REPUBLIKA SLOVENIJA
MINISTRSTVO ZA OBRAMBO

Politika SIMoD-PKI

Verzija 3.1

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 3.1	• Ukinitev Sveta za upravljanje z infrastrukturo javnih ključev; • uskladitev izrazov; nadomestitev izrazov »overitelj« in »infrastruktura javnih ključev« z izrazom »ponudnik storitev zaupanja«; • uredniški popravki.
Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, verzija 3.0, številka 386-12/2017-37, 3. maj 2017	• 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 priporočil ETSI; • uskladitev izrazov; konsistentna uporaba izrazov »overitelj« in »izdajatelj«; • ukinjena omejitev ponovne izdaje digitalnih potrdil brez preverjanja istovetnosti največ dvakrat zaporedoma.
Pravila o spremembah pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, verzija 2.0, številka 386-11/2014-20, 7. februar 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, 14. november 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 drugačni 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, 8. september 2011	• Odstranjene so vrednosti parametrov v povezavi z digitalnimi potrdili (dolžine in obdobje veljavnosti ključev); • 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, 24. avgust 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 s področnim nacionalnim zakonom 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, če 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 protokola PKCS#10 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, 27. december 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, 17. julij 2006	Vpeljan je hierarhični model infrastrukture javnih ključev.
Pravila overitelja digitalnih potrdil na Ministrstvu za obrambo Republike Slovenije – javni del notranjih pravil, šifra 471-01-6/2002-47, 29. julij 2005	

KAZALO

1 UVOD

1.1 Pregled

Ministrstvo za obrambo (v nadaljevanju: MO) upravlja infrastrukturo javnih ključev na MO (ang. Slovenian Ministry of Defence Public Key Infrastructure – SIMoD-PKI) za potrebe obrambe države.

SIMoD-PKI zagotavlja sredstva elektronske identifikacije in je ponudnik storitev zaupanja, kot je opredeljeno v [1] eIDAS za potrebe obrambe države.

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

Ta dokument imenujemo tudi politika SIMoD-PKI.

Politika SIMoD-PKI določa 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 izdajatelji SIMoD-PKI.

Politika SIMoD-PKI določa postopek izdajanja in upravljanja digitalnih potrdil za zagotavljanje naslednjih varnostnih storitev:

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

Digitalna potrdila se med seboj ločijo glede na stopnjo zaupanja v digitalno potrdilo in namen uporabe.

Politika SIMoD-PKI zagotavlja, da so digitalna potrdila skladna z nacionalno zakonodajo, [1] eIDAS in standardi ETSI ter drugimi veljavnimi predpisi in priporočili.

Podrobnosti o svojem delovanju posamezni izdajatelji določijo v svojih pravilih delovanja.

1.2 Identifikacijske oznake politik delovanja

Identifikacijske oznake politik delovanja izdajateljev SIMoD-PKI (ang. Policy Object Identifiers – Policy OIDs) se določijo po 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 preverjanje istovetnosti v prijavni službi (p2)	1	DA
	2	NE
Uporaba sredstva za varno hrambo zasebnih ključev in ustvarjanje elektronskega podpisa (p3)	1	DA
	2	NE
Imetnik digitalnega potrdila (p4)	1	fizična oseba
	3	splošni naziv; organizacijska enota ali organ v sestavi MO, funkcijska ali organizacijska vloga
	4	strežnik in druga strojna ter programska oprema
	5	izdajatelj časovnih žigov
	6	sistem 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 odzivov sprotnega preverjanja veljavnosti potrdil
Verzija (p6)	zaporedna številka izdaje politike	

Izdajatelji označijo, pod katero politiko izdajajo digitalna potrdila, v razširitvenem polju C*ertificate Policies,* kot je določeno v podpoglavju 7.1.2 Razširitvena polja.

Kvalificirana digitalna potrdila, skladna s [5] ETSI EN 319 411-2, morajo v razširitvenem polju *Certificate Policies* vsebovati tudi oznako skladnosti s politiko za kvalificirana potrdila EU.

1.3 Udeleženci infrastrukture javnih ključev

1.3.1 Ponudnik storitev zaupanja

Ponudnik storitev zaupanja na MO združuje korenskega izdajatelja in podrejene izdajatelje digitalnih potrdil.

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

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

Kontaktni podatki ponudnika storitev zaupanja na MO so:

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

1.3.2 Prijavna služba

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

1.3.3 Imetniki digitalnih potrdil

Imetniki digitalnih potrdil so:

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

Odgovorna oseba za digitalno potrdilo glede na imetnika potrdila je:

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

1.3.4 Tretje osebe

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

1.3.5 Posredno odgovorni organi

Izdajatelji delujejo v KIS MO skladno s pravnimi akti MO za KIS MO. Posredno odgovorne za delovanje SIMoD-PKI so tudi organizacijske enote MO, ki so pristojne za varovanje in nadzor KIS MO.

1.4 Namen uporabe digitalnih potrdil

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

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

Digitalna potrdila oziroma javni in zasebni ključi omogočajo implementacijo varnostnih storitev preverjanja istovetnosti, celovitosti in nezanikanja z varnostnim mehanizmom digitalnega podpisa, tajnost in selektivno omejevanje dostopa pa z mehanizmi izmenjave ključev kot podporo simetričnim šifrirnim algoritmom.

Digitalno potrdilo nedvoumno povezuje imetnika digitalnega potrdila z njegovim javnim ključem. Celovitost in varnost te povezave je ocenjena s stopnjo zaupanja v digitalno potrdilo. 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 oziroma ustvarjanje elektronskega podpisa v strojni obliki	DA	NE	NE
Stopnja zaupanja:	VISOKA	SREDNJA	NIZKA

1.4.1 Dovoljena uporaba digitalnih potrdil

Digitalna potrdila izdajateljev SIMoD-PKI se morajo uporabljati v skladu s politiko SIMoD-PKI in pravili delovanja izdajatelja. Namenjena so službeni uporabi na MO.

V nadaljevanju so smernice za uporabo digitalnih potrdil različnih stopenj zaupanja.

Uporaba digitalnih potrdil VISOKE in SREDNJE stopnje zaupanja zagotavlja:

- celovitost, preverjanje istovetnosti in nezanikanje za podatke vseh stopenj tajnosti,
- tajnost podatkov do vključno stopnje tajnosti INTERNO,
- selektivno omejevanje dostopa do podatkov do vključno stopnje tajnosti TAJNO,
- upravljanje varnostnih parametrov in šifrirnih ključev, daljinski nadzor ter preverjanje istovetnosti naprav v KIS (usmerjevalnikov, šifrirnih naprav).

