Državni center za storitve zaupanja
Korenski izdajatelj digitalnih potrdil za podrejene in povezane izdajatelje kvalificiranih digitalnih potrdil
SI-TRUST Root

SI-TRUST
SI-TRUST Root

POLITIKA SI-TRUST Root za korenskega izdajatelja digitalnih potrdil za podrejene in povezane izdajatelje kvalificiranih digitalnih potrdil

Javni del notranjih pravil Državnega centra za storitve zaupanja

veljavnost: od 23. maja 2016
verzija: 1.0

CP_{Name}: SI-TRUST Root
CP_{OID}: 1.3.6.1.4.1.6105.6.1.1

Zgodovina politik

Izdaje politik delovanja SI-TRUST Root
verzija: 1.0, veljavnost: od 23. maja 2016
Politika SI-TRUST Root za korenskega izdajatelja digitalnih potrdil za podrejene in povezane izdajatelje kvalificiranih digitalnih potrdil - CP_{OID}: 1.3.6.1.4.1.6105.6.1.1 - CP_{Name}: SI-TRUST Root

VSEBINA

POVZETEK

Politike za digitalna potrdila in varne časovne žige predstavljajo celoten javni del notranjih pravil Državnega centra za storitve zaupanja, ki deluje v okviru Ministrstva za javno upravo (v nadaljevanju *overitelj na MJU*) in določajo namen, delovanje in metodologijo upravljanja s kvalificiranimi in normaliziranimi digitalnimi potrdili, dodeljevanje časovnih žigov, odgovornost overitelja na MJU ter zahteve, ki jih morajo izpolnjevati uporabniki in tretje osebe, ki uporabljajo in se zanašajo na kvalificirana digitalna potrdila in na varne časovne žige, in drugi overitelji, ki želijo uporabljati storitve overitelja na MJU.

Overitelj na MJU izdaja kvalificirana digitalna potrdila ter varne časovne žige, za katera velja najvišja stopnja varovanja ter deluje v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14) in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06), Uredbo (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), evropskimi direktivami in standardi ETSI ter drugimi veljavnimi predpisi in priporočili.

Overitelj na MJU izdaja tudi normalizirana digitalna potrdila ter digitalna potrdila za posebne namene oz. zaprte sisteme. Pravila delovanja izdajateljev takih potrdil se določijo s politiko delovanja takega izdajatelja.

Normalizirana digitalna potrdila, ki jih izdaja overitelj na MJU, so namenjena:
- izdajateljem potrdil, izdajateljem časovnih žigov, strežnikom oz. informacijskim sistemom, sistemom OCSP, podpisovanju programske kode in registra preklicanih potrdil ter v ostalih primerih, kjer ni možna uporaba kvalificiranih potrdil,
- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba teh potrdil in
- za storitve oz. aplikacije, za katere se zahteva uporaba teh potrdil.

Kvalificirana digitalna potrdila, ki jih izdaja overitelj na MJU, so namenjena:
- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba teh potrdil,
- za varno elektronsko komuniciranje med imetniki potrdil in
- za storitve oz. aplikacije, za katere se zahteva uporaba teh potrdil.

Varni časovni žigi overitelja na MJU so namenjeni:
- zagotavljanju obstoja dokumenta v določenem časovnem trenutku in sicer tako, da se poveže datum in čas žigosanja z vsebino dokumenta na kriptografsko varen način,
- povsod, kjer je potrebno na varen način dokazati časovne lastnosti transakcij in drugih storitev,
- za druge potrebe, kjer se potrebuje varni časovni žig.

Znotraj overitelja na MJU deluje korenski izdajatelj digitalnih potrdil SI-TRUST Root (angl. *Slovenian Trust Service Root Certification Authority*), v nadaljevanju *korenski izdajatelj SI-TRUST Root* ali kratko *SI-TRUST Root*. SI-TRUST Root izdaja potrdila v dveh obsegih, znotraj Overitelja na MJU kot korenski izdajatelj, pri povezovanju z zunanjimi izdajatelji pa kot premostitveni izdajatelj.

Politika delovanja SI-TRUST Root določa notranja pravila delovanja korenskega izdajatelja, ki definirajo namen, delovanje in metodologijo upravljanja z digitalnimi potrdili, odgovornosti in zahteve, ki jih morajo izpolnjevati vsi subjekti.

1. UVOD

1.1. Pregled

(1) V okviru Ministrstva za javno upravo (v nadaljevanju *MJU*) deluje Državni center za storitve zaupanja (v nadaljevanju *overitelj na MJU*).

(2) Politike overitelja predstavljajo celoten javni del notranjih pravil overitelja na MJU in določajo namen, delovanje in metodologijo upravljanja s kvalificiranimi in normaliziranimi digitalnimi potrdili, dodeljevanje časovnih žigov, odgovornost overitelja na MJU ter zahteve, ki jih morajo izpolnjevati imetniki, uporabniki in tretje osebe, ki se zanašajo na kvalificirana in normalizirana digitalna potrdila ter na varne časovne žige, in drugi overitelji, ki želijo uporabljati storitve overitelja na MJU.

(3) Overitelj na MJU izdaja kvalificirana digitalna potrdila in varne časovne žige, za katera velja najvišja stopnja varovanja ter deluje v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14) in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06), Uredbo (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), evropskimi direktivami in standardi ETSI ter drugimi veljavnimi predpisi in priporočili.

(4) Overitelj na MJU izdaja tudi normalizirana digitalna potrdila ter digitalna potrdila za posebne namene oz. zaprte sisteme. Pravila delovanja izdajateljev takih potrdil se določijo s politiko delovanja takega izdajatelja.

(5) Normalizirana digitalna potrdila, ki jih izdaja overitelj na MJU, so namenjena:
- izdajateljem potrdil, izdajateljem časovnih žigov, strežnikom oz. informacijskim sistemom, sistemom OCSP, podpisovanju programske kode in registra preklicanih potrdil ter v ostalih primerih, kjer ni možna uporaba kvalificiranih potrdil,
- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba teh potrdil in
- za storitve oz. aplikacije, za katere se zahteva uporaba teh potrdil.

(6) Kvalificirana digitalna potrdila, ki jih izdaja overitelj na MJU, so namenjena:
- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba teh potrdil,
- za varno elektronsko komuniciranje med imetniki potrdil in
- za storitve oz. aplikacije, za katere se zahteva uporaba teh potrdil.

(7) Varni časovni žigi overitelja na MJU so namenjeni:
- zagotavljanju obstoja dokumenta v določenem časovnem trenutku in sicer tako, da se poveže datum in čas žigosanja z vsebino dokumenta na kriptografsko varen način,
- povsod, kjer je potrebno na varen način dokazati časovne lastnosti transakcij in drugih storitev,
- za druge potrebe, kjer se potrebuje varni časovni žig.

(8) Znotraj overitelja na MJU deluje korenski izdajatelj digitalnih potrdil SI-TRUST Root (angl. *Slovenian Trust Service Root Certification Authority*), v nadaljevanju *korenski izdajatelj SI-TRUST Root* ali kratko *SI-TRUST Root*. SI-TRUST Root izdaja potrdila v dveh obsegih, znotraj Overitelja na MJU kot korenski izdajatelj, pri povezovanju z zunanjimi izdajatelji pa kot premostitveni izdajatelj.

(9) Imetniki digitalnih potrdil, ki jih izdaja korenski izdajatelj SI-TRUST Root, so izdajatelji kvalificiranih potrdil. Korenski izdajatelj SI-TRUST Root izdaja:
- izdajateljem v okviru Overitelja na MJU potrdila za podrejene izdajatelje in enostranska potrdila za povezane izdajatelje;

- pri povezovanju z ostalimi izdajatelji (v nadaljevanju *zunanji izdajatelji*) povezovalna potrdila, ki so praviloma dvostranska.

(10) Pričujoča politika je pripravljena v skladu s priporočili glede strukture dokumenta po RFC 3647 »Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework«, določa pa notranja pravila korenskega izdajatelja SI-TRUST Root, ki definirajo namen, delovanje in metodologijo upravljanja z digitalnimi potrdili, odgovornost overitelja na MJU ter zahteve, ki jih morajo izpolnjevati imetniki digitalnih potrdil korenskega izdajatelja, tretje osebe, ki se zanašajo na digitalna potrdila, in drugi subjekti, ki skladno s predpisi uporabljajo storitve korenskega izdajatelja.

(11) Medsebojna razmerja med subjekti po tej politiki so lahko urejena tudi z medsebojnim dogovorom ali pogodbo oz. na druge načine z morebitnimi drugimi predpisi.

(12) Korenski izdajatelj SI-TRUST Root s podrejenimi oz. povezanimi izdajatelji, ki delujejo znotraj državnih organov Republike Slovenije, sklene medsebojni dogovor, z ostalimi izdajatelji pa pogodbo.

1.2. Identifikacijski podatki politike delovanja

(1) Pričujoči dokument je Politika SI-TRUST Root korenskega izdajatelja digitalnih potrdil za podrejene in povezane izdajatelje kvalificiranih digitalnih potrdil (v nadaljevanju *politika SI-TRUST Root*).

(2) Identifikacijska oznaka dokumenta, s katerim je določena politika delovanja korenskega izdajatelja SI-TRUST Root, je: CP_{OID}: 1.3.6.1.4.1.6105.6.1.1, CP_{Name}: SI-TRUST Root.

(3) Digitalna potrdila, ki jih izdaja korenski izdajatelj SI-TRUST Root, ne vključujejo identifikacijske oznake iz prejšnje točke, vključujejo pa:
- v potrdilih, izdanih izdajateljem v okviru overitelja na MJU, identifikacijsko oznako politike 2.5.29.32.0 (»anyPolicy«).
- v potrdilih, izdanih zunanjim izdajateljem, nabor identifikacijskih oznak politik, ki se uporabljajo v potrdilih, izdanih njihovim končnim uporabnikom.

(4) Identifikacijske oznake politik delovanja za zunanje izdajatelje, povezane s SI-TRUST Root, so določene v medsebojnem dogovoru oz. pogodbi.

1.3. Udeleženci infrastrukture javnih ključev

1.3.1. Overitelj

(1) Državni center za storitve zaupanja izdaja digitalna potrdila in varne časovne žige, za katera velja najvišja stopnja varovanja ter deluje v skladu z veljavnimi predpisi in priporočili.

(2) Kontaktni podatki Državnega centra za storitve zaupanja so:

Naslov:	Republika Slovenija Državni center za storitve zaupanja Ministrstvo za javno upravo Tržaška cesta 21 1000 Ljubljana
Telefon:	01 4788 330
Spletna stran:	http://www.ca.gov.si

Oznaka:	State-institutions

(3) Naloge upravljanja Državnega centra za storitve zaupanja opravlja upravni odbor overitelja na MJU (glej podpogl. 5.2).

(4) V okviru overitelja na MJU deluje korenski izdajatelj SI-TRUST Root ter drugi izdajatelji potrdil.

