izdajatelji imetniških digitalnih potrdil so dolžni objaviti nov register preklicanih potrdil:

- vsaj na petindvajset (25) ur in
- ob preklicu digitalnega potrdila.

Korenski izdajatelj objavi pogostost objav registrov preklicanih potrdil in registrov preklicanih izdajateljev v svojih pravilih delovanja.

4.9.8. Dovoljene zakasnitve pri objavi registrov preklicanih potrdil

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

Izdajatelji morajo izdati nov register preklicanih potrdil 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 mora biti protokol za sprotno preverjanje statusa digitalnih potrdil (ang. On-line Certificate Status Protocol, OCSP) v skladu s priporočilom [18] 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

Lokacije in tehnične lastnosti registrov preklicanih potrdil in storitve sprotnega preverjanja statusa digitalnih potrdil so navedene v pravilih delovanja posameznega izdajatelja SIMoD-PKI.

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 predpisane.

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 oziroma institucije, ki je opravlja naloge povezane z obrambo države,
- ukinitev organizacijske ali funkcijske vloge,
- sprememba statusa imetnika, zaposlenega v instituciji, ki je opravlja naloge povezane z obrambo države, ki ima za posledico dejstvo, da imetnik ne opravlja več nalog povezanih z obrambo države,
- sprememba statusa institucije, ki je opravlja naloge povezane z obrambo države, ki ima za posledico dejstvo, da institucija ne opravlja več nalog, povezanih z obrambo države,
- prenehanje potrebe po varnostni storitvi strežnika, druge strojne ali programske opreme in
- prenehanje potrebe po storitvi izdajanja časovnih žigov ali podobni storitvi overjanja.

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

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 izdajateljev in izdajateljev varnih časovnih žigov se zagotavlja v skladu s poglavji 6.2.4 Varnostno kopiranje zasebnih ključev.

4.12.1.Povrnitev zgodovine ključev za dešifriranje

Izdajatelji morajo v svojih pravilih delovanja navesti, za katera digitalna potrdila je omogočena storitev varnostnega kopiranja in povrnitve zgodovine ključev za dešifriranje.

Povrnitev zgodovine ključev za dešifriranje se izvede ob ponovni izdaji digitalnega potrdila (glej poglavje 4.7. Ponovna izdaja digitalnih potrdil).

Ob prošnji za pridobitev digitalnega potrdila po preklicu ali preteku veljavnosti digitalnih potrdil se imetniku ob izdaji novih digitalnih potrdil praviloma tudi povrne zgodovina zasebnih ključev za dešifriranje.

4.12.2.Odkrivanje kopije ključev za dešifriranje

Izdajatelji morajo v svojih pravilih delovanja navesti, za katera digitalna potrdila je omogočena storitev odkrivanja kopije ključev za dešifriranje.

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 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 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

Dejavnosti izdajateljev SIMoD-PKI se izvajajo v varovanih prostorih in na varnih lokacijah.

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. Druge osebe, ki izkažejo upravičeni interes, smejo vstopiti v prostore samo v spremstvu operativnega osebja izdajatelja. Vstop v prostore je video nadzorovan. O vstopih in izstopih v prostore se vodi evidenca.

5.1.3. Napajanje in klimatske naprave

Prostor s komunikacijsko in informacijsko opremo izdajatelja mora biti 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 izdajateljev SIMoD-PKI so na lokaciji, kjer je verjetnost poplave zelo majhna.

5.1.5. Zaščita pred ognjem

Prostori s komunikacijsko in informacijsko opremo izdajateljev SIMoD-PKI so opremljeni z detektorji temperature in dima.

5.1.6. Shranjevanje medijev

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

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

5.1.7. Odstranjevanje odpadkov

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

V primeru, da dokumentov in medijev ni mogoče varno izbrisati ali uničiti v prostorih izdajateljev, jih je potrebno dostaviti 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

Izdajatelji SIMoD-PKI uporabljajo oddaljeno lokacijo za varno hranjenje varnostnih kopij in arhivskih podatkov. Podatki, mediji ali naprave so na oddaljeni lokaciji shranjeni v varovanih prostorih, ki zagotavljajo enako raven varnosti, kot je v prostorih izdajateljev.