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

Uporaba digitalnih potrdil NIZKE stopnje zaupanja zagotavlja:

- celovitost, preverjanje istovetnosti, nezanikanje, tajnost in selektivno omejevanje dostopa za podatke brez stopnje tajnosti (npr. spletni dostop po protokolu SSL),
- zagotavljanje tajnosti podatkov stopnje tajnosti INTERNO ob prenosu, če se nezaščiteni KIS uporablja le kot prenosni medij, npr. podatki stopnje tajnosti INTERNO se prenašajo prek javnega omrežja Internet,
- upravljanje varnostnih parametrov in šifrirnih ključev, daljinski nadzor ter preverjanje istovetnosti naprav v KIS (usmerjevalnikov, šifrirnih naprav), ob pogoju, da so naprave fizično varovane, da je možnost zlorabe digitalnih potrdil majhna.

1.4.2 Nedovoljena uporaba digitalnih potrdil

Ni določb.

1.5 Upravljanje politike SIMoD-PKI

1.5.1 Organ, ki upravlja ta dokument

Organizacijska enota, pristojne za informatiko, vodi postopek izdelave politike SIMoD-PKI.

Spremembe in dopolnitve oziroma novo politiko SIMoD-PKI sprejme minister.

1.5.2 Kontaktni podatki

Glej podpoglavje 1.3.1 Ponudnik storitev zaupanja.

1.5.3 Organ za odobritev skladnosti pravil delovanja izdajatelja s politiko SIMoD-PKI

Odgovorni organ za odobritev skladnosti pravil delovanja izdajatelja SIMoD-PKI s to politiko je kolegij organizacijske enote, pristojne za informatiko.

1.5.4 Postopek odobritve pravil delovanja izdajatelja

Kolegij organizacijske enote, pristojne za informatiko:

- preveri skladnost pravil delovanja izdajatelja SIMoD-PKI s to politiko,
- sprejme pravila delovanja izdajatelja SIMoD-PKI.

1.6 Pojmi in kratice

Pojem	Definicija
Časovni žig	Podatki v elektronski obliki, ki druge podatke v elektronski obliki povezujejo z določenim trenutkom in tako zagotavljajo dokaz, da so slednji podatki v tistem trenutku obstajali.
Digitalno potrdilo	Potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z imetnikom potrdila.
Digitalno potrdilo izdajatelja časovnih žigov	Digitalno potrdilo, s katerim izdajatelj časovnih žigov izdaja časovne žige.
Digitalno potrdilo za preverjanje podpisa	Digitalno potrdilo, ki se uporablja za verifikacijo digitalnega podpisa in preverjanje celovitosti podatkov v elektronski obliki. V tem dokumentu uporabljen kot enakovreden izraz za »potrdilo za elektronski podpis ali žig« po [1] eIDAS.
Digitalno potrdilo za šifriranje	Digitalno potrdilo, ki se uporablja za izmenjavo simetričnih šifrirnih ključev pri zagotavljanju tajnosti podatkov v elektronski obliki.

Elektronski podpis	Niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika.
Elektronski žig	Niz podatkov v elektronski obliki, ki so dodani k drugim podatkom v elektronski obliki ali so z njimi logično povezani, da se zagotovita izvor in celovitost povezanih podatkov.
Imenik	Podatkovna struktura, ki vsebuje objekte z določenimi lastnosti in pripadajočimi vrednostmi. Imenik, ki vsebuje digitalna potrdila, je navadno v skladu s standardom X.500 oz. razširjenim standardom X.509 ver.3.
Imetnik potrdila	Fizična oseba, navedena v digitalnem potrdilu v polju *Subject*. Lastnik zasebnega ključa, ki ustreza javnemu ključu, vsebovanem v digitalnem potrdilu, oziroma odgovorna oseba za uporabo digitalnega potrdila.
Infrastruktura javnih ključev	Pravila, postopki, vloge in informacijski sistem za implementacijo varnostnih storitev na podlagi kriptografije javnih ključev oziroma za upravljanje digitalnih potrdil.
Izdajatelj	Izdajatelj digitalnih potrdil, ki deluje v okviru ponudnika storitev zaupanja.
Kvalificirano digitalno potrdilo	V tem dokumentu izraz za kvalificirano potrdilo za elektronski podpis ali elektronski žig. Potrdilo, ki ga izda ponudnik kvalificiranih storitev zaupanja in izpolnjuje zahteve iz Priloge I oziroma Priloge III [1] eIDAS.
Naprava	V tem dokumentu izraz za strežnik, drugo strojno ali programsko opremo, izdajatelja časovnih žigov, sistem za preverjanje veljavnosti digitalnih potrdil ali druga storitev overjanja
Naprava za ustvarjanje elektronskega podpisa	Po definiciji dvaindvajsetega odstavka 3. člena [1] eIDAS konfigurirana programska in strojna oprema, ki se uporablja za ustvarjanje elektronskega podpisa.
Naprava za ustvarjanje kvalificiranega elektronskega podpisa	Po definiciji triindvajsetega odstavka 3. člena [1] eIDAS naprava za ustvarjanje elektronskega podpisa, ki izpolnjuje zahteve iz Priloge II [1] eIDAS.
Politika digitalnih potrdil	Pravila, ki posledično definirajo uporabnost digitalnih potrdil v določeni skupini uporabnikov in/ali za določene aplikacije s skupnimi varnostnimi zahtevami.
Ponudnik storitev zaupanja	Po definiciji devetnajstega odstavka 3. člena [1] eIDAS fizična ali pravna oseba, ki zagotavlja eno ali več storitev zaupanja.
Potrdilo za elektronski podpis	Po definiciji 14. odstavka 3. člena [1] eIDAS elektronsko potrdilo, ki povezuje podatke za potrjevanje veljavnosti elektronskega podpisa s fizično osebo in potrjuje vsaj ime ali psevdonim te osebe. V tem dokumentu se namesto izraza »potrdilo za elektronski podpis« uporablja izraz »digitalno potrdilo«.
Prijavna služba	Služba oziroma organizacija, ki po pooblastilu izdajatelja sprejema zahtevke in preverja istovetnosti bodočih imetnikov.
Razločevalno ime	Oblika zapisa podatkov o imetniku digitalnega potrdila. Razločevalno ime se pripravlja v skladu s priporočilom IETF RFC 5280 in standardom X.501 (ang. Distinguished Name).
Sredstvo za elektronsko podpisovanje	Nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje elektronskega podpisa.
Storitev zaupanja	Elektronska storitev po definiciji šestnajstega odstavka 3. člena [1] eIDAS: a) ustvarjanje, preverjanje in potrjevanje veljavnosti elektronskih podpisov, elektronskih žigov ali elektronskih časovnih žigov, storitev elektronske priporočene dostave in potrdil, povezanih s temi storitvami; b) ustvarjanje, preverjanje in potrjevanje veljavnosti potrdil za avtentikacijo spletišč ali c) hramba elektronskih podpisov, žigov ali potrdil, povezanih s temi storitvami.
Tretja oseba	Subjekt, ki ni dejavno udeležen v storitvi, vendar zaupa izvajalcu in rezultatu storitve.