(5) Kontaktni podatki korenskega izdajatelja SI-TRUST Root so:

Naslov:	SI-TRUST Root Državni center za storitve zaupanja Ministrstvo za javno upravo Tržaška cesta 21 1000 Ljubljana
E-pošta:	overitelj@gov.si
Telefon:	01 4788 330
Spletna stran:	http://www.ca.gov.si
Dežurna tel. številka za preklice (24 ur vse dni v letu):	01 4788 777

(6) Korenski izdajatelj SI-TRUST Root opravlja naslednje naloge:
- določa in objavlja svojo politiko delovanja,
- v okviru overitelja na MJU izdaja potrdila za podrejene izdajatelje in enostranska potrdila za povezane izdajatelje;
- pri povezovanju z zunanjimi izdajatelji izdaja povezovalna potrdila, ki so praviloma dvostranska,
- skrbi za javni imenik potrdil,
- objavlja register preklicanih potrdil,
- določa pravila delovanja za podrejene izdajatelje,
- določa pogoje za medsebojno povezovanje z drugimi izdajatelji,
- pripravlja navodila in priporočila za varno uporabo svojih storitev,
- skrbi za nemoteno delovanje svojih storitev v skladu s politiko in ostalimi predpisi in
- opravlja vse ostale storitve v skladu s to politiko, medsebojnimi dogovori z drugimi subjekti ter ostalimi veljavnimi predpisi.

(7) Korenski izdajatelj SI-TRUST Root je ob začetku svojega produkcijskega delovanja tvoril svoje lastno digitalno potrdilo, ki je namenjeno overjanju potrdil, ki jih je SI-TRUST Root izdal podrejenim in povezanim izdajateljem kvalificiranih digitalnih potrdil.

Potrdilo SI-TRUST Root vsebuje naslednje podatke[1]:

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. *Version*	3
Identifikacijska oznaka potrdila, angl. *Serial Number*	90AE 7776 0000 0000 571D D06F
Algoritem za podpis, angl. *Signature algorithm*	sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11)

[1] Pomen je podan v podpogl. 3.1 in 7.

Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Imetnik, angl. *Subject*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Pričetek veljavnosti, angl. *Validity: Not Before*	Apr 25 07:38:17 2016 GMT
Konec veljavnosti, angl. *Validity: Not After*	Dec 25 08:08:17 2037 GMT
Algoritem za javni ključ, angl. *Subject Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. *RSA Public Key*	*ključ dolžine 3072 bitov*
Razširitve X.509v3	
Uporaba ključa, OID 2.5.29.15, *angl. Key Usage*	Kritično (Critical) Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)
Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. Auth*ority Key Identifier*	4CA3 C368 5E08 0263
Identifikator imetnikovega ključa, OID 2.5.*29.14,* *angl. Subject Key Identifier*	4CA3 C368 5E08 0263
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA1*	3A49 79B4 0FA8 4148 8200 B582 FBEE B63A AB99 19AE
Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA256*	FAD5 4081 1AFA E0DC 767C DF65 72A0 88FA 3CE8 493D D82B 3B86 9A67 D10A AB4E 8124

1.3.2. Prijavna služba

(1) Ker SI-TRUST Root ne izdaja digitalnih potrdil končnim uporabnikom, SI-TRUST Root nima vzpostavljene prijavne službe za naloge v skladu z veljavno zakonodajo.

(2) Vse naloge prijavne službe, ki so v skladu z RFC 3647 potrebne za korenskega izdajatelja, opravijo pooblaščene osebe overitelja na MJU oz. upravni odbor overitelja na MJU[2].

(3) Potrebna dokazila in ostale zahteve v zvezi z izdajo digitalnih potrdil izdajateljem predpiše korenski izdajatelj SI-TRUST Root.

(4) Prijavne službe imetnikov morajo izpolnjevati zahteve veljavne zakonodaje in korenskega izdajatelja SI-TRUST Root, ki so določne v medsebojnem dogovoru oz. pogodbi.

(5) Odgovornost glede vzpostavitve in delovanja teh prijavnih služb je na strani posameznih izdajateljev.

1.3.3. Imetniki potrdil

[2] Pomen je podan v podpogl. 5.2.

(1) Imetniki digitalnih potrdil, ki jih izdaja korenski izdajatelj SI-TRUST Root, so izdajatelji kvalificiranih potrdil in ne končni uporabniki digitalnih potrdil.

(2) Korenski izdajatelj SI-TRUST Root izdaja digitalna potrdila za:
- podrejene izdajatelje kvalificiranih digitalnih potrdil in
- povezane izdajatelje kvalificiranih digitalnih potrdil.

(3) Korenski izdajatelj SI-TRUST Root izdaja:
- izdajateljem v okviru Overitelja na MJU potrdila za podrejene izdajatelje in enostranska potrdila za povezane izdajatelje;
- pri povezovanju z ostalimi izdajatelji (v nadaljevanju *zunanji izdajatelji*) povezovalna potrdila, ki so praviloma dvostranska.

(4) Korenski izdajatelj SI-TRUST Root s podrejenimi oz. povezanimi zunanjimi izdajatelji, ki delujejo znotraj državnih organov Republike Slovenije, sklene medsebojni dogovor, z ostalimi izdajatelji pa pogodbo. Medsebojni dogovor oz. pogodba natančneje opredeli odgovornosti in postopke.

1.3.4. Tretje osebe

(1) Tretje osebe so vsi končni uporabniki znotraj infrastrukture javnih ključev korenskega izdajatelja SI-TRUST Root in vse ostale osebe oz. subjekti, ki se zanašajo na izdana digitalna potrdila korenskega izdajatelja SI-TRUST Root.

(2) Tretje osebe se morajo ravnati po navodilih korenskega izdajatelja SI-TRUST Root in morajo vedno preveriti veljavnost potrdila z preverjanjem celotne verige zaupanja, namen uporabe potrdila, čas veljavnosti potrdila itd. Podrobnejše obveznosti in odgovornosti tretjih oseb so navedene v podpogl. 4.5.2 in 9.6.4.

(3) Med tretjo osebo in korenskim izdajateljem SI-TRUST Root oz. overiteljem na MJU se lahko sklene medsebojni pisni dogovor.

1.3.5. Ostali udeleženci

Niso predvideni.

1.4. Namen uporabe potrdil

(1) Digitalna potrdila, ki jih izdaja SI-TRUST Root povezanim ali podrejenim izdajateljem, so namenjena preverjanju verige zaupanja za potrdila, ki so jih končnim uporabnikom izdali podrejeni ali povezani izdajatelji.

(2) Namen uporabe digitalnih potrdil, ki jih izdajajo podrejeni in povezani izdajatelji, določijo podrejeni in povezani izdajatelji v skladu z veljavno zakonodajo v svojih politikah delovanja.

(3) Namen uporabe digitalnih potrdil, ki jih izdajajo podrejeni in povezani izdajatelji, je določen tudi v medsebojnem dogovoru oz. pogodbi med SI-TRUST Root in posameznim zunanjim izdajateljem.

(4) Korenski izdajatelj SI-TRUST Root izdaja tudi potrdila za sistem OCSP za preverjanje veljavnosti potrdil, ki jih je izdal SI-TRUST Root.

1.4.1. Pravilna uporaba potrdil in ključev

(1) Namen potrdila oz. pripadajočih ključev je podan v potrdilu v polju *uporaba ključa* (angl. *Key Usage*), glej 7.1.2.

(2) Pri digitalnih potrdilih, ki jih izdaja SI-TRUST Root, je namen ključev in pripadajočega potrdila:
- zasebni ključ za podpisovanje digitalnih potrdil in registra preklicanih potrdil (v nadaljevanju *ključ za podpisovanje*) ter
- javni ključ za overjanje podpisa digitalnih potrdil in registra preklicanih potrdil (v nadaljevanju *ključ za overjanje podpisa*).

1.4.2. Nedovoljena uporaba potrdil in ključev

(1) Digitalna potrdila, ki jih izdaja SI-TRUST Root in njemu podrejeni ali z njim povezani izdajatelji, se morajo uporabljati v skladu s to politiko, veljavno zakonodajo in medsebojnim dogovorom oz. pogodbo, sicer njihova uporaba ni dovoljena.

(2) Drugih prepovedi v zvezi z uporabo potrdil korenskega izdajatelja SI-TRUST Root ni.

1.5. Upravljanje s politiko

Podrobnosti o upravljanju politik delovanja korenskemu izdajatelju SI-TRUST Root podrejeni ali z njim povezani izdajatelji določijo v svoji politiki delovanja.

1.5.1. Upravljavec politike

Upravni odbor overitelja na MJU je odgovoren za pripravo, prijavo, objavo, upravljanje in interpretacijo tega dokumenta.

1.5.2. Kontaktne osebe

Kontaktne osebe v zvezi s politiko in ostalo dokumentacijo so pooblaščene osebe overitelja na MJU (kontaktni podatki so podani v podpogl. 1.3).

1.5.3. Odgovorna oseba glede skladnosti delovanja izdajatelja s politiko

Odgovorne osebe glede skladnosti delovanja korenskega izdajatelja SI-TRUST Root skladno s to politiko so pooblaščene osebe overitelja na MJU v skladu z nalogami, ki jih opravljajo znotraj organizacijskih skupin (glej podpogl. 5.2).

1.5.4. Postopek za sprejem nove politike

(1) Overitelj na MJU lahko izda tudi amandmaje k politiki, glej podpogl. 9.12.

(2) Upravni odbor overitelja na MJU pripravi predlog nove politike oz. amandmaja.

(3) Novo politiko oz. amandmaje potrdi minister, pristojen za javno upravo.

(4) Skladno z ZEPEP se prijava novosti storitev overitelja na MJU opravi na pristojno ministrstvo za register overiteljev v Republiki Sloveniji.

1.6. Izrazi in okrajšave

1.6.1. Izrazi

(1) Splošni izrazi, ki se uporabljajo v tej politiki, so naslednji.

Digitalni podpis	Varen elektronski podpis, ki izpolnjuje zahteve 2. člena ZEPEP in 25. člena Uredbe k ZEPEP.
Digitalno potrdilo (Potrdilo)	Potrdilo v elektronski obliki, ki podaja naslednje ključne informacije: (1) podatek o izdajatelju, (2) podatek o imetniku, (3) imetnikov javni ključ, (4) čas veljavnosti in (5) digitalni podpis izdajatelja, ki je to potrdilo izdal.
Državni organ	Ministrstva, organi v sestavi ministrstev, vladne službe in upravne enote, Državni zbor, Državni svet, Ustavno sodišče, Računsko sodišče, Varuh človekovih pravic, pravosodni organi in druge osebe javnega prava, ki so neposredni uporabniki državnega proračuna v skladu z Zakonom o javnih financah (Uradni list RS, št. 11/11 – uradno prečiščeno besedilo, 14/13 – popr., 101/13 in 55/15 – ZFisP).
Infrastruktura javnih ključev	Nabor vlog, politik in postopkov, ki so potrebni za tvorjenje, upravljanje, distribucijo, uporabo, hrambo in preklic digitalnih potrdil ter za upravljanje šifriranja z javnimi ključi (primerjaj okrajšavo *PKI*).
Kvalificirano digitalno potrdilo	Digitalno potrdilo, ki izpolnjuje zahteve iz 28. člena ZEPEP in ki ga izda overitelj, ki deluje v skladu z zahtevami iz 29. do 36. člena ZEPEP in Uredbo k ZEPEP (primerjaj okrajšavo *ZEPEP* in izraz *Uredba k ZEPEP*).
Overitelj	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi in ki izpolnjuje zahteve overiteljev potrdil v skladu z Uredbo k ZEPEP in ZEPEP (primerjaj okrajšavo *CA* in izraz *Potrdilo*).
Register preklicanih potrdil	Seznam digitalnih potrdil, ki so bila preklicana pred potekom veljavnosti (angl. *Certification Revocation List*). Izdajatelj SI-TRUST Root ta seznam objavlja v svojem repozitoriju (primerjaj okrajšavo *CRL*).
Tretja oseba	Pravna ali fizična oseba oz. drug subjekt, ki se zanaša na izdana digitalna potrdila oz. na digitalni podpis, ki ga lahko verificira s pomočjo javnega ključa, ki se nahaja v digitalnem potrdilu.
Uredba k ZEPEP	Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06).
Zanesljivi seznam overiteljev	Zanesljivi seznam države članice Evropske Unije, ki določa minimalne podatke o nadzorovanih/akreditiranih overiteljih, ki izdajajo kvalificirana potrdila v skladu z veljavno zakonodajo, vključno z informacijami o kvalificiranih potrdilih (angl. *QC*) za overjanje elektronskega podpisa in informacijami, ali je podpis ustvarjen s sredstvi za varno elektronsko podpisovanje (angl. *SSCD*).