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 upravljanja overitelja na MO

5.2.1.1. Operativno osebje izdajateljev SIMoD-PKI

Naloge upravljanja z infrastrukturo javnih ključev na MO na nivoju posameznega izdajatelja so porazdeljene med operativno osebje tako, da je zagotovljena ločitev med zaključenimi vsebinskimi področji upravljanja. Operativno osebje izdajatelja je glede na vsebinska področja upravljanja razdeljeno na zaključene organizacijske skupine:

- upravljanje z digitalnimi potrdili,
- upravljanje s programsko in strojno opremo izdajatelja ter
- varovanje in nadzor komunikacijskega sistema za infrastrukturo javnih ključev na MO.

Posamezni operativni osebi izdajatelja je dovoljeno opravljanje nalog samo znotraj ene zaključene organizacijske skupine. Posamezna oseba lahko opravlja naloge za več izdajateljev, pri čemer mora biti pri vsakem izdajatelju član natanko ene organizacijske skupine.

V organizacijski skupini za upravljanje z digitalnimi potrdili so:

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

V organizacijski skupini za upravljanje s programsko in strojno opremo izdajatelja so:

- prvi administrator izdajatelja in
- administratorji izdajatelja.

V organizacijski skupini za varovanje in nadzor komunikacijskega sistema so:

- prvi administrator komunikacijskega sistema in
- administratorji komunikacijskega sistema.

5.2.1.2. Prijavna služba

Naloge prijavne službe opravlja pooblaščeno osebje organizacijske enote MO, pristojne za kadrovske zadeve. Naloge prijavne služba 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, ki upravlja z digitalnimi potrdili in
- obveščanje operativnega osebja, ki upravlja z digitalnimi potrdili, o spremembah podatkov o imetnikih digitalnih potrdil (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 izdajateljev 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 izdajateljev SIMoD-PKI.

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 izdajateljev SIMoD-PKI.

5.2.2. Število oseb, potrebnih za izvedbo postopkov

V organizacijski skupini za upravljane z digitalnimi potrdili izdajatelja morajo biti najmanj tri (3) osebe, v organizacijski skupini za upravljane s programsko in strojno opremo izdajatelja morata biti najmanj dve osebi (2), v organizacijski skupini za varovanje in nadzor komunikacijskega sistema morata biti najmanj dve (2) osebi.

V pravilih delovanja izdajatelja so določene varnostno občutljive operacije, za izvedbo katerih je zahtevana prisotnost vsaj dveh oseb.

5.2.3. Preverjanje istovetnosti operativnega osebja

Operativno osebje izdajatelja izkaže svojo istovetnost:

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

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

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

5.3. Zahteve za osebje

5.3.1. Kvalifikacije, izkušnje in varnostno preverjanje

Operativno osebje izdajatelja:

- mora biti ustrezno usposobljeno in o tem imeti dokazila,
- mora imeti za opravljanje nalog pri izdajatelju imenovanje Sveta za upravljanje z infrastrukturo javnih ključev na MO,
- ne sme opravljati drugih nalog, ki bi bile v nasprotju z opravljanjem nalog v okviru infrastrukture javnih ključev na MO,
- ne sme biti na prejšnjih podobnih dolžnostih (npr. skrbnik kriptografskih naprav, varnostni inženir v informacijskem sistemu) razrešeno nalog zaradi malomarnosti ali neizpolnjevanja obveznosti in
- mora imeti dovoljenje za dostop do tajnih podatkov najmanj TAJNO.

5.3.2. Dovoljenja za dostop do tajnih podatkov

V skladu z [20] ZTP.

5.3.3. Usposabljanje osebja

Operativno osebje izdajateljev SIMoD-PKI mora biti usposobljeno na naslednjih področjih:

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

Osebje prijavne službe mora biti usposobljeno za:

- identifikacijo naročnikov in preverjanje pravilnosti podatkov v zahtevkih ter

- delo s programsko opremo prijavne službe.

5.3.4. Pogostost dodatnih usposabljanj

Osebje se usposablja glede na potrebe oziroma novosti v zvezi z delovanjem infrastrukture javnih ključev na MO.

5.3.5. Kroženje med delovnimi mesti

Ni predpisano.