Uporabnik	Naročnik ali imetnik digitalnega potrdila
Zloraba	Razkritje tajnega podatka, izguba celovitosti ali razpoložljivosti podatka

Kratica	Opis
CN	Splošno ime objekta v imeniku (ang. Common Name)
CRL	Register preklicanih potrdil (ang. Certificate Revocation List)
eIDAS	Uredba (EU) št. 910/2014 Evropskega parlamenta ter Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES
ETSI	Evropski inštitut za standardizacijo na področju telekomunikacij, izdaja serijo standardov s področja elektronskega podpisa in delovanja ponudnikov storitev zaupanja (ang. European Telecommunications Standards Institute).
HTTP	Protokol za prenos podatkov v spletnem okolju (ang. Hypertext Transfer Protocol)
LDAP	Protokol, ki določa dostop do imenika in je specificiran po priporočilu IETF (ang. Internet Engineering Task Force) RFC 1777 (ang. Leightweight Directory Access Protocol).
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#10	Sintaksa zahtevka za digitalno potrdilo. Zahtevek za digitalno potrdilo vsebuje razločevalno ime, javni ključ in druge atribute.
PKCS#7	Sintaksa za kriptografsko obdelane podatke, kot so elektronski podpisi in ovojnice.
PKI	Infrastruktura javnih ključev; strojna in programska oprema ter varnostni mehanizmi za zaupanja vredno implementacijo varnostnih storitev, ki temeljijo na nesimetrični kriptografiji (ang. Public Key Infrastructure).
PKIX	Delovna skupina za infrastrukturo javnih ključev v okviru IETF, ki je izdala serijo priporočil za digitalna potrdila in registre preklicanih potrdil (ang. Public Key Infrastrukture X.509).
PKIX- CMP	Postopek izmenjave podatkov, ki se nanašajo na digitalna potrdila med subjekti infrastrukture izdajatelja (ang. PKIX Certificate Management Protocol). Vključuje PKCS#7 in PKCS#10.
QCP	Oznaka politike ETSI za kvalificirana potrdila (ang. Qualified Certificate Policy); [5] ETSI EN 319 411-2
QSCD	Naprava za ustvarjanje kvalificiranega elektronskega podpisa (ang. Qualified Signature/Seal Creation Device); [5] ETSI EN 319 411-2
RFC 5280	Priporočilo, ki določa elemente potrdil in registra preklicanih potrdil.
RFC 3647	Priporočilo, ki določa elemente, ki naj bodo v politiki infrastrukture javnih ključev (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.
SIMoD-PKI	Infrastruktura javnih ključev Ministrstva za obrambo (ang. Slovenian Ministry of Defence Public Key Infrastructure – SIMoD-PKI)
X.509	Standard organizacij ITU-T in ISO, ki definira strukturo digitalnih potrdil, eden izmed serije standardov ITU-ISO iz imenikov in 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:

- imeniku na naslovu imenik.simod-pki.mors.si,
- 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,
- digitalna potrdila izdajateljev,
- registri preklicih potrdil,
- navodila za varno uporabo digitalnih potrdil, zahtevki za pridobitev in preklic digitalnih potrdil ter druge javne objave izdajateljev.

Izdajatelji v imeniku objavljajo naslednje podatke:

- digitalna potrdila imetnikov,
- registre preklicanih potrdil.

Podrobnejše določbe in tehnične lastnosti glede objav so opredeljene v pravilih delovanja posameznega izdajatelja.

2.3 Čas in pogostost objav

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

2.4 Dostop do podatkov v repozitorijih

Vpogled v podatke v repozitorijih je brez omejitev.

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

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 v skladu s priporočili [13] RFC 5280, [8] ETSI EN 319 412-2, [9] ETSI EN 319 412-3 ter [10] ETSI EN 319 412-4.

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

3.1.2 Potreba po smiselnosti imen

Splošno ime v digitalnem potrdilu mora nedvoumno označevati imetnika.

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

Ni posebnih določil.

3.1.5 Edinstvenost imen

Razločevalno ime v digitalnem potrdilu mora enolično določati imetnika.

3.1.6 Priznavanje, preverjanje in vloga registriranih znamk

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

3.2 Preverjanje istovetnosti imetnikov ob prvi registraciji

3.2.1 Metode dokazovanja lastništva zasebnega ključa

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

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

3.2.2 Preverjanje istovetnosti za imetnike, ki niso fizične osebe

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

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

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

Za pravilnost podatkov na zahtevkih jamči vodja organizacijske enote MO.

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

Za digitalna potrdila NIZKE stopnje zaupanja preverjanje podatkov in osebna identifikacija nista obvezna. Zahtevke prejme in obdela operativno osebje izdajatelja.

3.2.3 Preverjanje istovetnosti za fizične osebe

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

Za pravilnost podatkov na zahtevku jamči vodja organizacijske enote MO.

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

Za digitalna potrdila NIZKE stopnje zaupanja preverjanje podatkov in osebna identifikacija nista obvezna. Zahtevke prejme in obdela operativno osebje izdajatelja.

3.2.4 Podatki o naročniku, ki se ne preverjajo

Prijavna služba ne preverja naslednjih podatkov:

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

Za pravilnost zgoraj navedenih podatkov jamči vodja organizacijske enote MO.

3.2.5 Preverjanje pooblastil

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

3.2.6 Merila za medsebojno povezovanje

Način in pogoji medsebojnega povezovanja z drugimi ponudniki storitev zaupanja bodo določeni dogovorno.

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 veljavnega zasebnega ključa.

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

3.3.2 Preverjanje istovetnosti za ponovno izdajo digitalnega potrdila po preklicu

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

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.

4 UPRAVLJANJE DIGITALNIH POTRDIL

4.1 Pridobitev digitalnega potrdila

4.1.1 Kdo lahko zaprosi za izdajo digitalnega potrdila

Zahtevek za pridobitev digitalnega potrdila za fizične osebe oddajo zaposleni na MO, za splošne nazive za organizacijske enote MO predstojniki organizacijske enote najmanj na ravni vodje sektorja, za splošne nazive za funkcijske ali organizacijske vloge nosilci, skrbniki ali administratorji vloge, za naprave in storitve pa skrbniki naprave oziroma storitve.

4.1.2 Postopek za pridobitev digitalnega potrdila in odgovornosti

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

Bodoči imetnik odda zahtevek za pridobitev digitalnega potrdila SREDNJE in VISOKE stopnje zaupanja v prijavno službo. Podrobnejše določbe so opredeljene v pravilih delovanja izdajatelja.

Bodoči imetnik odda zahtevek za izdajo digitalnega potrdila NIZKE stopnje zaupanja operativnemu osebju izdajatelja.

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 ter istovetnost bodočega imetnika v skladu s podpoglavjema 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 bodočega imetnika ne preverja.

4.2.2 Odobritev ali zavrnitev izdaje digitalnega potrdila

Zahtevek za pridobitev digitalnega potrdila izdajatelja ne obvezuje k izdaji digitalnega potrdila.