(2) Drugi izrazi, uporabljeni v tej politiki, so podani spodaj.

Domena	Neodvisna infrastruktura PKI za potrebe povezovanja overiteljev, ki je vzpostavljena znotraj določene organizacije. Izdajatelji znotraj

	posamezne domene uporabljajo nabor skupnih politik, ki jih označujemo kot politike domene.
Državni center za storitve zaupanja	Državni center za storitve zaupanja, ki deluje v okviru Ministrstva za javno upravo.
Imetnik	Uporabnik, ki mu je izdajatelj izdal digitalno potrdilo. V primeru korenskega izdajatelja SI-TRUST Root je to izdajatelj kvalificiranih digitalnih potrdil, ki je lahko korenskemu potrdilu SI-TRUST Root podrejen ali z njim povezan.
Infrastruktura overitelja	Vsi prostori overitelja, njegova strojna in programska oprema ter varnostni mehanizmi, ki so potrebni za varno delovanje njegovih izdajateljev.
Interna politika overitelja na MJU	Zaupni del notranjih pravil delovanja overitelja na Ministrstvu za javno upravo v skladu z Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06).
Izdajatelj	Izdajatelj digitalnih potrdil, ki deluje v okviru overitelja (primerjaj okrajšavo *CA* in izraza *Overitelj* in *Potrdilo*).
Javni imenik	Javni imenik, v katerem se objavijo izdana digitalna potrdila in register preklicanih potrdil. Za potrebe korenskega izdajatelja SI-TRUST Root je javni imenik vzpostavljen na strežniku *x500.gov.si* po standardu LDAP.
Končni uporabnik	Imetnik potrdila, izdanega od povezanega ali podrejenega izdajatelja.
Korenski izdajatelj	V hierarhičnem modelu infrastrukture javnih ključev korenski izdajatelj predstavlja osnovno izhodiščno točko zaupanja znotraj določene domene, njegovo potrdilo se uporablja pri preverjanju veljavnosti potrdil znotraj verige zaupanja.
Korenski izdajatelj SI-TRUST Root	Korenski izdajatelj digitalnih potrdil, ki deluje znotraj overitelja na MJU in izdaja digitalna potrdila za podrejene in povezane izdajatelje kvalificiranih digitalnih potrdil (angl. *Slovenian Trust Service Root Certification Authority*), http://www.ca.gov.si.
Medsebojno povezovanje	Medsebojno povezovanje ali tudi navzkrižno overjanje se uporablja za vzpostavljanje zaupanja tako med izdajatelji znotraj posamezne domene kot tudi za povezovanje izdajateljev iz različnih domen (znotrajdomensko (intra-domain) in meddomensko (inter-domain) overjanje).
Objava SI-TRUST Root	Javna objava na spletnih straneh overitelja na MJU, http://www.ca.gov.si.
Obvestila SI-TRUST Root	Vsa navodila, pojasnila, seznami, pogoji, posamezna obvestila, priporočila, standardi in drugi dokumenti, ki jih določi ali priporoči SI-TRUST Root oz. overitelj na MJU in jih objavi ali kako drugače posreduje imetnikom, organizacijam ali tretjim osebam.
Organizacija	Pravna ali fizična oseba, ki upravlja z izdajateljem potrdil, kateremu je SI-TRUST Root izdal povezovalno potrdilo (primerjaj izraz *Overitelj*).
Overitelj na MJU	Glej izraz Državni center za storitve zaupanja.
Podrejeni izdajatelj	V hierarhičnem modelu infrastrukture javnih ključev podrejeni izdajatelj nima samoizdanega potrdila, temveč mu je njegovo osnovno digitalno potrdilo izdal neposredno nadrejeni izdajatelj. Delovanje podrejenega izdajatelja je določeno s pravili nadrejenega izdajatelja. V infrastrukturi javnih ključev, ki jo vzpostavlja korenski izdajatelj SI-TRUST Root, le-ta v vlogi nadrejenega izdajatelja izdaja digitalna potrdila za podrejene izdajatelje. Hkrati SI-TRUST Root predstavlja osnovno izhodišče zaupanja znotraj domene pod SI-TRUST Root.
Politika	Javni del notranjih pravil overitelja, ki določajo namen, delovanje in metodologijo upravljanja z digitalnimi potrdili, odgovornost overitelja ter zahteve, ki jih morajo izpolnjevati uporabniki in tretje osebe, ki uporabljajo in se zanašajo na digitalna potrdila overitelja.

Povezani izdajatelj	Izdajatelj digitalnih potrdil, ki mu je korenski izdajatelj SI-TRUST Root izdal povezovalno potrdilo.
Povezovalno potrdilo	Digitalno potrdilo, ki vzpostavlja zaupanje med dvema izdajateljema.
Veriga zaupanja	Nabor potrdil, ki se uporabljajo pri preverjanju veljavnosti potrdila končnega uporabnika. Poleg potrdila končnega uporabnika vključuje še potrdilo korenskega izdajatelja ter potrdila podrejenih ali povezanih izdajateljev.
Vezno potrdilo	Digitalno potrdilo, v katerem se nov javni ključ podpiše s prejšnjim zasebnim ključem in tudi obratno

1.6.2. Okrajšave

CA	Izdajatelj digitalnih potrdil, angl. *Certification Authority*.
CP_{Name}	Ime politike delovanja overitelja oz. izdajatelja (angl. *Certification Policy Name*), povezano z enolično oznako politike delovanja (primerjaj okrajšavo CP_{OID}).
CP_{OID}	Enolična oznaka politike delovanja, ki temelji na številki OID, angl. *Certification Policy Object IDentifier.*
CRL	Seznam preklicanih potrdil (CRL, angl. *Certification Revocation List*) (primerjaj izraz *Register preklicanih potrdil*).
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	Mednarodna priporočila za področje telekomunikacij, angl. *European Telecommunications Standards Institut,* http://www.etsi.org.
FIPS	Nabor standardov ameriške vlade za uporabo v računalniških sistemih, angl. *Federal Information Processing Standard*
HSM	Strojna oprema za varno shranjevanje zasebnih ključev ali strojni varnostni modul, angl. *Hardware Security Module.*
LDAP	Protokol, ki določa dostop do imenika in je specificiran po IETF (angl. *Internet Engineering Task Force*) priporočilu RFC 1777»Leightweight Directory Access Protocol«.
MJU	Ministrstvo za javno upravo, Tržaška cesta 21, 1000 Ljubljana.
OCSP	Protokol za sprotno preverjanje veljavnosti kvalificiranih digitalnih potrdil po priporočilu RFC 2560 »X.509 Internet Public Key Infrastructure Online Certificate Status Protocol, (angl. *Online Certificate Status* Protocol).
OI	Polje v digitalnem potrdilu z imenom organizationIdentifier in OID številko 2.5.4.97, ki vsebuje identifikacijsko oznako organizacije, različno od njenega uradnega imena. Overitelj na MJU v skladu s standardi ETSI v ta namen uporablja davčno številko organizacije s predpono VATSI.
OID	Mednarodna številka, ki enolično določa posamezni objekt v skladu z mednarodnim standardom ITU-T X.208 (ASN.1), angl. *Object IDentifier.*

PKCS#7 in PKCS#10	Priporočila (angl. *Public Key Cryptography Standards*) podjetja RSA Security za razvijalce računalniških sistemov, ki uporabljajo asimetrične kriptografske algoritme. • PKCS#7 določa sintakso za kriptografsko obdelane podatke, kot so digitalni podpisi in digitalne ovojnice. Uporablja se npr. za pošiljanje digitalnih potrdil in seznamov preklicanih potrdil. • PKCS#10 določa sintakso za zahtevek za overitev javnega ključa, imena in drugih atributov.
PKI	Infrastruktura javnih ključev, angl. *Public Key Infrastructure*
PKIX-CMP	Določa postopek za izmenjavo podatkov, ki se nanašajo na digitalna potrdila med entitetami infrastrukture overitelja. Zajema tudi *de-facto* standarda PKCS#7 in PKCS#10. Objavljen je kot priporočilo RFC 4210 »*Public Key Infrastructure (based on) X.509 - Certificate Management Protocols*«.
RFC	Mednarodna priporočila za Internet skupine IETF, angl. *Internet Engineering Task Force* in IESG, angl. *Internet Engineering Steering Group*, angl. *Request for Comments*, http://www.ietf.org/rfc.html.
SI-TRUST Root	Korenski izdajatelj digitalnih potrdil, angl. *Slovenian Trust Service Root Certification Authority*.
UTF-8	Način kodiranja mednarodnega nabora znakov unicode, pri katerem znaki ASCII ostanejo enozložni, ostali znaki pa lahko zasedajo več zlogov.
X.501	Priporočila za razločevalna imena: »ITU-T Recommendation X.501 - Information technology - Open Systems Interconnection - The Directory: Models«.
X.509	Priporočila za profil digitalnih potrdil in registra preklicanih potrdil: RFC 5280: »Internet X.509 Public Key Infrastructure Certificate and CRL Profile«.
TSA	Izdajatelj varnih časovnih žigov (TSA, angl. *Time Stamping Authority*).
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14).

2. OBJAVE IN ODGOVORNOSTI GLEDE REPOZITORIJA

2.1. Repozitoriji

Overitelj na MJU dokumente oz. podatke korenskega izdajatelja SI-TRUST Root javno objavlja v dveh repozitorijih:

- v javnem imeniku na strežniku x500.gov.si ter
- na spletnih straneh http://www.ca.gov.si.

2.2. Objava informacij o potrdilih

(1) Overitelj na MJU javno objavlja naslednje dokumente oz. podatke korenskega izdajatelja SI-TRUST Root:

- politike delovanja izdajatelja,
- izdana digitalna potrdila,
- register preklicanih digitalnih potrdil,

- informacije o veljavni zakonodaji in drugih pravilih, ki določajo delovanje overitelja na MJU ter
- ostale informacije v zvezi z delovanjem SI-TRUST Root.

(2) Digitalna potrdila, ki jih je izdal SI-TRUST Root, se objavijo v strukturi javnega imenika na strežniku x500.gov.si (podrobneje podano v podpogl. 7).

(3) Preklicana potrdila, ki jih je izdal SI-TRUST Root, le ta objavi v registru preklicanih potrdil, ki se nahaja v strukturi javnega imenika na strežniku x500.gov.si ter na spletnih straneh http://www.ca.gov.si (podrobneje podano v podpogl. 7.2).

(4) Ostali dokumenti oz. ključni podatki o delovanju korenskega izdajatelja SI-TRUST Root ter splošna obvestila imetnikom in tretjim osebam se objavijo na spletnih straneh http://www.ca.gov.si.