5.3.6. Ukrepi ob kršitvah pooblastil

Proti operativni osebi izdajatelja, 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 zahteva odvzem pooblastila osebi ter 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 [20] ZTP in varnostne zahteve izdajateljev.

5.3.8. Dokumentacija za operativno osebje

Operativnemu osebju izdajateljev, skupini za pomoč uporabnikom in skupini za nastavitev uporabniškega okolja so na voljo interni priročniki, originalna dokumentacija programske in strojne opreme ter priročniki šolanj, glede na njihovo funkcijo.

5.4. Postopki varnostnih pregledov sistema

5.4.1. Vrste beleženih dogodkov

Izdajatelji so dolžni beležiti dogodke:

- na operacijskem sistemu, programski in strojni opremi izdajatelja,
- na operacijskih sistemih, programski in strojni opremi elementov komunikacijskega sistema,
- v zvezi s ključi izdajatelja,
- v zvezi z imetniškimi ključi in digitalnimi potrdili - izdaja, prevzem, ponovna izdaja, preklic, povrnitev zgodovine ključev za dešifriranje in odkrivanje kopije ključev za dešifriranje,
- v zvezi z varnostno politiko in upravljanjem informacijskega sistema izdajatelja in
- v zvezi z varnostno politiko in upravljanjem komunikacijskega sistema.

Izdajatelji so dolžni zbirati in beležiti v elektronski ali pisni obliki tudi podatke, ki vplivajo na varnost, niso pa del komunikacijsko informacijskega sistema izdajatelja:

- dogodke v zvezi s fizičnim dostopom do sistemov izdajatelja ter fizično lokacijo,
- kadrovske spremembe operativnega osebja izdajatelja in
- dogodke povezane 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.

Dostop do dnevnikov beleženih dogodkov je dovoljen samo pooblaščenim osebam:

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

5.4.5. Varnostne kopije dnevnikov beleženih dogodkov

Varnostne kopije dnevnikov beleženih dogodkov, ki se zbirajo v elektronski obliki, se izdelujejo v okviru rednega varnostnega kopiranja sistemov. Pogostost rednega varnostnega kopiranja sistemov je določena v pravilih delovanja izdajatelja.

Periodično, kot določeno v pravilih delovanja izdajatelja, 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 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

Izdajatelji morajo hraniti naslednje podatke:

- dnevnike beleženih dogodkov iz poglavja 5.4.1 Vrste beleženih dogodkov,
- zahtevke imetnikov digitalnih potrdil,
- korespondenco in pogodbe imetnikov z izdajateljem,
- dokumentacijo o izvedbi preverjanja istovetnosti uporabnikov,
- sklenjene medsebojne dogovore in pogodbe,
- digitalna potrdila in liste preklicanih potrdil,
- Politike SIMoD-PKI in svoja pravila delovanja ter
- zasebne ključe za dešifriranje.

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 imetnikov, dokumentacija o izvedbi identifikacije, korespondenca in pogodbe imetnikov digitalnih potrdil z izdajatelji, verzije Politik SIMoD-PKI, verzije pravil delovanja izdajateljev in dnevniki beleženih dogodkov v pisni obliki), se hranijo in arhivirajo v skladu s postopki dela z dokumentarnim gradivom na MO.

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

5.5.4. Varnostna kopija arhiva

Podatkom, ki sodijo v dokumentarno gradivo (zahtevki imetnikov, dokumentacija o izvedbi identifikacije, korespondenca in pogodbe imetnikov digitalnih potrdil z izdajatelji, verzije Politik SIMoD-PKI, verzije pravil delovanja izdajateljev in dnevniki beleženih dogodkov v pisni obliki), se zagotavlja razpoložljivost arhiva v skladu s postopki dela z dokumentarnim gradivom na MO.

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

5.5.5. Časovno žigosanje zapisov

Ni predpisano.

5.5.6. Način arhiviranja

Ni predpisano.

5.5.7. Postopek vpogleda v arhiv in njegova verifikacija

Dostop do arhiva je dovoljen samo:

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

Ob kreiranju arhiva se preveri integriteta medija. V pravilih delovanja izdajatelja so podrobneje določeni postopki za zagotavljanje integritete arhiva, način in pogostost preverjanja integritete medijev z arhiviranimi podatki in možnost branja podatkov iz arhiva.