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

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

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

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

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

4.2.3 Čas za obdelavo zahtevka za izdajo digitalnega potrdila

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

4.3 Izdaja digitalnega potrdila

4.3.1 Postopki izdajatelja ob izdaji potrdil

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

Operativno osebje izdajatelja začne postopke 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, praviloma referenčno številko po elektronski pošti, avtorizacijsko kodo pa v kuverti po pošti.

Za digitalna potrdila z obvezno uporabo pametne kartice, če izdajatelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, 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 varno dostavi imetniku.

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

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

4.4 Prevzem digitalnega potrdila

4.4.1 Postopek prevzema digitalnega potrdila

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

Veljavnost aktivacijskih podatkov je 60 dni od izdaje.

Izdajatelji morajo v svojih pravilih delovanja opisati postopek prevzema oziroma objaviti uporabniška navodila za prevzem digitalnih potrdil.

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

Ob prevzemu digitalnega potrdila mora imetnik preveriti vsebino digitalnega potrdila, ali je digitalno potrdilo podpisal pravi izdajatelj in polno pot digitalnih podpisov do korenskega izdajatelja. S prvo uporabo oziroma če imetnik osem dni od prevzema digitalnega potrdila izdajatelja ne obvesti o morebitnih napakah, velja, da je imetnik potrdil točnost podatkov v digitalnem potrdilu in da prevzema vse obveznosti in jamstva iz podpoglavja 9.6.3 Odgovornost in jamstva imetnikov digitalnih potrdil.

4.4.2 Objava digitalnega potrdila

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

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

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

4.5.1 Uporaba ključev in digitalnih potrdil imetnikov

Imetnik digitalnega potrdila mora:

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

4.5.2 Uporaba digitalnih potrdil tretjih oseb

Tretja oseba mora:

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

4.6 Ponovna izdaja digitalnega potrdila brez spremembe javnega ključa

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

4.7 Ponovna izdaja digitalnih potrdil

Ponovna izdaja digitalnega potrdila za preverjanje digitalnega podpisa in digitalnega potrdila za preverjanje digitalnega podpisa ter šifriranje pomeni generiranje novega para ključev in novega digitalnega potrdila.

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

4.7.1 Razlogi za ponovno izdajo digitalnega potrdila

Ponovna izdaja digitalnega potrdila se opravi:

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

4.7.2 Kdo lahko zahteva ponovno izdajo digitalnega potrdila

Za ponovno izdajo digitalnega potrdila lahko zaprosijo imetniki oziroma subjekti iz podpoglavja 4.1.1 Kdo lahko zaprosi za izdajo digitalnega potrdila.

4.7.3 Obdelava zahtevkov za ponovno izdajo digitalnega potrdila

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

V pravilih 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 lahko izvede na podlagi ustreznega elektronskega zahtevka, ki je podpisan z veljavnim digitalnim potrdilom.

Ponovna izdaja digitalnih potrdil pred pretekom veljavnosti se za digitalna potrdila, izdana po protokolu PKIX-CMP, opravi samodejno ob uporabi digitalnega potrdila z neposrednim dostopom do izdajatelja v določenem obdobju pred pretekom veljavnosti zasebnega ključa.

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

4.7.4 Obvestilo imetniku o izdaji novega digitalnega potrdila

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

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

4.7.5 Postopek potrditve prevzema novega digitalnega potrdila

Enako kot je v podpoglavju 4.4.1 Postopek prevzema digitalnega potrdila.

4.7.6 Objava novega digitalnega potrdila

Enako kot je v podpoglavju 4.4.2 Objava digitalnega potrdila.

4.7.7 Obveščanje drugih udeležencev o izdaji digitalnega potrdila

Enako kot je v podpoglavju 4.4.3 Obveščanje drugih udeležencev o izdaji digitalnega potrdila.

4.8 Sprememba digitalnega potrdila

Sprememba podatkov v digitalnem potrdilu ni mogoča. Ob spremembah podatkov v digitalnem potrdilu je treba digitalno potrdilo preklicati.

4.9 Začasna ukinitev veljavnosti in preklic digitalnega potrdila

4.9.1 Okoliščine preklica

Razlogi za preklic digitalnih potrdil imetnikov so:

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

4.9.2 Kdo lahko zahteva preklic

Zahtevo za preklic digitalnega potrdila imetnika lahko poda:

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

4.9.3 Postopki za preklic

Zahtevki za preklic se lahko posredujejo:

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

Operativno osebje izdajatelja izvede preklic in o preklicu obvesti imetnika.

Po preklicu mora izdajatelj objaviti preklicano digitalno potrdilo v registru preklicanih potrdil.

4.9.4 Čas za posredovanje zahtevka za preklic

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

4.9.5 Čas od prejema zahtevka za preklic do preklica

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

- sumu zlorabe zasebnih ključev ali
- neizpolnjevanju obveznosti iz politike SIMoD-PKI ali pravil delovanja izdajatelja.

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

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

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

4.9.6 Obveza preverjanja registra preklicanih potrdil

Tretje osebe, ki se zanašajo na digitalno potrdilo, morajo pred uporabo preveriti najnovejši register preklicanih potrdil. V postopku preverjanja je treba preveriti tudi veljavnost in verodostojnost registra preklicanih potrdil. Tretja oseba mora za vsako uporabljeno digitalno potrdilo opraviti popoln postopek preverjanja poti zaupanja v skladu s [13] RFC 5280.

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

4.9.7 Pogostost objav registrov preklicanih potrdil

Izdajatelji imetniških digitalnih potrdil morajo objaviti nov register preklicanih potrdil:

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

Izdajatelj objavi pogostost objav registrov preklicanih potrdil v svojih pravilih delovanja.

4.9.8 Dovoljene zakasnitve pri objavi registrov preklicanih potrdil

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

Izdajatelji morajo izdati nov register preklicanih potrdil pred iztekom veljavnosti starega.

4.9.9 Sprotno preverjanje statusa digitalnih potrdil

Podprt je protokol za sprotno preverjanje statusa digitalnih potrdil (ang. On-line Certificate Status Protocol – OCSP) v skladu s priporočilom [14] RFC 6960.

4.9.10 Obveza sprotnega preverjanja statusa preklicanih potrdil

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

4.9.11 Druge oblike objavljanja preklicanih digitalnih potrdil

Niso podprte.

4.9.12 Posebne zahteve glede zlorabe ključa

Niso predpisane.

4.9.13 Okoliščine za začasno ukinitev veljavnosti

Niso podprte.

4.9.14 Kdo lahko zahteva začasno ukinitev veljavnosti

Ni podprto.

4.9.15 Postopki za začasno ukinitev veljavnosti

Niso podprti.

4.9.16 Omejitve obdobja začasne ukinitve veljavnosti

Niso podprte.