(5) Zaupni del notranjih pravil overitelja na MJU, znotraj katerega deluje korenski izdajatelj SI-TRUST Root, ni javno dostopen dokument.

(6) Imetniki digitalnih potrdil morajo javno objaviti dokumente, ki jih za izdajatelje kvalificiranih digitalnih potrdil določa veljavna zakonodaja. V primeru povezovanja izdajateljev s sedežem izven Republike Slovenije morajo le-ti objaviti dokumente v skladu z ekvivalentno evropsko oz. domicilno zakonodajo. Korenski izdajatelj SI-TRUST Root in imetnik lahko zahteve glede objav določita tudi v medsebojnem dogovoru oz. pogodbi.

(7) Overitelj na MJU je odgovoren za pravočasnost in verodostojnost objavljenih dokumentov in ostalih podatkov.

(8) Korenskemu izdajatelju SI-TRUST Root podrejeni in z njim povezani izdajatelji so odgovorni za objavo dokumentov in podatkov v skladu s to politiko, medsebojnim dogovorom oz. pogodbo in veljavno zakonodajo.

2.3. Pogostnost javne objave

(1) Nove politike so objavljene v skladu z navedbo v podpogl. 9.10.

(2) Javno dostopne informacije oz. dokumenti se objavijo takoj po njihovem nastanku.

(3) Digitalna potrdila se objavijo v javnem imeniku takoj ob njihovi izdaji.

(4) Preklicana potrdila se v registru preklicanih potrdil objavijo takoj (podrobno o tem v podpogl. 4.9.8).

(5) Ostale javno dostopne informacije oz. dokumenti se objavijo po potrebi.

2.4. Dostop do repozitorijev

(1) Javno dostopne informacije oz. dokumenti, digitalna potrdila in register preklicanih potrdil so na razpolago 24ur/7dni/365dni brez omejitev.

(2) Vsak izdajatelj, bodisi korenski bodisi podrejeni ali povezani, zagotavlja in odgovarja za ustrezne mehanizme za avtoriziran dostop do objave in spremembe javno objavljenih podatkov.

(3) Natančna določila o tem so objavljena v notranjih pravilih overitelja na MJU, lahko pa so določena tudi v medsebojnem dogovoru oz. pogodbi med korenskim izdajateljem SI-TRUST Root in imetnikom.

3. ISTOVETNOST IN VERODOSTOJNOST

3.1. Določanje imen

Korenskemu izdajatelju SI-TRUST Root podrejeni in z njim povezani izdajatelji podrobnosti o imenovanju subjektov, ki jim izdajajo digitalna potrdila, določijo v svoji politiki delovanja skladno z interno politiko overitelja na MJU ter morebitnim medsebojnim dogovorom oz. pogodbo.

3.1.1. Oblika imen

Vsako potrdilo vsebuje v skladu s priporočilom RFC 5280 podatke o imetniku ter izdajatelju v obliki razločevalnega imena, ki je oblikovano kot *UTF8String* oz. *PrintableString* v skladu s priporočilom RFC 5280 »Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile« in s standardom *X.501.*

3.1.2. Zahteva po smiselnosti imen

(1) Razločevalno ime imetnika, vsebovano v polju *imetnik,* enolično identificira podrejenega ali povezanega izdajatelja (glej podpogl. 3.1.4).

(2) Razločevalno ime imetnika je določeno skladno s standardi ETSI EN 319412-1, ETSI EN 319412-2 in ETSI EN 319412-3. Pri izdajateljih, ki so z delovanjem pričeli pred uveljavitvijo eIDAS, se lahko razločevalno ime imetnika določi skladno z interno politiko overitelja na MJU ter morebitnim medsebojnim dogovorom oz. pogodbo.

3.1.3. Uporaba anonimnih imen ali psevdonimov

Ni predvidena.

3.1.4. Pravila za interpretacijo imen

(1) Korenski izdajatelj SI-TRUST Root je v vseh potrdilih, ki jih izda, naveden v obliki razločevalnega imena v polju *izdajatelj* (angl. *issuer*). Imetnik potrdila je v potrdilu naveden v obliki razločevalnega imena v polju *imetnik (*angl. *subject*).

(2) Razločevalna imena v digitalnih potrdil za imetnike se določijo skladno z interno politiko overitelja na MJU ter morebitnim medsebojnim dogovorom oz. pogodbo.

3.1.5. Enoličnost imen

(1) Podeljeno razločevalno ime je enolično za vsako izdano potrdilo.

(2) Razločevalno ime se pri postopku obnove potrdila ohranja, če se imetnik in korenski izdajatelj ne dogovorita drugače.

3.1.6. Priznavanje, verodostojnost in vloga blagovnih znamk

(1) Imetnik ne sme zahtevati razločevalnega imena, ki bi pripadalo nekomu drugemu in bi bile s tem kršene kakršnekoli pravice glede blagovne znamke ali druge avtorske pravice drugih oseb.

(2) Odgovornost v zvezi s pravico uporabe imen oz. zaščitenih znamk in drugih pravic je izključno na strani imetnika. Korenski Izdajatelj SI-TRUST Root ni dolžan preverjati in/ali na to opozoriti imetnika.

(3) Morebitne spore rešujeta izključno prizadeta stran in imetnik.

3.2. Začetno preverjanje istovetnosti

Korenskemu izdajatelju SI-TRUST Root podrejeni in z njim povezani izdajatelji podrobnosti o začetnem preverjanju istovetnosti svojih imetnikov, ki jim izdajajo digitalna potrdila, določijo v svoji politiki delovanja v skladu s to politiko in morebitnim medsebojnim dogovorom oz. pogodbo.

3.2.1. Metoda za dokazovanje lastništva zasebnega ključa

Dokazovanje posedovanja zasebnega ključa, ki pripada javnemu ključu v potrdilu, je zagotovljeno z varnimi postopki pred in ob prevzemu potrdila. Zahtevek za izdajo potrdila vsebuje javni ključ in je podpisan s pripadajočim zasebnim ključem, npr. v obliki PKCS#10 v skladu z RSA PKCS#10 Certification Request Syntax Standard.

3.2.2. Preverjanje istovetnosti organizacij

(1) Bodoči imetnik mora korenskemu izdajatelju SI-TRUST Root predložiti ustrezna dokazila o svoji istovetnosti in druge svoje podatke.

(2) SI-TRUST Root preveri podatke v ustreznih in dostopnih registrih oz. v primeru povezovanja z izdajatelji izven Republike Slovenije tudi pri ustreznih drugih institucijah.

(3) Podrobnosti o postopku preverjanja določi korenski izdajatelj SI-TRUST Root v interni politiki overitelja na MJU in morebitnem medsebojnem dogovoru oz. pogodbi.

3.2.3. Preverjanje istovetnosti fizičnih oseb

(1) Pooblaščena oseba bodočega imetnika korenskemu izdajatelju SI-TRUST Root predloži dokumente z ustreznimi dokazili svoje istovetnosti in pooblastilom. Korenski izdajatelj SI-TRUST Root lahko njegovo istovetnost dodatno preveri v ustreznih registrih oz. v primeru povezovanja z izdajatelji izven Republike Slovenije tudi pri ustreznih drugih institucijah.

(2) Podrobnosti postopka in zahteve so predpisane v interni politiki overitelja na MJU in morebitnem medsebojnem dogovoru oz. pogodbi.

3.2.4. Nepreverjeni podatki pri začetnem preverjanju

(1) Nepreverjeni so vsi tisti podatki, ki jih korenski izdajatelj ne more preveriti v ustreznih registrih oz. drugih

institucijah oz. za katere se medsebojno dogovorita SI-TRUST Root in imetnik.

(2) Obseg podatkov določi korenski izdajatelj SI-TRUST Root v interni politiki overitelja na MJU in morebitnem medsebojnem dogovoru oz. pogodbi.

3.2.5. Preverjanje pooblastil

Preverjanje pooblastila za pridobitev digitalnega potrdila se izvaja v okviru postopka preverjanja istovetnosti za fizične osebe skladno z podpogl. 3.2.3

3.2.6. Merila za medsebojno povezovanje

(1) Povezani izdajatelji, ki se želijo povezati z infrastrukturo javnih ključev v okviru korenskega izdajatelja SI-TRUST Root, morajo izpolnjevati najmanj naslednje pogoje:
- izdajatelj izdaja kvalificirana digitalna potrdila v skladu s svojo politiko delovanja,
- je naveden v zanesljivem seznamu overiteljev, če ima sedež v državi članici Evropske Unije, oz. je vključen v drug ustrezen sistem, ki omogoča nadzor nad njegovim delovanjem v skladu z zahtevami slovenske in evropske zakonodaje, če ima sedež v državah izven Evropske Unije.

(2) Pri povezovanju z zunanjimi izdajatelji so način in pogoji medsebojnega povezovanja določeni z medsebojnim dogovorom oz. pogodbo.

(3) Overitelj na MJU ni dolžan priznati drugih izdajateljev tudi, če izpolnjujejo pogoje iz prvega odstavka. Končno odločitev o medsebojnemu povezovanju sprejme upravni odbor overitelja na MJU.

(4) Overitelj na MJU zagotavlja, da bo izvajal medsebojno priznavanje izključno po podpisu pisne pogodbe oz. dogovora z drugimi overitelji, ki morajo izpolnjevati raven varnostnih zahtev, ki je primerljiva ali višja, kot jo predpiše overitelj na MJU.

(5) Overitelj na MJU lahko od imetnika iz države članice EU zahteva vpogled v zadnje poročilo o ugotavljanju skladnosti v skladu z eIDAS oz. ekvivalentno poročilo o zunanjem preverjanju od ostalih imetnikov.

(6) Stroške potrebne infrastrukture, ki jo zahteva overitelj na MJU za medsebojno priznavanje, krije drugi overitelj.

3.3. Istovetnost in verodostojnost ob obnovi potrdila

Korenskemu izdajatelju SI-TRUST Root podrejeni in z njim povezani izdajatelji podrobnosti o postopku obnove določijo v svoji politiki delovanja v skladu s to politiko in morebitnim medsebojnim dogovorom oz. pogodbo.

3.3.1. Istovetnost in verodostojnost ob obnovi

Pred potekom zasebnega ključa za podpisovanje mora imetnik zahtevati obnovo potrdila po postopku za izdajo novega digitalnega potrdila kot ob prvi pridobitvi digitalnega potrdila in začetnem preverjanju istovetnosti v skladu s podpogl. 3.2.

3.3.2. Istovetnost in verodostojnost ob obnovi po preklicu

(1) Obnova digitalnega potrdila po preklicu ni mogoča.

(2) Za ponovno pridobitev digitalnega potrdila po preklicu za podrejene in povezane izdajatelje se izvede postopek za izdajo novega digitalnega potrdila kot ob prvi pridobitvi digitalnega potrdila in začetnem preverjanju istovetnosti v skladu s podpogl. 3.2.

3.4. Istovetnost in verodostojnost ob zahtevi za preklic

(1) Korenski izdajatelj SI-TRUST Root preveri imetnikovo istovetnost in druge podatke po postopku, ki je določen v interni politiki overitelja na MJU ter morebitnem medsebojnem dogovoru oz. pogodbi.

(2) Korenskemu izdajatelju SI-TRUST Root podrejeni in z njim povezani izdajatelji podrobnosti o tem postopku določijo v svoji politiki delovanja v skladu s to politiko in morebitnim medsebojnim dogovorom oz. pogodbo.