5.6. Zamenjava ključev izdajateljev

5.6.1. Ponovna izdaja digitalnega potrdila korenskega izdajatelja

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

Za podpisovanje digitalnih potrdil podrejenih izdajateljev se vedno uporablja najnovejši zasebni ključ korenskega izdajatelja. Za preverjanje veljavnosti digitalnih potrdil podrejenih izdajateljev pa se uporablja predhodno digitalno potrdilo korenskega izdajatelja vse dokler ne poteče veljavnost zadnjega digitalnega potrdila, podpisanega s starim zasebnim ključem

korenskega izdajatelja. Zasebni ključ se vedno uporablja krajše obdobje kot je veljavnost pripadajočega digitalnega potrdila.

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

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

5.6.2. Ponovna izdaja digitalnih potrdil podrejenih izdajateljev

Veljavnost izdajateljevega digitalnega potrdila 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 izdajateljevim zasebnim ključem. Zasebni ključ izdajatelja se vedno uporablja krajše obdobje kot je veljavnost pripadajočega izdajateljevega digitalnega potrdila.

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

Ponovna izdaja digitalnih potrdil podrejenih izdajateljev se izvede po predpisanem in nadzorovanem postopku. Posamezne korake postopka izvaja operativno osebje korenskega izdajatelja in podrejenega izdajatelja. 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 pravilih delovanja izdajatelja.

5.7.2. Uničenje programske, strojne opreme ali podatkov izdajatelja

V primeru okvare strojne ali programske opreme oziroma podatkov, pri kateri zasebni ključ izdajatelja ni bil uničen, bodo storitve izdajatelja ponovno vzpostavljene v najkrajšem možnem času. Izdajatelj mora v najkrajšem možnem času vzpostaviti vsaj funkcionalnost preklica digitalnih potrdil in objavljanja registra preklicanih potrdil.

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 4.9.3.2 Postopki preklica digitalnega potrdila korenskega izdajatelja oziroma 4.9.3.4 Postopki preklica digitalnega potrdila podrejenega izdajatelja.

5.7.3. Zloraba zasebnega ključa izdajatelja

Postopki ob zlorabi zasebnega ključa izdajatelja so predpisani v poglavju 4.9.3.2 Postopki preklica digitalnega potrdila korenskega izdajatelja oziroma 4.9.3.4 Postopki preklica digitalnega potrdila podrejenega izdajatelja.

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 oziroma uničenje in poškodovanje varovanih prostorov izdajatelja, so predpisani v pravilih delovanja posameznega izdajatelja.

5.8. Prenehanje delovanja izdajatelja

Vzroki za prenehanje delovanja izdajatelja so podani v poglavju 4.9.1.2 Okoliščine preklica digitalnega potrdila korenskega izdajatelja oziroma 4.9.1.4 Okoliščine preklica digitalnega potrdila podrejenega izdajatelja ter v veljavni zakonodaji.

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

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

- celotno operativno osebje,
- vse imetnike digitalnih potrdil oziroma odgovorne osebe,
- morebitne medsebojno priznane ali podrejene izdajatelje.

Izdajatelj bo po prenehanju delovanja izvedel postopke predpisane v poglavju 4.9.3.2 Postopki preklica digitalnega potrdila korenskega izdajatelja oziroma 4.9.3.4 Postopki preklica digitalnega potrdila podrejenega izdajatelja.

Ob prenehanju delovanja bo overitelj na MO ukrepal v skladu z veljavno zakonodajo.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev para ključev

6.1.1. Generiranje para ključev

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

Imetniški par ključev za podpisovanje oziroma par ključev za oba namena uporabe (podpisovanje in šifriranje) se razen v primerih iz naslednjega odstavka generira pri bodočem imetniku oziroma pod njegovo izključno kontrolo. Če ima bodoči imetnik sredstvo za varno elektronsko podpisovanje, to je varnostni kriptografski modul ali pametno kartico, je generiranje para ključev izvedeno znotraj tega sredstva.

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 zasebni ključ za podpisovanje oziroma za oba namena uporabe (podpisovanje in šifriranje) generira na pametni kartici pri izdajatelju.

Imetniški par ključev za šifriranje, za katerega izdajatelj zagotavlja storitev povrnitve zgodovine ključev, se generira pri izdajatelju in varno prenese bodočemu imetniku.