4.10 Preverjanje statusa digitalnih potrdil

4.10.1 Tehnične lastnosti storitve

Lokacije in tehnične lastnosti registrov preklicanih potrdil ter storitve sprotnega preverjanja statusa digitalnih potrdil so navedene v pravilih delovanja izdajatelja.

4.10.2 Razpoložljivost storitve

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

4.10.3 Dodatne možnosti

Niso določene.

4.11 Predčasna prekinitev veljavnosti digitalnih potrdil

Predčasno se prekine veljavnost digitalnega potrdila iz naslednjih razlogov:

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

4.12 Varnostno kopiranje in odkrivanje zasebnega ključa

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

Dovoljeni so varnostno kopiranje (Key Backup) in posledično povrnitev zgodovine ključev (Key Recovery) ter odkrivanje ključev le 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 mogoče.

4.12.1 Povrnitev zgodovine ključev za dešifriranje

Izdajatelji morajo v svojih pravilih delovanja navesti, za katera digitalna potrdila sta omogočeni storitvi varnostnega kopiranja in povrnitve zgodovine ključev za dešifriranje.

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

4.12.2 Odkrivanje kopije ključev za dešifriranje

Odkrivanje kopije ključev za dešifriranje drugim osebam, kot je imetnik povezanih digitalnih potrdil za šifriranje, ni omogočeno. Aplikacije in informacijske rešitve MO morajo šifrirati službene podatke tako, da so selektivno dostopni vsem osebam, ki so pooblaščene za dostop do teh podatkov.

5 FIZIČNO VAROVANJE, ORGANIZACIJSKI VARNOSTNI UKREPI IN ZAHTEVE ZA OSEBJE

5.1 Fizično varovanje

5.1.1 Lokacija in konstrukcija prostorov

Izdajatelji delujejo v varovanih prostorih in na varnih lokacijah na MO.

5.1.2 Fizični dostop

Fizični dostop nadzira pristojna služba MO.

Nadzor fizičnega dostopa se izvaja z uporabo tehničnih sredstev, ki preprečujejo nepooblaščen vstop. Vstop je dovoljen le operativnemu osebju izdajatelja. Druge osebe, ki izkažejo upravičen interes, smejo vstopiti v prostore le 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,
- klimatsko napravo za nadzor temperature in vlage.

5.1.4 Zaščita pred poplavo

Prostori s komunikacijsko in informacijsko opremo izdajateljev so na lokaciji, kjer je verjetnost poplave majhna.

5.1.5 Zaščita pred ognjem

Prostori s komunikacijsko in informacijsko opremo izdajateljev 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.

5.1.8 Hranjenje na oddaljeni lokaciji

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

5.2 Organizacijski varnostni ukrepi

5.2.1 Organizacija upravljanja ponudnika storitev zaupanja na MO

Operativno osebje je za upravljanje posameznega izdajatelja razdeljeno v zaključene organizacijske skupine za:

- upravljanje digitalnih potrdil,
- upravljanje programske in strojne opreme izdajatelja,
- varovanje in nadzor komunikacijskega sistema ponudnika storitev na MO.

Posamezna oseba lahko opravlja naloge za več izdajateljev, pri čemer je pri vsakem izdajatelju lahko član le ene organizacijske skupine.

V organizacijski skupini za upravljanje digitalnih potrdil so:

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

V organizacijski skupini za upravljanje programske in strojne opreme izdajatelja so:

- prvi administrator izdajatelja,
- administratorji izdajatelja.

V organizacijski skupini za varovanje in nadzor komunikacijskega sistema so:

- prvi administrator komunikacijskega sistema,
- administratorji komunikacijskega sistema.

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

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

5.2.2 Število oseb za izvedbo postopkov

V skupini za upravljanje digitalnih potrdil izdajatelja morajo biti najmanj tri osebe, v skupini za upravljanje programske in strojne opreme izdajatelja najmanj dve osebi, v skupini za varovanje in nadzor komunikacijskega sistema pa najmanj dve 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 ter vstopno kodo,
- za delo na izdajateljevem informacijskem sistemu s prijavnim imenom in geslom,
- za upravljanje digitalnih potrdil z digitalnim potrdilom.

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

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

5.3 Zahteve za osebje

5.3.1 Kvalifikacije, izkušnje in varnostno preverjanje

Operativno osebje izdajatelja:

- mora biti ustrezno usposobljeno,
- ne sme opravljati nalog, ki bi bile v nasprotju z opravljanjem nalog pri ponudniku storitev zaupanja na MO.

5.3.2 Dovoljenja za dostop do tajnih podatkov

Morajo biti v skladu s [16] ZTP.

5.3.3 Usposabljanje osebja

Operativno osebje izdajateljev mora biti usposobljeno na naslednjih področjih:

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

Osebje prijavne službe mora biti usposobljeno za:

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

5.3.4 Pogostost dodatnih usposabljanj

Osebje se dodatno usposablja glede na izkazane potrebe oziroma novosti v povezavi s ponudnikom storitev zaupanja na MO.

5.3.5 Kroženje med delovnimi mesti

Ni določeno.

5.3.6 Ukrepi ob kršitvah pooblastil

Proti operativni osebi izdajatelja, ki ne opravlja svojih nalog ali zlorabi svoja pooblastila, se ukrepa v skladu s predpisi.

5.3.7 Zunanji izvajalci

Zunanji izvajalci morajo izpolnjevati vse pogoje, določene v [16] ZTP, in varnostne zahteve izdajateljev.

5.3.8 Dokumentacija za operativno osebje

Operativnemu osebju izdajateljev 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 morajo beležiti naslednje dogodke:

- na operacijskem sistemu, programski in strojni opremi izdajatelja ter elementov komunikacijskega sistema,
- glede ključev izdajatelja,
- glede imetniških ključev in digitalnih potrdil,
- glede varnostne politike in upravljanja svojega informacijsko-komunikacijskega sistema.

Izdajatelji morajo beležiti tudi podatke, ki vplivajo na varnost, niso pa del komunikacijsko-informacijskega sistema izdajatelja:

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

5.4.2 Pogostost pregleda dnevnikov beleženih dogodkov

Operativno osebje izdajateljev uporablja nadzorne sisteme za spremljanje stanja sistemov in sprotno obveščanje o dogodkih. Ob vsakem opozorilu iz nadzornih sistemov operativno osebje pregleda dnevnike beleženih dogodkov.

5.4.3 Obdobje hranjenja dnevnikov beleženih dogodkov

Najmanj sedem let v arhivu.

5.4.4 Zaščita dnevnikov beleženih dogodkov

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

Dostop do dnevnikov beleženih dogodkov je dovoljen le:

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

5.4.5 Varnostne kopije dnevnikov beleženih dogodkov

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

Pogostost varnostnega kopiranja sistemov je določena v pravilih delovanja izdajatelja.

Periodično, kot je določeno v pravilih delovanja izdajatelja, se en izvod varnostne kopije prenese na oddaljeno lokacijo.

5.4.6 Način zbiranja beleženih dogodkov

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

5.4.7 Obveščanje povzročitelja dogodka

Povzročitelja dogodka o dogodku ni treba obvestiti.