4. UPRAVLJANJE S POTRDILI

4.1. Zahtevek za pridobitev potrdila

Vsi podrejeni in povezani izdajatelji določijo podrobnosti glede pridobitve digitalnih potrdil v svojih politikah delovanja v skladu s to politiko in morebitnim medsebojnim dogovorom oz. pogodbo.

4.1.1. Kdo lahko predloži zahtevek za pridobitev potrdila

(1) Zahtevek za pridobitev potrdila lahko korenskemu izdajatelju SI-TRUST Root predloži izdajatelj oz. bodoči izdajatelj, ki izpolnjuje pogoje za povezane oz. podrejene izdajatelje, ki jih s pričujočo politiko in morebitnim medsebojnim dogovorom oz. pogodbo zahteva korenski izdajatelj SI-TRUST Root.

(2) Če je bodoči imetnik zunanji izdajatelj, mora ob zahtevku za pridobitev v skladu s pogoji iz medsebojnega dogovora oz. pogodbe korenskemu izdajatelju SI-TRUST Root predložiti tudi druga dokazila o ustreznosti svojega delovanja.

(3) Overitelj na MJU lahko zahtevek za pridobitev potrdila zavrne tudi, če izdajatelj izpolnjuje vse zahtevane pogoje (glej podpogl. 3.2.6).

4.1.2. Postopek za pridobitev potrdila in odgovornosti

(1) Če je bodoči imetnik zunanji izdajatelj, mora s korenskim izdajateljem SI-TRUST Root skleniti medsebojni dogovor oz. pogodbo.

(2) Obliko pisnega zahtevka in način za oddajo zahtevka ter ostale podrobnosti določi korenski izdajatelj SI-TRUST Root v interni politiki overitelja na MJU ter morebitnem medsebojnem dogovoru oz. pogodbi.

(3) Imetnik odgovarja za verodostojnost podatkov in ravnanje v skladu s to politiko in morebitnim medsebojnim dogovorom oz pogodbo.

(4) Podrobnosti postopka za oddajo zahtevka za pridobitev digitalnega potrdila so podane v interni politiki overitelja na MJU ter morebitnem medsebojnem dogovoru oz. pogodbi.

4.2. Postopek ob sprejemu zahtevka za pridobitev potrdila

Vsi podrejeni in povezani izdajatelji določijo podrobnosti glede pridobitve digitalnih potrdil v svojih politikah delovanja v skladu s to politiko in morebitnim medsebojnim dogovorom oz. pogodbo.

4.2.1. Postopek preverjanja istovetnosti in verodostojnosti bodočega imetnika

Glej podpogl. 3.2.2.

4.2.2. Odobritev/zavrnitev zahtevka

(1) Zahtevek za pridobitev potrdila odobrijo oz. zavrnejo pooblaščene osebe overitelja na MJU v skladu z odločitvijo upravnega odbora overitelja na MJU.

(2) Postopek je podrobnejše opisan v interni politiki overitelja na MJU ter morebitnem medsebojnem dogovoru oz. pogodbi.

4.2.3. Čas za izdajo potrdila

(1) Korenski izdajatelj SI-TRUST Root mora prosilcu za pridobitev digitalnega potrdila podati odgovor glede odobritve oz. zavrnitve njegovega zahtevka najkasneje v tridesetih (30) dneh.

(2) SI-TRUST Root in bodoči imetnik se medsebojno dogovorita glede roka za izdajo potrdila potem, ko so izpolnjeni vsi potrebni pogoji za njegovo izdajo.

4.3. Izdaja potrdila

Vsi podrejeni in povezani izdajatelji določijo podrobnosti glede izdaje digitalnih potrdil v svojih politikah delovanja v skladu z veljavno zakonodajo ter to politiko in morebitnim medsebojnim dogovorom oz. pogodbo.

4.3.1. Postopek izdajatelja ob izdaji potrdila

(1) Po odobritvi izdaje in sklenitvi medsebojnega dogovora oz. pogodbe z zunanjim izdajateljem korenski izdajatelj SI-TRUST Root izda digitalno potrdilo na podlagi zahtevka v skladu s podpogl. 3.2.

(2) Izdano digitalno potrdilo SI-TRUST Root objavi v javnem imeniku in na spletnih straneh (glej podpogl. 4.4.2).

(3) Podrobnosti o postopku izdaje so določene v interni politiki overitelja na MJU ter morebitnem medsebojnem dogovoru oz. pogodbi.

4.3.2. Obvestilo imetniku o izdaji potrdila

(1) Korenski izdajatelj SI-TRUST Root obvesti bodočega imetnika o izdaji in podrobnostih prevzema digitalnega potrdila.

(2) SI-TRUST Root imetniku posreduje digitalno potrdilo na način, določen v interni politiki overitelja na MJU ter morebitnem medsebojnem dogovoru oz. pogodbi.

4.4. Prevzem potrdila

Vsi podrejeni in povezani izdajatelji določijo podrobnosti glede prevzema digitalnih potrdil v svojih politikah delovanja v skladu s to politiko in morebitnim medsebojnim dogovorom oz. pogodbo.

4.4.1. Postopek prevzema potrdila

(1) Podrobnosti postopka prevzema potrdila določi korenski izdajatelj SI-TRUST Root in z njimi na dogovorjen način seznani bodočega imetnika.

(2) Imetnik je odgovoren, da takoj po prevzemu potrdila preveri podatke v tem potrdilu. Če korenskega izdajatelja SI-TRUST Root ne obvesti o morebitnih napakah, se smatra, da se z vsebino in pogoji za posedovanje in uporabo strinja.

4.4.2. Objava potrdila

Izdano potrdilo se na vnaprej dogovorjen način javno objavi v repozitoriju overitelja na MJU, kot je navedeno v pogl.2.

4.4.3. Obvestilo o izdaji tretjim osebam

Ni predpisano.

4.5. Uporaba potrdil in ključev

4.5.1. Uporaba potrdila in zasebnega ključa imetnika

(1) Imetnik potrdila je glede varovanja zasebnih ključev dolžan:

- uporabljati opremo za zaščito zasebnega ključa, ki ustreza svetovno uveljavljenim varnostnim in tehničnim standardom, pri čemer mora izpolnjevati vsaj enega izmed pogojev, določenih v standardu ETSI EN 319 411-1 (glej podpogl. 6.2),
- uporabljati programsko opremo, ki je certificirana v skladu s Common Criteria vsaj EAL4+ ali je vzpostavljena v skladu s standardom ETSI EN 319 401 (glej podpogl. 6.6),
- zasebne ključe in vse druge zaupne podatke ščititi s primernim geslom v skladu s priporočili SI-TRUST Root ali na drug način tako, da je onemogočen nepooblaščeni dostop do njih,
- skrbno varovati gesla za zaščito zasebnih ključev,
- po preteku veljavnosti oz. preklicu potrdila ravnati v skladu z obvestili izdajatelja SI-TRUST Root.

(2) Imetnik mora varovati zasebni ključ za podpisovanje podatkov pred nepooblaščeno uporabo.

(3) Ostale dolžnosti in odgovornosti so določene v podpogl. 9.6.3.

4.5.2. Uporaba potrdila in javnega ključa za tretje osebe

(1) Tretja oseba, ki se zanaša na potrdilo, mora ravnati in uporabljati potrdila v skladu s politiko in ostalimi veljavnimi predpisi.

(2) Tretja oseba se lahko zanaša na potrdilo samo za namen, določen v potrdilu (glej podpogl. 6.1.7), in na način, ki je določen s politiko,

(3) Ob uporabi potrdila mora tretja oseba vedno preveriti veljavnost digitalnega potrdila v skladu z navodili korenskega izdajatelja SI-TRUST Root*:*

- v času uporabe potrdila preveriti, če potrdilo ni preklicano,
- v času uporabe potrdila preveriti, če je bil digitalni podpis kreiran v času veljavnosti in z ustreznim namenom potrdila,
- v času uporabe potrdila preveriti podpis korenskega izdajatelja potrdila SI-TRUST Root, ki je objavljen v tej politiki in tudi na morebiten drug način posredovan tretjim osebam,

(4) Ostale dolžnosti in odgovornosti so določene v podpogl. 9.6.4.

4.6. Ponovna izdaja potrdila brez spremembe javnega ključa

Ni podprta.

4.6.1. Razlogi za ponovno izdajo potrdila

Ni podprto.

4.6.2. Kdo lahko zahteva ponovno izdajo

Ni podprto.

4.6.3. Postopek ob ponovni izdaji potrdila

Ni podprto.

4.6.4. Obvestilo imetniku o izdaji novega potrdila

Ni podprto.

4.6.5. Prevzem ponovno izdanega potrdila

Ni podprto.

4.6.6. Objava ponovno izdanega potrdila

Ni podprto.

4.6.7. Obvestilo o izdaji drugim subjektom

Ni podprto.

4.7. Obnova potrdila

4.7.1. Razlogi za obnovo potrdila

(1) Obnova potrdila se izvede zaradi poteka veljavnosti potrdila, ki ga je imetniku izdal SI-TRUST Root. Ob tem se izda novo potrdilo z enakimi podatki o imetniku.

(2) Postopek se praviloma izvede pred potekom veljavnosti potrdila (glede veljavnosti ključev glej podpogl. 6.3.2.).

4.7.2. Kdo lahko zahteva obnovo potrdila

Obnovo zahteva imetnik ali od njega pooblaščena oseba.

4.7.3. Postopek pri obnovi potrdila

Postopek je enak kot pri prvi izdaji potrdila, glej podpogl. 4.3

4.7.4. Obvestilo imetniku o obnovi potrdila

Postopek je enak kot pri prvi izdaji potrdila, glej podpogl. 4.3.2.

4.7.5. Prevzem obnovljenega potrdila

Postopek je enak kot pri prvem prevzemu potrdila, glej podpogl. 4.4.

4.7.6. Objava obnovljenega potrdila

Postopek je enak kot pri prvem prevzemu potrdila, glej podpogl. 4.4.2.

4.7.7. Obvestilo o izdaji drugim subjektom

Postopek je enak kot pri prvem prevzemu potrdila, glej podpogl. 4.4.3.

4.8. Sprememba potrdila

(1) Če pride do spremembe politike imetnika, ki vpliva na zaupanje v veljavnost njegovega potrdila oz. potrdil njegovih končnih uporabnikov, je potrebno potrdilo preklicati.

(2) Za pridobitev novega potrdila je potrebno ponoviti postopek, kot je naveden v podpogl. 4. Storitev izdajatelja za spremembo potrdil ni podprta.

4.8.1. Razlogi za spremembo potrdila

Ni podprto.

4.8.2. Kdo lahko zahteva spremembo

Ni podprto.

4.8.3. Postopek ob spremembi potrdila

Ni podprto.

4.8.4. Obvestilo imetniku o izdaji novega potrdila

Ni podprto.

4.8.5. Prevzem spremenjenega potrdila

Ni podprto.

4.8.6. Objava spremenjenega potrdila

Ni podprto.

4.8.7. Obvestilo o izdaji drugim subjektom

Ni podprto.

4.9. Preklic in začasna razveljavitev potrdila[3]

4.9.1. Razlogi za preklic

(1) Preklic se lahko zahteva v primeru razkritja ključa ali drugih razlogov, ki vplivajo na nivo zaupanja in

[3] Po priporočilu RFC 3647 to podpoglavje vključuje tudi postopek za storitev suspenza, ki jo SI-TRUST Root ne omogoča.

zanesljivost zasebnega ključa.