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 na strani bodočega imetnika oziroma v primeru uporabe pametnih kartic znotraj le te. Zasebni ključ za podpisovanje se 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, se zasebni ključ za podpisovanje oziroma za oba namena uporabe (podpisovanje in šifriranje) generira na pametni kartici pri izdajatelju. 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 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 (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

Dolžine zasebnih ključev so določene v pravilih delovanja posameznega izdajatelja.

6.1.6. Parametri za generiranje javnih ključev in preverjanje parametrov

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

6.1.7. Namen uporabe ključev

Namen uporabe ključev je določen v razširitvenem polju *keyUsage* in *extKeyUsage* po priporočilu [17] RFC 5280.

6.2. Zaščita zasebnih ključev in zahteve za kriptografske module

6.2.1. Standardi za kriptografske module

Izdajatelji digitalnih potrdil in izdajatelji varnih časovnih žigov morajo uporabljati strojne varnostne kriptografske module, ki ustrezajo uveljavljenim varnostnim in tehničnim standardom.

6.2.2. Nadzor zasebnega ključa z več pooblaščenimi osebami

Za upravljanje z zasebnim ključem izdajatelja 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 izdajateljev ni dovoljeno. Tehnična izvedba varnostnega kriptografskega modula ne omogoča prikaza zasebnega ključa izdajatelja v nešifrirani obliki.

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 se zagotavlja z mehanizmi varnostnega kriptografskega modula. Varnostna kopija se pred izvozom iz varnostnega kriptografskega modula šifrira. Dešifrirni ključ je porazdeljen na N[5] od M[6] administratorskih pametnih karticah.

Kopije zasebnih ključev za dešifriranje digitalnih potrdil, za katera izdajatelj zagotavlja storitev povrnitve zgodovine ključev, se morajo hraniti pri izdajatelju v šifrirani obliki.

6.2.5. Arhiviranje zasebnega ključa

Izdajateljev zasebni ključ se ne arhivira.

Arhivira se samo zasebne dešifrirne ključe v povezavi z imetniškimi digitalnimi potrdili, za katere izdajatelj zagotavlja povrnitev zgodovine in odkrivanje kopije ključev za dešifriranje.

6.2.6. Zapis zasebnega ključa v kriptografski modul in iz njega

Zasebni ključ izdajatelja digitalnih potrdil ali izdajatelja varnih časovnih žigov se generira v varnostnem kriptografskem modulu.

[5] N mora biti večji ali enak 2

[6] M mora biti večji ali enak 3

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 zagotavlja storitev povrnitve zgodovine in odkrivanja kopije ključev, generirajo v izdajateljevem kriptografskem modulu in se prenesejo k bodočemu imetniku z uporabo protokola PKIX-CMP.

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

6.2.7. Hranjenje zasebnega ključev v kriptografskem modulu

Zasebni ključi izdajatelja digitalnih potrdil oziroma izdajatelja varnih časovnih žigov so shranjeni v varnostnem kriptografskem modulu v šifrirani obliki in se nikdar ne pojavijo izven modula v nešifrirani obliki.

6.2.8. Postopek za aktiviranje zasebnega ključa

Zasebni ključ izdajatelja digitalnih potrdil oziroma izdajatelja varnih časovnih žigov se aktivira ob zagonu aplikativne programske opreme. Za aktiviranje je potrebno predložiti operatersko pametno kartico varnostnega kriptografskega modula ter geslo administratorja izdajatelja.

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

6.2.9. Postopek za deaktiviranje zasebnega ključa

Zasebni ključ izdajatelja digitalnih potrdil oziroma izdajatelja varnih časovnih žigov se deaktivira 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 digitalnih potrdil 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

Zasebne ključe izdajateljev digitalnih potrdil oziroma izdajateljev varnih časovnih žigov je obvezno uničiti, ko jim poteče obdobje uporabe, oziroma se ne uporabljajo več iz drugih razlogov. Ob uničenju ključev je potrebno uničiti aktivno kopijo na varnostnem kriptografskem modulu in vse varnostne kopije.

6.2.11.Stopnja varnosti kriptografskih modulov

Opisano v poglavju 6.2.1 Standardi za kriptografske modul.