5.4.8 Ocena in odprava ranljivosti

Dnevnike beleženih dogodkov pregleduje operativno osebje izdajatelja zaradi odkrivanja in odprave ranljivosti. Ugotovljena ranljivost se oceni s stališča verjetnosti povzročitve škode in predvidijo se ukrepi za zmanjšanje grožnje.

5.5 Arhiviranje podatkov

5.5.1 Vrste arhiviranih podatkov

Izdajatelji morajo hraniti naslednje podatke:

- dnevnike beleženih dogodkov iz poglavja 5.4.1 Vrste beleženih dogodkov,
- zahtevke za pridobitev in preklic digitalnih potrdil,
- korespondenco imetnikov z izdajateljem,
- dokumentacijo o izvedbi identifikacije naročnikov digitalnih potrdil,
- digitalna potrdila in liste preklicanih potrdil,
- politiko SIMoD-PKI in svoja pravila delovanja,
- zasebne ključe za dešifriranje.

5.5.2 Obdobje hranjenja arhiva

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

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

5.5.3 Zaščita arhiva

Zahtevke za pridobitev in preklic digitalnih potrdil, dokumentacijo o izvedbi identifikacije, korespondenco imetnikov digitalnih potrdil z izdajatelji, politiko SIMoD-PKI, pravila delovanja izdajateljev in dnevnike beleženih dogodkov v pisni obliki, je treba hraniti in arhivirati v skladu s internimi splošnimi pravnimi akti, ki urejajo delo z dokumentarnim gradivom na MO.

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

5.5.4 Varnostna kopija arhiva

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

Ob vzpostavitvi arhiva podatkov, ki se beležijo v okviru informacijskega sistema, se ustvari varnostna kopija.

5.5.5 Časovno žigosanje zapisov

Ni določeno.

5.5.6 Način arhiviranja

Ni določen.

5.5.7 Postopek vpogleda v arhiv in njegova verifikacija

Dostop do arhiva je dovoljen le:

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

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

5.6 Zamenjava ključev izdajateljev

Veljavnost izdajateljevega digitalnega potrdila je daljša, kot je veljavnost katerega koli digitalnega potrdila imetnika, podpisanega s pripadajočim zasebnim ključem.

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

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

Ponovna izdaja digitalnega potrdila izdajatelja poteka po predpisanem in nadzorovanem postopku. Postopek izvede operativno osebje izdajatelja. Izvedba postopka je dokumentirana v zapisniku.

5.7 Okrevalni načrt

5.7.1 Postopki ob okvarah in zlorabah

Postopki ob okvarah in zlorabah so del okrevalnega načrta, ki se določi v pravilih delovanja izdajatelja.

5.7.2 Uničenje programske ali strojne opreme oziroma podatkov izdajatelja

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

Ob okvari, pri kateri pride do uničenja izdajateljevega zasebnega ključa in vseh njegovih kopij, se ravna v skladu s podpoglavjem 5.8 Prenehanje delovanja izdajatelja.

5.7.3 Zloraba zasebnega ključa izdajatelja

Ob zlorabi zasebnega ključa izdajatelja, ki zahteva preklic digitalnega potrdila izdajatelja, je potrebno postopati skladno s podpoglavjem 5.8 Prenehanje delovanja izdajatelja.

5.7.4 Zagotavljanje kontinuitete delovanja po nesrečah

Postopki ob naravnih in drugih nesrečah, ki imajo za posledico fizično uničenje ali varnostno vprašljivo delovanje programske ali strojne opreme, ogroženo celovitost podatkov izdajatelja oziroma uničenje in poškodovanje varovanih prostorov izdajatelja, se določijo v pravilih delovanja izdajatelja.

5.8 Prenehanje delovanja izdajatelja

Razlogi za prenehanje delovanja izdajatelja oziroma preklic digitalnega potrdila izdajatelja so:

- domnevna ali dejanska zloraba zasebnega ključa,
- nezmožnost pravočasne ponovne vzpostavitve delovanja po okvari oziroma uničenju,
- sklep predstojnika organizacijske enote, pristojne za informatiko, o prenehanju delovanja izdajatelja,
- sklep ministra o prenehanju delovanja ponudnika storitev zaupanja na MO,
- druge okoliščine, ki lahko ogrozijo zaupanje v digitalno potrdilo izdajatelja.

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

Izdajatelj mora ob preklicu svojega digitalnega potrdila opraviti naslednje postopke:

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

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

6 TEHNIČNE VARNOSTNE ZAHTEVE

6.1 Generiranje in namestitev para ključev

6.1.1 Generiranje para ključev

Generiranje para ključev izdajatelja opravi operativno osebje izdajatelja. Izvedba postopka je dokumentirana v zapisniku. Generiranje para ključev vedno poteka znotraj varnostnega kriptografskega modula.

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

Za digitalna potrdila z obvezno uporabo pametne kartice, če izdajatelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, se zasebni ključ za podpisovanje oziroma za oba namena uporabe, in sicer 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

Ko bodoči imetnik sam generira ključe, kot je to pri ključih za podpisovanje, ni potrebe po prenašanju zasebnih ključev. Zasebni ključ za podpisovanje se mora generirati pri imetniku oziroma mora biti vedno pod nadzorom imetnika. Izdajatelj v nobenem trenutku ne poseduje in ne hrani kopije zasebnih ključev za podpisovanje.

Ko izdajatelj generira zasebne ključe, kot je to pri dešifrirnih ključih 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, če izdajatelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, generira ključe izdajatelj. Izdajatelj varno dostavi zasebni ključ imetniku skupaj s pametno kartico z digitalnim potrdilom.

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.

Za digitalna potrdila z obvezno uporabo pametne kartice, če izdajatelj ne more jamčiti, da bo bodoči imetnik zanesljivo generiral in hranil ključe na pametni kartici, generira imetniške ključe in digitalno potrdilo izdajatelj. Izdajatelj v postopku zapiše na pametno kartico tudi javni ključ izdajatelja oziroma izdajateljevo digitalno potrdilo.

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

6.1.5 Dolžina ključev

Dolžine zasebnih ključev se določijo v pravilih delovanja posameznega izdajatelja.

6.1.6 Parametri za generiranje javnih ključev in preverjanje parametrov

Izdajatelji in imetniki morajo uporabljati opremo za generiranje ključev, ki ustreza uveljavljenim varnostnim ter tehničnim standardom.

Parametri za generiranje javnih ključev in postopki preverjanja teh parametrov morajo biti skladni z najnovejšimi priporočili kriptografije.

Izdajatelji morajo v svojih pravilih delovanja navesti podatke o uporabljenih kriptografskih parametrih in standardih.

6.1.7 Namen uporabe ključev

Namen uporabe ključev je določen v dveh razširitvenih poljih *Key Usage* in *Extended Key Usage* po priporočilu [13] RFC 5280.