(2) Ostali razlogi za preklic so lahko:
- neizpolnjevanje pogojev oz. zahtev za imetnike iz te politike ali morebitnega medsebojnega dogovora oz. pogodbe,
- prekinitev dejavnosti korenskega izdajatelja SI-TRUST Root, prekinitev izdajanja potrdil ali prepoved upravljanja s potrdili,
- prekinitev dejavnosti podrejenega oz. povezanega izdajatelja,
- prevzem dejavnosti korenskega izdajatelja SI-TRUST Root s strani drugega overitelja,
- odredba pristojnega sodišča ali upravnega organa.

(3) Korenski izdajatelj SI-TRUST Root prekliče potrdilo tudi brez zahteve imetnika takoj, ko izve:
- da je podatek v potrdilu napačen ali je bilo potrdilo izdano na podlagi napačnih podatkov,
- da so se spremenile druge okoliščine, ki vplivajo na veljavnost potrdila,
- za neizpolnjevanje obveznosti imetnika iz te politike in morebitnega medsebojnega dogovora oz. pogodbe,
- da niso poravnani stroški za upravljanje digitalnih potrdil,
- da je bila infrastruktura overitelja na MJU ogrožena na način, ki vpliva na zanesljivost potrdila,
- da je bil zasebni ključ imetnika potrdila ogrožen na način, ki vpliva na zanesljivost uporabe,
- da bo SI-TRUST Root prenehal z izdajanjem potrdil ali da je bilo overitelju na MJU prepovedano upravljanje s potrdili in njegove dejavnosti ni prevzel drug overitelj,
- da je preklic odredilo pristojno sodišče ali upravni organ.

4.9.2. Kdo lahko zahteva preklic

(1) Preklic potrdila lahko zahteva:
- pooblaščena oseba korenskega izdajatelja SI-TRUST Root,
- imetnik,
- pristojno sodišče ali
- upravni organ.

(2) Korenski izdajatelj SI-TRUST Root si pridržuje pravico za preklic izdanega digitalnega potrdila v primeru neizpolnjevanja zahtev za podrejene in povezane izdajatelje.

4.9.3. Postopek za preklic

(1) V primeru, če preklic zahteva imetnik, je postopek določen v interni politiki overitelja na MJU ter morebitnem medsebojnem dogovoru oz. pogodbi.

(2) O preklicu korenski izdajatelj SI-TRUST Root obvesti imetnika ter druge subjekte, na katere lahko vpliva preklic digitalnega potrdila (t.j. tretje osebe oz. ostale subjekte, ki se zanašajo na digitalno potrdilo).

(3) Odločitev o preklicu potrdila sprejme upravni odbor overitelja na MJU najkasneje v šestnajstih (16) urah od prejema zahtevka za preklic, če gre za preklic zaradi nevarnosti zlorabe ali nezanesljivosti ipd., sicer pa prvi delovni dan po prejetju zahtevka za preklic.

(4) Če preklic odredi sodišče ali upravni organ, se to izvede po veljavnih postopkih.

(5) Po izvedenem preklicu je imetnik obveščen o datumu ter času preklica, izdajatelju zahtevka za preklic ter vzrokih za preklic.

4.9.4. Čas za izdajo zahtevka za preklic

Zahtevek za preklic je potrebno zahtevati nemudoma, če gre za možnost zlorabe ali nezanesljivosti.

4.9.5. Čas od prejetega zahtevka za preklic do izvedbe preklica

(1) Korenski izdajatelj SI-TRUST Root po odločitvi upravnega odbora overitelja na MJU prekliče potrdilo najkasneje v štirih (4) urah, če gre za preklic zaradi nevarnosti zlorabe ali nezanesljivosti ipd., sicer pa prvi delovni dan po odločitvi upravnega odbora overitelja na MJU.

(2) Po preklicu je tako potrdilo takoj dodano v register preklicanih potrdil in brisano iz javnega imenika potrdil, v katerem ostanejo le evidenčni podatki potrdila.

4.9.6. Zahteve po preverjanju registra preklicanih potrdil za tretje osebe

(1) Tretje osebe, ki se zanašajo na potrdilo, morajo pred uporabo preveriti najnovejši register preklicanih potrdil.

(2) Zaradi verodostojnosti in celovitosti je vedno potrebno preveriti veljavnost in verodostojnost tega registra, ki je digitalno podpisan s strani korenskega izdajatelja SI-TRUST Root.

(3) Tretja oseba mora za vsako uporabljeno digitalno potrdilo izvesti popoln postopek preverjanja verige zaupanja v skladu z RFC 5280.

(4) Če tretja oseba ne more preveriti statusa digitalnega potrdila v registru preklicanih potrdil, lahko zavrne uporabo digitalnega potrdila oz. digitalno potrdilo kljub temu uporabi in zavestno sprejme.

4.9.7. Pogostnost objave registra preklicanih potrdil

Register preklicanih potrdil se osvežuje (za dostop do registra glej podpogl. 7.2.2):
- po vsakem preklicu potrdila,
- najmanj enkrat letno, če ni novih zapisov oz. sprememb v registru preklicanih potrdil.

4.9.8. Čas do objave registra preklicanih potrdil

(1) Objava novega registra preklicanih potrdil se izvede:
- v javnem imeniku na strežniku *x500.gov.si* takoj,
- na spletni strani pa z zakasnitvijo največ ene (1) ure.

(2) Register preklicanih potrdila se posreduje morebitnim tretjim osebam in ostalim subjektom, ki se zanašajo na izdana digitalna potrdila korenskega izdajatelja SI-TRUST Root.

4.9.9. Sprotno preverjanje statusa potrdil

Podprt je protokol za sprotno preverjanje statusa potrdil (OCSP) v skladu s priporočilom RFC 2560 »X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP«. Podrobno o tem glej podpogl. 7.3.

4.9.10. Zahteve za sprotno preverjanje statusa potrdil

Tretje osebe morajo ob uporabi potrdila vedno preveriti, ali je potrdilo, na katerega se zanašajo, preklicano. Glej tudi podpogl. 4.9.6.

4.9.11. Drugi načini za dostop do statusa potrdil

Niso podprti.

4.9.12. Druge zahteve pri zlorabi zasebnega ključa

Niso predpisane.

4.9.13. Razlogi za začasno razveljavitev

Ni podprto.

4.9.14. Kdo lahko zahteva začasno razveljavitev

Ni podprto.

4.9.15. Postopek za začasno razveljavitev

Ni podprto.

4.9.16. Čas začasne razveljavitve

Ni podprto.

4.10. Preverjanje statusa potrdil

4.10.1. Dostop za preverjanje

Register preklicanih potrdil je objavljen v javnem imeniku na strežniku *x500.gov.si* ter na spletnih straneh http://www.ca.gov.si, sprotno preverjanje statusa potrdila je dostopno na naslovu http://ocsp.ca.gov.si, podrobnosti o dostopu pa so v podpogl. 7.2 in 7.3.

4.10.2. Razpoložljivost

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

4.10.3. Druge možnosti

Niso predpisane.

4.11. Prekinitev razmerja med imetnikom in overiteljem

(1) Določila glede prekinitve razmerja med zunanjim izdajateljem in korenskim izdajateljem SI-TRUST Root so določena v medsebojnem dogovoru oz. pogodbi.

(2) Razmerje med zunanjim izdajateljem in korenskim izdajateljem SI-TRUST Root se prekine, če
- imetnikovo potrdilo preteče in le-ta ne zahteva njegove obnove,
- je potrdilo preklicano, imetnik pa ne zaprosi za novega.

4.12. Odkrivanje kopije ključev za dešifriranje

Ni podprto.

4.12.1. Postopek za odkrivanje ključev za dešifriranje

Ni podprto.

4.12.2. Postopek za odkrivanje ključa seje

Ni podprto.

5. UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE

5.1. Fizično varovanje

(1) Oprema overitelja na MJU je varovana z večnivojskim sistemom fizičnega in elektronskega varovanja.

(2) Varovanje infrastrukture overitelja na MJU se izvaja v skladu s priporočili stroke za najvišji nivo varovanja.

(3) Celoten opis infrastrukture overitelja na MJU in postopki upravljanja ter varovanje le-te so določeni z Interno politiko overitelja na MJU.

5.1.1. Lokacija in zgradba overitelja

(1) Oprema overitelja na MJU je postavljena v posebnih, varovanih, ločenih prostorih v okviru infrastrukture Ministrstva za javno upravo.

(2) Zavarovana je z večnivojskim sistemom fizičnega in elektronskega varovanja.

(3) Podrobna določila so v Interni politiki overitelja na MJU.

5.1.2. Fizični dostop do infrastrukture overitelja

(1) Dostop do infrastrukture overitelja na MJU oz. izdajatelja je omogočen samo pooblaščenim osebam overitelja na MJU skladno z njihovimi nalogami in pooblastili, glej podpogl. 5.2.

(2) Vsi dostopi so varovani v skladu z veljavno zakonodajo in priporočili.

(3) Podrobna določila so v Interni politiki overitelja na MJU.

5.1.3. Napajanje in prezračevanje

(1) Infrastruktura overitelja na MJU ima zagotovljeno neprekinjeno napajanje in ustrezne klimatske sisteme.

(2) Podrobno o tem je določeno v Interni politiki overitelja na MJU.

5.1.4. Zaščita pred poplavo

(1) Infrastruktura overitelja na MJU ni izpostavljena nevarnosti poplav.

(2) Podrobno o tem je določeno v Interni politiki overitelja na MJU.

5.1.5. Zaščita pred požari

(1) Prostori overitelja na MJU so varovani pred morebitnim izbruhom požara.

(2) Podrobno o tem je določeno v Interni politiki overitelja na MJU.

5.1.6. Hramba nosilcev podatkov

(1) Podatki v fizični ali elektronski obliki se zapisujejo na nosilce podatkov, ki se varno hranijo v zaščitenih objektih.

(2) Varnostne kopije programske opreme in šifriranih baz overitelja na MJU se redno obnavljajo in shranjujejo v dveh ločenih in fizično varovanih prostorih, na različnih lokacijah.

(3) Podrobno o tem je določeno v Interni politiki overitelja na MJU.

5.1.7. Odstranjevanje odpadkov

(1) Overitelj na MJU zagotavlja varno odstranjevanje in uničevanje dokumentov v fizični in elektronski obliki.

(2) Odstranjevanje odpadkov izvaja posebna komisija v skladu z Interno politiko overitelja na MJU.

5.1.8. Hramba na oddaljeni lokaciji

Glej podpogl. 5.1.6.

5.2. Organizacijska struktura izdajatelja oz. overitelja

5.2.1. Organizacija overitelja in zaupanja vredne vloge

(1) Operativno, organizacijsko in strokovno pravilno delovanje overitelja na MJU vodi pooblaščena oseba overitelja na MJU, ki jo za opravljanje navedenih nalog pooblasti vodja notranje organizacijske enote v okviru Ministrstva za javno upravo, ki je odgovorna za upravljanje digitalnih potrdil (v nadaljevanju *vodja NOE*).

(2) Med pooblaščene osebe overitelja na MJU spadajo zaposleni pri overitelju na MJU.

(3) Zaposleni pri overitelju na MJU so razporejeni v šest organizacijskih skupin, ki pokrivajo naslednja vsebinska področja:
- upravljanje overitelja,
- upravljanje s potrdili,
- upravljanje z infrastrukturo,
- varovanje in kontrola,
- notranje preverjanje skladnosti,
- pravno-administrativno.