6.3. Ostali vidiki upravljanja s pari ključev

6.3.1. Arhiviranje javnega ključa

Izdajatelj arhivira svoj javni ključ za preverjanje podpisa in imetniške javne ključe v povezavi z digitalnimi potrdili za preverjanje podpisa kot del arhiviranja digitalnih potrdil kot predpisano v poglavju 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 digitalnih potrdil oziroma javnih in zasebnih ključev je določena v pravilih delovanja posameznega izdajatelja.

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 že določeno pri izdajatelju, ga izdajatelj dostavi imetniku na varen način.

6.4.3. Druge zahteve za gesla

Zahteve glede dolžine in kompleksnosti gesla določi izdajatelj v svojih pravilih delovanja.

6.5. Varnostne zahteve za računalnike

6.5.1. Specifične tehnične varnostne zahteve za računalnike

Izdajatelj 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 vseh varnostno relevantnih dogodkov,
- varen arhiv informacijskega sistema izdajatelja, kopij ključev imetnikov in varnostnih beležk, ter
- mehanizme restavriranja informacijskega sistema, ključev ter baze podatkov izdajatelja.

6.5.2. Raven varnostne zaščite računalnikov

Ni predpisano.

6.6. Tehnični nadzor življenjskega cikla izdajatelja

6.6.1. Nadzor razvoja sistema

Strojna oprema, operacijski sistem in programska oprema izdajateljev so komercialni proizvodi.

6.6.2. Upravljanje varnosti

Izdajatelj mora evidentirati postopke inštalacije, sprememb konfiguracije in nadgradnje za vse svoje informacijske in komunikacijske komponente.

Programska oprema izdajatelja 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, oziroma upravljanje varnosti skozi celoten življenjski cikel, morajo biti v skladu z 6.6.2 Upravljanje varnosti.

6.7. Varnostne kontrole na ravni računalniškega omrežja

Korenski izdajatelj ni povezan v nobeno računalniško omrežje.

Komunikacijsko informacijski sistemi posameznega izdajatelja delujejo v izoliranih omrežjih, ki so z drugimi omrežji KIS MO in SV povezani preko varnostnih pregrad. Varnostna pravila na varnostnih pregradah dovoljujejo prehod samo protokolom, potrebnim za dostop do storitev izdajateljev.

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

Izdajatelji SIMoD-PKI izdajajo digitalna potrdila X.509 verzije 3 v skladu s priporočilom [17] RFC 5280, ki vsebujejo naslednja osnovna polja:

Ime osnovnega polja	Slovenski prevod ali opis	Vrednost
Version	verzija potrdila X.509	*v3*
Serial Number	enolična serijska številka	enolična serijska številka
Signature Algorithm	algoritem za podpis potrdila	*sha256WithRSAEncryption*
Issuer	izdajatelj	razločevalno ime izdajatelja
Validity	veljavnost potrdila	*Not Before*: začetek veljavnosti *Not After*: konec veljavnosti
Subject	imetnik	Razločevalno ime 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 [17] RFC 5280, uporabljena v digitalnih potrdilih izdajateljev SIMoD-PKI:

Ime standardnega razširitvenega polja		Slovenski prevod ali opis	Vrednost
Authority Key Identifier		identifikator javnega ključa izdajatelja	SHA256 odtis javnega ključa izdajatelja
Subject Key Identifier		identifikator imetnikovega javnega ključa	SHA256 odtis javnega ključa imetnika
Key Usage		namen uporabe ključa	določeno v 6.1.7 Namen uporabe ključev
Extended Key Usage		razširjen namen uporabe ključa	določeno v 6.1.7 Namen uporabe ključev
Private Key Usage Period		veljavnost zasebnega ključa	*Not Before*: začetek veljavnosti *Not After*: konec veljavnosti
Certificate Policies:		oznaka politike potrdila	
	Policy Identifier	enolična oznaka politike	Skladno s 1.2. Identifikacijske oznake politik delovanja in 7.1.6 Identifikacijske oznake politik
	Policy Qualifier	identifikator politike	*[1,1]Policy Qualifier Info:* *Policy Qualifier Id=CPS* *Qualifier:* *http:/www.simod-pki.mors.si/*
CRL Distribution Points		objave registra preklicanih potrdil	določeno v pravilih delovanja izdajatelja
Subject Alternative Name		alternativno ime imetnika	določeno v pravilih delovanja izdajatelja
Basic Constraints		osnovne omejitve	določeno v pravilih delovanja izdajatelja

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.