6.2 Zaščita zasebnih ključev in zahteve za kriptografske module

6.2.1 Standardi za kriptografske module

Izdajatelji 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 zasebnega ključa izdajatelja oziroma varnostnega kriptografskega modula je nujna prisotnost vsaj dveh oseb z ustreznimi pooblastili, ki izkažeta svojo istovetnost s pametno kartico s porazdeljenim ključem kriptografskega modula in geslom kartice.

6.2.3 Odkrivanje zasebnega ključa

Odkrivanje zasebnega ključa izdajateljev ni dovoljeno. Tehnična izvedba varnostnega kriptografskega modula ne omogoča prikaza zasebnega ključa izdajatelja v nešifrirani obliki.

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

6.2.4 Varnostno kopiranje zasebnih ključev

Varnostna kopija zasebnega ključa izdajatelja se zagotavlja z mehanizmi varnostnega kriptografskega modula. Datoteka z zasebnim ključem oziroma varnostna kopija se pred izvozom iz varnostnega kriptografskega modula šifrira. Dešifrirni ključ je porazdeljen na administratorskih pametnih karticah N (N mora biti večji ali enak 2) od M (M mora biti večji ali enak 3).

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

6.2.5 Arhiviranje zasebnega ključa

Izdajateljev zasebni ključ se ne arhivira.

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

6.2.6 Zapis zasebnega ključa v kriptografski modul in iz njega

Zasebni ključ izdajatelja se generira v varnostnem kriptografskem modulu.

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

Zasebni ključi za podpisovanje se pri digitalnih potrdilih VISOKE stopnje varnosti generirajo na pametni kartici.

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

Zasebni ključi za dešifriranje se pri digitalnih potrdilih, za katera izdajatelj zagotavlja storitev povrnitve zgodovine, generirajo v izdajateljevem kriptografskem modulu in se prenesejo k bodočemu imetniku z uporabo protokola PKIX-CMP.

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

6.2.7 Hranjenje zasebnega ključa v kriptografskem modulu

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

6.2.8 Postopek za aktiviranje zasebnega ključa

Zasebni ključ izdajatelja se aktivira ob zagonu aplikativne programske opreme. Za aktiviranje je treba predložiti operatersko pametno kartico varnostnega kriptografskega modula in geslo administratorja izdajatelja.

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

6.2.9 Postopek za deaktiviranje zasebnega ključa

Zasebni ključ izdajatelja se deaktivira z ustavitvijo aplikativne programske opreme.

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

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

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

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

6.2.10 Postopek za uničenje zasebnega ključa

Zasebne ključe izdajateljev je treba uničiti, ko jim poteče obdobje uporabe oziroma se ne uporabljajo več iz drugih razlogov. Ob uničenju ključev je treba uničiti aktivno kopijo na varnostnem kriptografskem modulu in vse šifrirane datoteke z zasebnim ključem.

6.2.11 Stopnja varnosti kriptografskih modulov

Stopnja varnosti je določena v podpoglavju 6.2.1 Standardi za kriptografske modul.

6.3 Drugi vidiki upravljanja para 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 je predpisano v podpoglavju 5.5 Arhiviranje podatkov. Javni ključi v povezavi s šifrirnimi digitalnimi potrdili se ne arhivirajo.

6.3.2 Obdobje veljavnosti ključev in digitalnih potrdil

Veljavnost digitalnih potrdil oziroma javnih in zasebnih ključev se določi v pravilih delovanja 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 med inicializacijo varnostnega kriptografskega modula.

Imetniki pametnih kartic ali drugih varnih nosilcev digitalnih potrdil morajo imeti nadzor nad geslom za aktiviranje pametne kartice oziroma nosilca. Imeti morajo možnost določitve gesla med inicializacijo pametne kartice ali nosilca oziroma morajo v primeru predhodno nastavljenih gesel imeti možnost geslo spremeniti.

Za dostop do zasebnih ključev, ki se hranijo v programski obliki (npr. Microsoft Cryptographic Store), morajo uporabniki uporabljati visoko stopnjo zaščite. 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 tako, da se zagotavlja njihova tajnost. Če je bilo geslo za dostop do pametne kartice določeno pri izdajatelju, ga izdajatelj varno dostavi imetniku.

6.4.3 Druge zahteve za gesla

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

6.5 Varnostne zahteve za računalniško opremo izdajateljev

6.5.1 Specifične tehnične varnostne zahteve

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

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

6.5.2 Raven varnostne zaščite računalnikov

Elementi informacijskega sistema izdajateljev morajo dosegati raven varnostne zaščite v skladu z uveljavljenimi varnostnimi in tehničnimi priporočili.

Tehnične zahteve in varnostne nastavitve morajo biti v skladu z varnostno politiko za KIS MO.

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 namestitve, sprememb konfiguracije in nadgradnje za vse svoje informacijske in komunikacijske komponente.

Programska oprema izdajatelja je zaščitena tako, da se lahko preverita njen izvor in celovitost.

6.6.3 Upravljanje varnosti med življenjskim ciklom

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

6.7 Varnostni nadzor 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 povezani prek varnostnih pregrad. Varnostna pravila na varnostnih pregradah dovoljujejo prehod le protokolom za dostop do storitev izdajateljev.

Redno se izvajajo vdorni testi oziroma pregledi ranljivosti.

6.8 Časovno žigosanje

Ni določeno.

7 PROFIL DIGITALNIH POTRDIL IN REGISTROV PREKLICANIH POTRDIL

7.1 Profil digitalnih potrdil

7.1.1 Verzija digitalnih potrdil

Izdajatelji SIMoD-PKI izdajajo digitalna potrdila v skladu s priporočilom [13] RFC 5280.

7.1.2 Razširitvena polja

Izdajatelji SIMoD-PKI v svojih digitalnih potrdilih uporabljajo razširitvena polja po priporočilu [13] RFC 5280.

Kvalificirana digitalna potrdila, skladna s [5] ETSI EN 319 411-2, morajo vsebovati dodatno razširitveno polje *qcStatement* z izjavo, da ustrezajo profilu kvalificiranih potrdil po priporočilu v [11] ETSI EN 319 412-5.

Izdajatelji lahko uporabljajo dodatna standardna in svoja razširitvena polja.

7.1.3 Identifikacijske oznake algoritmov

Izdajatelji v pravilih delovanja navedejo identifikacijske oznake kriptografskih algoritmov, uporabljenih v digitalnih potrdilih.

7.1.4 Oblike imen

So določene v podpoglavju 3.1.1 Oblika imen.

7.1.5 Omejitve imen

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

7.1.6 Identifikacijske oznake politik

Digitalno potrdilo vsebuje v polju *Certificate Policies* identifikacijsko oznako politike skladno s podpoglavjem 1.2. Identifikacijske oznake politik delovanja oziroma kot je določena v pravilih delovanja izdajatelja.