(4) Zaupanja vredne vloge opravljajo zaposleni, ki izvajajo naloge s sledečih vsebinskih področij:
- upravljanje overitelja,
- upravljanje s potrdili,
- upravljanje z infrastrukturo,
- varovanje in kontrola.

Organizacijska skupina	Vloga	Osnovne naloge	Število oseb
Upravljanje overitelja	Upravljavec sistema	– Strategija delovanja overitelja na MJU – Določevanje prvega varnostnega inženirja – Operativno vodenje overitelja na MJU	3
Upravljanje s potrdili	Prvi varnostni inženir	– Določevanje in izvajanje pravil varnega delovanja sistema za podeljevanje potrdil – Določevanje drugih varnostnih inženirjev	1
	Drugi varnostni inženirji	– Določevanje in izvajanje pravil varnega delovanja sistema za podeljevanje potrdil	2
	Administratorji potrdil	– Upravljanje s potrdili (zaradi posebnosti izdajatelja SI-TRUST Root vlogo opravljajo varnostni inženirji)	2
Upravljanje z infrastrukturo	Sistemski administrator	– Upravljanje s operacijskim sistemom (nameščanje, konfiguracija, vzdrževanje…) – Upravljanje s telekomunikacijami (sistem za preprečevanje in odkrivanje vdorov, požarna pregrada, ...)	2
Varovanje in kontrola	Varnostni administrator	– Pregled dnevnikov	1

		– Vzdrževanje varnostnih kopij	
Notranje preverjanje skladnosti	Notranji revizor		1
Pravno-administrativno	Pravnik		1

(5) Upravni odbor overitelja na MJU sestavljajo upravljavec sistema, varnostni inženir, pravnik in vodja NOE.

(6) Naloge upravnega odbora overitelja na MJU so:
- imenovanje zaposlenih, ki izvajajo zaupanja vredne vloge,
- priprava sprememb in novih verzij politike,
- izvajanje ugotavljanja skladnosti v skladu z eIDAS,
- odločanje o izdaji in preklicu potrdil za podrejene in povezane izdajatelje,
- druge naloge upravljanja Državnega centra za storitve zaupanja.

5.2.2. Število oseb za posamezne vloge

(1) Posamezne občutljive naloge mora skladno z veljavno zakonodajo in Interno politiko overitelja na MJU opravljati več oseb hkrati.

(2) Na infrastrukturi je zagotovljeno, da varnostne ali kritične postopke odobrita dve pooblaščeni osebi istočasno.

(3) Navedeno število oseb v tabeli v podpogl. 5.2 predstavlja minimalno število oseb.

5.2.3. Izkazovanje istovetnosti za opravljanje posameznih vlog

Izkazovanje istovetnosti in pravice dostopov za opravljanje posameznih nalog skladno z vlogo posamezne organizacijske skupine kot tudi za opravljanje nalog prijavne službe je zagotovljena z varnostnimi mehanizmi in kontrolnimi postopki na programski opremi overitelja na MJU.

5.2.4. Nezdružljivost vlog

(1) Vse organizacijske skupine overitelja na MJU, navedene v tabeli podpogl. 5.2, so med seboj nezdružljive.

(2) Ob pomanjkanju ustrezno usposobljenega kadra se lahko zaradi podobne vrste opravil združi osebje določenih skupin z enakimi oz. podobnimi privilegiji delovanja.

(3) Vloge posameznih organizacijskih skupin so določene z Interno politiko overitelja na MJU.

5.3. Nadzor nad osebjem

V skladu z veljavno zakonodajo so podrobnejša določila glede nadzora osebja določena v Interni politiki overitelja na MJU.

5.3.1. Potrebne kvalifikacije in izkušnje osebja ter njegova primernost

(1) Osebje overitelja na MJU ima skladno z zahtevami veljavne zakonodaje ustrezne kvalifikacije in izkušnje ter

je skladno z zahtevami veljavne zakonodaje primerno za opravljanje svojih nalog.

(2) Pooblaščene osebe overitelja na MJU pred pričetkom opravljanja nalog za potrebe overitelja na MJU podpišejo izjavo o opravljanju nalog s posebnimi odgovornostmi.

(3) Zaposleni pri overitelju na MJU, ki opravljajo zaupanja vredne vloge:
- morajo biti za opravljanje teh vlog imenovani s strani upravnega odbora overitelja na MJU,
- ne smejo opravljati drugih nalog, ki bi bile v nasprotju z opravljanjem nalog pri overitelju na MJU,
- ne smejo biti na prejšnjih podobnih dolžnostih (npr. skrbnik kriptografskih naprav, varnostni inženir) razrešeni nalog zaradi malomarnosti ali neizpolnjevanja obveznosti in
- morajo imeti dovoljenje za dostop do tajnih podatkov najmanj stopnje ZAUPNO.

5.3.2. Preverjanje primernosti osebja

(1) Preverjanje primernosti osebja overitelja na MJU se pred sklenitvijo delovnega razmerja izvede s strani kadrovske službe Ministrstva za javno upravo skladno z veljavno zakonodajo, ki velja za javne uslužbence.

(2) Preverjanje primernosti osebja overitelja na MJU, ki opravlja zaupanja vredne vloge, se ob pridobitvi dovoljenja za dostop do tajnih podatkov izvaja s strani organa, pristojnega po Zakonu o tajnih podatkih (ZTP, Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10 in 60/11).

5.3.3. Izobraževanje osebja

Osebam, ki opravljajo naloge zgoraj navedenih organizacijskih skupin in naloge prijavne službe, se zagotavlja vsa potrebna izobraževanja.

5.3.4. Zahteve za redna usposabljanja

Osebje se usposablja glede na potrebe oz. novosti v zvezi z delovanjem infrastrukture korenskega izdajatelja SI-TRUST Root.

5.3.5. Menjava nalog

Ni predpisana.

5.3.6. Sankcije

Sankcije v primeru nepooblaščenega ali malomarnega izvajanja nalog se za pooblaščene osebe overitelja na MJU izvajajo skladno z veljavno zakonodajo, ki velja za javne uslužbence in drugo veljavno zakonodajo.

5.3.7. Zahteve za zunanje izvajalce

Za morebitne zunanje izvajalce veljajo enake zahteve kot za pooblaščene osebe overitelja na MJU.

5.3.8. Dostop osebja do dokumentacije

Pooblaščenim osebam overitelja na MJU je na voljo vsa potrebna dokumentacija skladno z njihovimi zadolžitvami in nalogami.

5.4. Varnostni pregledi sistema

(1) Korenski izdajatelj SI-TRUST Root ima skladno z veljavno zakonodajo vzpostavljen stalen nadzor delovanja svoje infrastrukture, v okviru katerega se preverja:
- fizična varnost informacijsko-komunikacijske infrastrukture,
- nemoteno delovanje vseh varnostnih sistemov,
- nemoteno delovanje vseh informacijsko-komunikacijskih sistemov in
- ali je v vmesnem času prišlo do vdora ali poskusa vdora nepooblaščenih oseb do opreme ali podatkov.

(2) Podrobni podatki o tem so skladno z veljavno zakonodajo določeni v Interni politiki overitelja na MJU.

5.4.1. Vrste beleženih dogodkov

(1) Korenski izdajatelj SI-TRUST Root skladno z veljavno zakonodajo beleži naslednje vrste dogodkov:
- dogodke na operacijskem sistemu, programski in strojni opremi izdajatelja,
- dogodke na operacijskih sistemih, programski in strojni opremi elementov komunikacijskega sistema,
- dogodke v zvezi s ključi izdajatelja,
- dogodke v zvezi z ključi in digitalnimi potrdili imetnikov (izdaja, prevzem, obnova, preklic, odkrivanje kopije ključev za dešifriranje),
- dogodke v zvezi z varnostno politiko in upravljanjem informacijskega sistema izdajatelja,
- dogodke v zvezi z varnostno politiko in upravljanjem komunikacijskega sistema.

(2) Korenski izdajatelj SI-TRUST Root zbira in beleži v elektronski ali pisni obliki tudi podatke, ki vplivajo na varnost, niso pa del informacijsko-komunikacijskega sistema izdajatelja:
- dogodke v zvezi s fizičnim dostopom do sistemov izdajatelja ter fizično lokacijo,
- kadrovske spremembe osebja overitelja na MJU,
- dogodke, povezane z uničevanjem občutljivega materiala (na primer kriptografskega materiala oziroma ključev in nosilcev ključev, aktivacijskih podatkov, osebnih podatkov o imetnikih).

(3) Dnevniki beleženih dogodkov v pisni obliki ali elektronski obliki se hranijo v varovanih prostorih overitelja na MJU.

5.4.2. Pogostost pregledov dnevnikov beleženih dogodkov

(1) Korenski izdajatelj SI-TRUST Root opravlja redne varnostne preglede svoje infrastrukture, pri čemer uporablja nadzorne in alarmne sisteme za sprotno obveščanje o dogodkih.

(2) Osebje overitelja na MJU pregleduje dnevnike beleženih dogodkov ob vsakem prejetem opozorilu iz nadzornih sistemov. Pregled vključuje:
- preverjanje integritete dnevnikov,
- pregled zapisov v dnevniku ter
- analizo in poročanje o relevantnih dogodkih - razreševanje problemov.

5.4.3. Čas hrambe dnevnikov beleženih dogodkov

(1) Dnevniki beleženih dogodkov v zvezi s ključi in digitalnimi potrdili se hranijo vsaj sedem (7) let po poteku potrdila, na katerega se dnevniški zapis nanaša.

(2) Ostali dnevniki beleženih dogodkov se hranijo vsaj sedem (7) let po nastanku dogodka.

(3) Dnevniki beleženih dogodkov iz prejšnjega odstavka, ki vsebujejo osebne podatke, se hranijo v skladu z veljavno zakonodajo.

5.4.4. Zaščita dnevnikov beleženih dogodkov

(1) Dnevniki so varovani v skladu z varnostnimi mehanizmi, ki zagotavljajo najvišji nivo varnosti.

(2) Podrobnosti so v skladu z veljavno zakonodajo določene v Interni politiki overitelja na MJU.

5.4.5. Varnostne kopije dnevnikov beleženih dogodkov

(1) Varnostne kopije dnevnikov se izvajajo dnevno v okviru rednega varnostnega kopiranja sistemov.

(2) Podrobnosti so v skladu z veljavno zakonodajo določene v Interni politiki overitelja na MJU.

5.4.6. Zbiranje podatkov za dnevnike beleženih dogodkov

(1) Podatki se zbirajo bodisi avtomatsko ali pa ročno, odvisno od vrste podatkov.

(2) Podrobnosti so v skladu z veljavno zakonodajo določene v Interni politiki overitelja na MJU.

5.4.7. Obveščanje povzročitelja dogodka

Povzročitelja dogodkov ni potrebno obveščati.

5.4.8. Ocena ranljivosti sistema

(1) Analizo dnevnikov in nadzor nad izvajanjem vseh postopkov redno izvajajo pooblaščene osebe overitelja na MJU ali pa se to izvaja avtomatsko z drugimi varnostnimi mehanizmi na vseh računalniško-komunikacijskih napravah v pristojnosti overitelja na MJU.

(2) Ocena ranljivosti se izvaja na podlagi analize dnevnikov in ugotovitev nadzora nad izvajanjem postopkov.

(3) Podrobnosti so v skladu z veljavno zakonodajo določene v Interni politiki overitelja na MJU.