Polja *certificatePolicies*, *keyUsage* in *extKeyUsage* so označena kot kritična.

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

Izdajatelji lahko uporabljajo dodatna standardna in lastna razširitvena polja.

7.1.3. Identifikacijske oznake algoritmov

Identifikacijski oznaki kriptografskih algoritmov, uporabljenih 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 poglavju 3.1.2 Potreba po smiselnosti imen.

Uporaba in način uporabe polja *nameConstraints* nista predpisana.

7.1.6. Identifikacijske oznake politik

Digitalno potrdilo vsebuje v polju *certificatePolicies* identifikacijsko oznako politike, ki je določena v pravilih delovanja izdajatelja.

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

7.1.7. Način uporabe razširitvenega polja za omejitev uporabe politik

Ni predpisano.

7.1.8. Specifični podatki o politiki

Razširitveno polje za specifične podatke o politiki *certificatePolicies, policyQualifier* se obravnava v skladu z [17] RFC 5280.

7.1.9. Procesiranje oznake kritičnosti razširitvenih polj

Uporabniške aplikacije morajo procesirati razširitvena polja, označena kot kritična, v skladu s priporočili [17] RFC 5280.

7.2. Profil registrov preklicanih potrdil

7.2.1. Verzija registrov preklicanih potrdil

Izdajatelji SIMoD-PKI izdajajo registre preklicanih potrdil verzije 2 v skladu s priporočilom [17] RFC 5280, ki vsebujejo naslednja osnovna polja:

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

7.2.2. Razširitvena polja registrov preklicanih potrdil

Izdajatelji SIMoD-PKI izdajajo registre preklicanih potrdil verzije 2 v skladu s priporočilom [17] RFC 5280, ki vsebujejo naslednja standardna razširitvena polja:

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

Izdajatelji lahko v registrih preklicanih potrdil uporabljajo dodatna standardna in lastna razširitvena polja.

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 [18] RFC 6960.

7.3.2. Razširitve sprotnega preverjanja statusa digitalnih potrdil

Razširitve storitve za sprotno preverjanje statusa digitalnih potrdil so predpisane v pravilih delovanja izdajatelja SIMoD-PKI.

8. PREVERJANJE SKLADNOSTI IN OSTALE OBLIKE NADZORA

8.1. Pogostost inšpekcije

Pogostost inšpekcijskega nadzora je določena z veljavno zakonodajo.

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

8.2. Pogoji za inšpektorja

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

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

8.3. Relacija med inšpektorjem in izdajatelji SIMoD-PKI

Inšpektor mora biti neodvisen od infrastrukture javnih ključev na MO.

8.4. Področja inšpekcije

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

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

8.5. Postopki po opravljeni inšpekciji

V primeru ugotovljenih nepravilnosti mora izdajatelj 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 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 do naslednje predvidene inšpekcije ali
- pred preklicem izdajateljevega digitalnega potrdila dodeli izdajatelju rok za odpravo pomanjkljivosti, v tem času dovoli izdajatelju delovanje ali
- odredi preklic izdajateljevega digitalnega potrdila.

8.6. Prejemniki ugotovitev o inšpekciji

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

Izdajatelj 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.

Način in podrobnosti izmenjave ugotovitev o inšpekciji med medsebojno priznanimi izdajatelji so določeni v pogodbi o medsebojnem priznavanju.

9. OSTALE POSLOVNE IN PRAVNE ZADEVE

9.1. Cenik

9.1.1. Cena prve in ponovne izdaje digitalnega potrdila

Ni predpisano.

9.1.2. Cena dostopa do digitalnega potrdila

Ni predpisano.

9.1.3. Cena dostopa do podatka o statusu in preklicu potrdila

Ni predpisano.

9.1.4. Cene drugih storitev

Ni predpisano.

9.1.5. Povračilo stroškov

Ni predpisano.