Kvalificirano digitalno potrdilo ima skladno s priporočilom [5] ETSI EN 319 411-2 poleg oznake politike, določene s pravili delovanja izdajatelja, še vrednost, ki ga označuje kot kvalificirano digitalno potrdilo EU.

7.1.7 Način uporabe razširitvenega polja za omejitev uporabe politik

Ni predpisan.

7.1.8 Posebni podatki o politiki

Razširitveno polje za posebne podatke o politiki *Certificate Policies, Policy Qualifier* se obravnava v skladu s priporočili [13] RFC 5280.

7.1.9 Procesiranje oznake kritičnosti razširitvenih polj

Uporabniške aplikacije morajo procesirati razširitvena polja, označena kot kritična, v skladu s priporočili [13] RFC 5280.

7.2 Profil registrov preklicanih potrdil

7.2.1 Verzija registrov preklicanih potrdil

Izdajatelji izdajajo registre preklicanih potrdil v skladu s priporočilom [13] RFC 5280.

7.2.2 Razširitveni polji registrov preklicanih potrdil

Izdajatelji v svojih registrih preklicanih potrdil uporabljajo razširitvena polja po priporočilu [13] RFC 5280.

Izdajatelji lahko v registrih preklicanih potrdil uporabljajo dodatna standardna in svoja 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 [14] RFC 6960.

7.3.2 Razširitve sprotnega preverjanja statusa digitalnih potrdil

Razširitve storitve za sprotno preverjanje statusa digitalnih potrdil se določijo v pravilih delovanja izdajatelja.

8 PREVERJANJE SKLADNOSTI IN DRUGE OBLIKE NADZORA

8.1 Pogostost preverjanja skladnosti

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

8.2 Pogoji za izvajalca preverjanja skladnosti

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

8.3 Neodvisnost izvajalca preverjanja skladnosti

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

8.4 Področja preverjanja skladnosti

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

8.5 Postopki po opravljenem pregledu skladnosti

Postopki po opravljeni presoji skladnosti so v skladu s predpisi.

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

8.6 Prejemniki ugotovitev o pregledu skladnosti

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

9 DRUGE POSLOVNE IN PRAVNE ZADEVE

9.1 Cenik

Ni določeno.

9.2 Finančna odgovornost

Skladno s predpisi.

9.3 Zaupnost poslovnih informacij

Skladno s predpisi.

9.4 Zaupnost osebnih podatkov

Skladno s predpisi.

9.5 Zaščita intelektualne lastnine

Skladno s predpisi.

9.6 Odgovornosti in jamstva

9.6.1 Odgovornosti in jamstva izdajatelja

Izdajatelj jamči, da upravlja digitalna potrdila v skladu s politiko SIMoD-PKI in svojimi pravili delovanja.

9.6.2 Odgovornost in jamstva prijavne službe

Prijavna služba je odgovorna za skladnost identifikacijskih postopkov s politiko SIMoD-PKI.

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 drugimi pravnimi akti,
- spremlja obvestila izdajateljev in ravna v skladu z njimi,
- je prijavni službi ali operativnemu osebju izdajatelja posredoval popolne in točne podatke,
- se strinja z javno objavo svojega digitalnega potrdila.

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

9.6.4 Odgovornost in jamstva tretjih oseb

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

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

9.6.5 Odgovornost in jamstva drugih udeležencev

Ni predpisano.

9.7 Zanikanje odgovornosti

Ponudnik storitev zaupanja na MO ni odgovoren za škodo, ki izhaja iz uporabe digitalnih potrdil in z njimi povezanih ključev, če:

- je bilo digitalno potrdilo izdano kot rezultat napake ali neverodostojnosti podatkov v zahtevku,
- je bilo digitalno potrdilo spremenjeno,
- je bilo digitalno potrdilo uporabljeno po preteku veljavnosti,
- je bilo digitalno potrdilo uporabljeno po preklicu in objavi v registru preklicanih potrdil,
- je bil zasebni ključ zlorabljen ali obstaja sum, da je bil zlorabljen,
- je bilo digitalno potrdilo uporabljeno za drugačne namene, kot je dovoljeno s politiko SIMoD-PKI ali pravili delovanja izdajatelja,
- imetnik ali tretja oseba ni ravnala v skladu s predpisanimi postopki v politiki SIMoD-PKI, pravilih delovanja izdajatelja,
- je nastala škoda zaradi napake v delovanju strojne ali programske opreme,
- je do ravnanja v nasprotju s politiko SIMoD-PKI ali pravili delovanja izdajatelja prišlo zaradi višje sile.

9.8 Omejitve odgovornosti

Skladno s predpisi.

9.9 Poravnava škode

Skladno s predpisi.

9.10 Začetek in prenehanje veljavnosti

9.10.1 Začetek veljavnosti

Nova verzija politike SIMoD-PKI se objavi na spletni strani http://www.simod-pki.mors.si.

Določbe politike SIMoD-PKI začnejo veljati in se uporabljati naslednji dan po podpisu.

9.10.2 Prenehanje veljavnosti

Veljavnost politike SIMoD-PKI ni časovno omejena oziroma 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 katerih so bila izdana.

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

Organizacijska enota, pristojna za informatiko, pripravi spremembe politike SIMoD-PKI in jih predlaga ministru v sprejem.

9.12.2 Postopek in roki obveščanja

Spremembe politike SIMoD-PKI je treba objaviti v skladu s poglavjem 9.11 Obvestila in komuniciranje z udeleženci.

9.12.3 Spremembe, ki zahtevajo novo identifikacijsko oznako politike

Izdajatelj odloči, ali so spremembe politike SIMoD-PKI take, da zahtevajo objavo novih pravil delovanja in spremembo identifikacijskih oznak politik izdajatelja.

9.13 Reševanje sporov

V skladu s predpisi.

9.14 Predpisi in priporočila

Izdajatelji SIMoD-PKI delujejo v skladu s predpisi in priporočili:

[1]	eIDAS	Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (Uradni list EU, št. L 257/83 z dne 28. avgusta 2014)
[2]	ETSI ES 319 401	Electronic Signatures and Infrastructures (ESI); General Policy requirements for Trust Service Providers
[3]	ETSI EN 319 411	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Provider issuing certificates
[4]	ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Provider issuing certificates, Part 1: General requirements
[5]	ETSI EN 319 411-2	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
[6]	ETSI EN 319 412	Electronic Signatures and Infrastructures (ESI); Certificate Profiles
[7]	ETSI EN 319 412-1	Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

[8] ETSI EN 319 412-2 — Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

[9] ETSI EN 319 412-3 — Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

[10] ETSI EN 319 412-4 — Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

[11] ETSI EN 319 412-5 — Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

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

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

[14] RFC 6960 — X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OSCP

[15] ZObr — Zakon o obrambi (Uradni list RS, št. 103/04 – UPB1, 95/15 in 139/20)

[16] ZTP — Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – UPB2, 9/10, 60/11 in 8/20)

[17] ZVOP-1 — Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – UPB1, 177/20)