9.2. Finančna odgovornost

9.2.1. Višina zavarovanja

Ministrstvo za obrambo ima 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

Izdajatelji pridobijo 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

Izdajatelj jamči, da upravlja z digitalnimi potrdili v skladu s Politiko SIMoD-PKI in svojimi pravili delovanja. Svet za upravljanje z infrastrukturo javnih ključev na MO predstavlja izdajatelje SIMoD-PKI in jamči za izpolnjevanje njihovih obveznosti.

9.6.2. Odgovornost in jamstva prijavne službe

Prijavna služba je odgovorna za skladnost identifikacijskih postopkov s Politiko SIMoD-PKI in 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 pravili delovanja izdajatelja pred podpisom zahtevka za izdajo digitalnega potrdila,
- ravna v skladu s Politiko SIMoD-PKI, pravili delovanja izdajatelja in ostalimi pravnimi akti,
- spremlja obvestila izdajateljev SIMoD-PKI in ravna v skladu z njimi,
- je prijavni službi ali operativnemu osebju izdajatelja, ki upravlja z digitalnimi potrdili, 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 tretjih oseb

Tretja oseba, ki se zanaša na digitalna potrdila izdajatelja SIMoD-PKI, jamči, da uporablja digitalna potrdila le za namene, določene v Politiki SIMoD-PKI in pravilih delovanja izdajatelja, ki je izdal digitalno potrdilo 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

Overitelj na MO ni odgovoren za škodo (direktno ali posredno), izgube, stroške ter terjatve, ki izhajajo iz ali so nastale zaradi uporabe digitalnih potrdil in z njimi povezanih ključev, če:

- je bilo digitalno potrdilo izdano kot rezultat napake ali neverodostojnosti podatkov v zahtevku,
- je bilo digitalno potrdilo spremenjeno 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 ali morebitni drugi pogodbi,
- imetnik ali tretja oseba ni postopala v skladu s predpisanimi postopki v Politiki SIMoD-PKI, pravili delovanja izdajatelja ali morebitni drugi pogodbi in obvestili izdajatelja ali

- je nastala škoda zaradi napake v delovanju strojne ali programske opreme imetnika ali tretje osebe,
- je do ravnanja v nasprotju s Politiko SIMoD-PKI ali ostalimi dokumenti prišlo zaradi višje sile, to je izredne nepredvidljive okoliščine, na katero udeleženci infrastrukture javnih ključev na MO ne morejo vplivati (na primer naravne nesreče, teroristična dejanja…).

9.8. Omejitve odgovornosti

Overitelj na MO 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 izdajatelji SIMoD-PKI ne prevzemajo 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 Politika SIMoD-PKI se objavi na spletnih straneh http://www.simod-pki.mors.si.

Določbe Politike SIMoD-PKI za nekvalificirana digitalna potrdila začnejo veljati in se uporabljati naslednji dan po podpisu.

Določbe Politike SIMoD-PKI 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 Politike SIMoD-PKI ni časovno omejena. Politika SIMoD-PKI velja do uveljavitve nove verzije.

9.10.3.Posledice prenehanja veljavnosti

Po prenehanju veljavnosti Politike SIMoD-PKI zaradi objave nove verzije imetniki praviloma uporabljajo obstoječa digitalna potrdila v skladu z določili Politike SIMoD-PKI in pravili delovanja izdajatelja, po kateri so bila izdana. V primeru, da to ni mogoče, izdajatelj ob izdaji nove verzije Politike SIMoD-PKI in posledično novih pravilih delovanja izdajatelja obvesti imetnike.

9.11. Obvestila in komuniciranje z udeleženci

Obvestila udeležencem infrastrukture javnih ključev na MO so objavljena 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 pripravi spremembe Politike SIMoD-PKI in jih predlaga ministru v sprejem.

9.12.2.Postopek in roki obveščanja

Spremembe Politike SIMoD-PKI 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 Politike SIMoD-PKI.

9.12.3.Spremembe, ki zahtevajo novo identifikacijsko oznako politike

Izdajatelj po lastni presoji odloči, ali so spremembe Politike SIMoD-PKI takšne, da zahtevajo objavo novih pravil delovanja in spremembo identifikacijskih oznak politik izdajatelja.

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

Izdajatelji SIMoD-PKI delujejo 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] RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

[17] RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[18] 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:

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

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

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

9.16. Razne določbe

Ni raznih določb.

9.17. Ostale določbe

Ni ostalih določb.