5.5. Arhiviranje podatkov

5.5.1. Vrste arhiviranih podatkov

Korenski izdajatelj SI-TRUST Root skladno z veljavno zakonodajo hrani naslednje podatke oz. dokumente:

- dnevnike,
- zapisnike,
- vsa dokazila o opravljenem preverjanju istovetnosti oz. drugih podatkov o imetnikih,
- sklenjene medsebojne dogovore oz. pogodbe,
- vse zahtevke,
- izdana potrdila in register preklicanih potrdil,
- politike delovanja,
- objave in obvestila korenskega izdajatelja SI-TRUST Root ter
- druge dokumente v skladu z veljavnimi predpisi.

5.5.2. Čas hrambe

(1) Arhivirani podatki v zvezi s ključi in digitalnimi potrdili se hranijo vsaj sedem (7) let po poteku potrdila, na katerega se podatek nanaša.

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

(3) Arhivirani podatki iz prejšnjega odstavka, ki vsebujejo osebne podatke, se hranijo v skladu z veljavno zakonodajo.

5.5.3. Zaščita arhiviranih podatkov

(1) Arhivirani podatki, ki sodijo v dokumentarno gradivo (zahtevki imetnikov, dogovori in pogodbe ter dnevniki beleženih dogodkov v pisni obliki), se hranijo in arhivirajo v skladu s postopki dela z dokumentarnim gradivom na MJU.

(2) Arhivirani podatki, ki se beležijo v okviru informacijskega sistema (avtomatsko generirani dnevniki beleženih dogodkov, digitalna potrdila, registri preklicanih potrdil ter zasebni dešifrirni ključi), se nahajajo na vsaj dveh kopijah na ločenih lokacijah.

(3) V skladu z veljavno zakonodajo je podrobno to določeno v Interni politiki overitelja na MJU.

5.5.4. Varnostno kopiranje arhiviranih podatkov

(1) Za podatke, ki sodijo v dokumentarno gradivo (zahtevki imetnikov, dogovori in pogodbe ter dnevniki beleženih dogodkov v pisni obliki), se zagotavlja razpoložljivost v skladu s postopki dela z dokumentarnim gradivom na MJU.

(2) Ob izdelavi arhiva podatkov, ki se beležijo v okviru informacijskega sistema (avtomatsko generirani dnevniki beleženih dogodkov, digitalna potrdila, registri preklicanih potrdil ter zasebni dešifrirni ključi), se izdela varnostna kopija. Kopija arhiviranih podatkov se varno hrani na dveh fizičnih lokacijah.

(3) Podrobnosti o tem so v skladu z veljavno zakonodajo določene v Interni politiki overitelja na MJU.

5.5.5. Zahteva po časovnem žigosanju

Ni predpisana.

5.5.6. Način zbiranja arhiviranih podatkov

(1) Podatki se zbirajo na način, skladen z vrsto dokumenta.

(2) V skladu z veljavno zakonodajo je to podrobno določeno v Interni politiki overitelja na MJU.

5.5.7. Postopek za dostop do arhiviranih podatkov in njihova verifikacija

(1) Dostop do arhiviranih podatkov je dovoljen:
- upravnemu odboru overitelja na MJU,
- pooblaščenim osebam overitelja na MJU in
- za potrebe izvajanja inšpekcijskega nadzora.

(2) V skladu z veljavno zakonodajo je to podrobno določeno v Interni politiki overitelja na MJU.

5.6. Obnova izdajateljevega potrdila

(1) Imetniki in drugi udeleženci bodo o obnovi in postopku posredovanja novega digitalnega potrdila pravočasno obveščeni.

(2) Povezani in podrejeni izdajatelji določijo obnovo svojega potrdila s svojo politiko delovanja.

5.7. Okrevalni načrt

5.7.1. Postopek v primeru vdorov in zlorabe

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

5.7.2. Postopek v primeru okvare strojne in programske opreme ali podatkov

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

5.7.3. Postopek v primeru ogroženega zasebnega ključa izdajatelja

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

5.7.4. Okrevalni načrt

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

5.8. Prenehanje delovanja izdajatelja

Če bo overitelj na MJU prenehal z opravljanjem svoje dejavnosti ali korenski izdajatelj SI-TRUST Root prenehal z izdajanjem potrdil, bo ukrepal skladno z veljavno zakonodajo ter morebitnim medsebojnim dogovorom oz. pogodbo

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev ključev

6.1.1. Generiranje ključev

(1) Generiranje para ključev korenskega izdajatelja SI-TRUST Root za podpisovanje in overjanje je formalen in kontroliran postopek ob namestitvi programske opreme SI-TRUST Root, o katerem se vodi poseben zapisnik (dokument »Zapisnik postopka generiranja ključev korenskega izdajatelja SI-TRUST Root«). Zapisnik postopka zagotavlja celovitost in revizijsko sled izvedbe postopka, zato se izvaja po natančno pripravljenih navodilih.

(2) Zapisnik postopka se varno shrani.

(3) Morebitne kasnejše spremembe v avtorizacijah ali pomembne spremembe nastavitev informacijskega sistema SI-TRUST Root, ki so opravljene ob vzpostavitvi sistema, se dokumentirajo v posebnem zapisniku oz. v ustreznem dnevniku.

(4) Za generiranje para ključev korenskega izdajatelja SI-TRUST Root se uporabi strojni varnostni modul (glej podpogl. 6.2.1).

(5) Imetnikov par ključev se generira pri imetniku predvidoma na strojnem varnostnem modulu (glej podpogl. 6.2.1).

6.1.2. Dostava zasebnega ključa imetnikom

Imetnikov zasebni ključ se generira pri imetniku in se ne prenaša.

6.1.3. Dostava javnega ključa izdajatelju potrdil

Imetnik v postopku prevzema dostavi svoj javni ključ v podpis korenskemu izdajatelju SI-TRUST Root na način, ki je določen v Interni politiki delovanja overitelja na MJU in morebitnem medsebojnem dogovoru oz. pogodbi.

6.1.4. Dostava izdajateljevega javnega ključa tretjim osebam

Potrdilo z javnim ključem korenskega izdajatelja SI-TRUST Root je objavljeno v repozitoriju overitelja na MJU (glej podpogl. 2).

6.1.5. Dolžina ključev

Dolžina ključev za korenskega izdajatelja SI-TRUST Root in minimalna dopustna dolžina ključev za imetnike je

podana v tabeli spodaj.

subjekt	Dolžina ključa po RSA [bit]
Korenski izdajatelj SI-TRUST Root	3072
Podrejeni oz. povezani izdajatelj	najmanj 2048
Sistem OCSP	2048

6.1.6. Generiranje in kakovost parametrov javnih ključev

Kvaliteta parametrov ključa korenskega izdajatelja SI-TRUST Root je zagotovljena s strani proizvajalca strojne opreme za varno shranjevanje zasebnih ključev, ki uporablja generator naključnih števil (angl. *random number generator*) v skladu s standardom FIPS 140-2 Level 3.

6.1.7. Namen ključev in potrdil

(1) Namen uporabe ključev oz. potrdil je v skladu z *X.509 v.3* določen v potrdilu v polju *uporaba ključa* (angl. *keyUsage)* in *razširjena uporaba ključa* (angl. *extended keyUsage)*.

(2) Za podpis digitalnih potrdil in registra preklicanih potrdil je namenjen zasebni ključ korenskega izdajatelja SI-TRUST Root, za overjanje pa javni ključ v izdajateljevem potrdilu.

(3) Profil izdajateljevega potrdila in potrdil imetnikov je podan v podpogl. 7.

6.2. Zaščita zasebnega ključa in varnostni moduli

6.2.1. Standardi za kriptografski modul

(1) Zasebni ključ korenskega izdajatelja SI-TRUST Root se generira in hrani na strojni opremi za varno shranjevanje zasebnih ključev (ali strojni varnostni modul, HSM angl. *Hardware Security Module*), ki izpolnjuje zahteve v skladu s standardom FIPS 140-2 Level 3.

(2) Oprema, ki jo uporabljajo imetniki, mora ustrezati svetovno uveljavljenim varnostnim in tehničnim standardom, pri čemer mora izpolnjevati vsaj enega izmed pogojev, določenih v standardu ETSI EN 319 411-1, poglavje 6.5.2.

6.2.2. Nadzor zasebnega ključa s strani pooblaščenih oseb

Določila glede dostopa do zasebnega ključa korenskega izdajatelja SI-TRUST Root so v skladu z veljavno zakonodajo določena v Interni politiki overitelja na MJU.

6.2.3. Odkrivanje kopije zasebnega ključa

Ni podprto.

6.2.4. Varnostna kopija zasebnega ključa

(1) Korenski izdajatelj SI-TRUST Root zagotavlja varnostno kopijo svojega zasebnega ključa. Podrobnosti so določene v Interni politiki overitelja na MJU.

(2) Imetnik mora poskrbeti za varnostno kopijo svojega zasebnega ključa.

6.2.5. Arhiviranje zasebnega ključa

Ni podprto.

6.2.6. Prenos zasebnega ključa iz/v kriptografski modul

(1) Prenos zasebnega ključa korenskega izdajatelja SI-TRUST Root iz strojnega varnostnega modula se izvede v šifrirani obliki po generiranju para ključev korenskega izdajatelja SI-TRUST Root z namenom izdelave varnostne kopije zasebnega ključa (glej podpogl. 6.2.4). Prenos zasebnega ključa v strojni varnostni modul se izvede v šifrirani obliki v primeru zamenjave ali ponastavitve varnostnega modula.

(2) Prenos zasebnega ključa iz oziroma v kriptografski modul se izvede z odobritvijo vsaj dveh pooblaščenih oseb overitelja na MJU.

(3) Podrobnosti o prenosu izdajateljevega zasebnega ključa so določene v Interni politiki overitelja na MJU.

(4) Če strojni varnostni modul imetnika omogoča prenos zasebnega ključa iz/v modul, se mora prenos izvesti v šifrirani obliki.

6.2.7. Zapis zasebnega ključa v kriptografskem modulu

Zasebni ključ je v strojnem varnostnem modulu varovan z mehanizmi v skladu s standardom FIPS 140-2 Level 3.

6.2.8. Postopek za aktiviranje zasebnega ključa

(1) Aktiviranje zasebnega ključa korenskega izdajatelja SI-TRUST Root se izvede ob zagonu programske opreme izdajatelja in poteka v skladu z določili Interne politike overitelja na MJU.

(2) Imetniki morajo zagotoviti varno aktiviranje svojega zasebnega ključa.

6.2.9. Postopek za deaktiviranje zasebnega ključa

(1) Ob zaustavitvi delovanja korenskega izdajatelja SI-TRUST Root programska oprema SI-TRUST Root deaktivira zasebni ključ SI-TRUST Root.

(2) Imetniki morajo uporabljati tako programsko opremo, ki ob zaustavitvi delovanja izdajatelja deaktivira njegov zasebni ključ.

6.2.10. Postopek za uničenje zasebnega ključa

(1) Postopek za uničenje zasebnega ključa korenskega izdajatelja SI-TRUST Root poteka na varen način skladno z določili Interne politike overitelja na MJU. Zasebni ključ se uniči tako, da ga ni mogoče restavrirati.

(2) Uničenje zasebnih ključev na strani imetnikov je v njihovi pristojnosti.

6.2.11. Lastnosti kriptografskega modula

Strojni varnostni modul ustreza standardom, podanim v podpogl. 6.2.

6.3. Ostali vidiki upravljanja ključev

6.3.1. Arhiviranje javnega ključa

Korenski izdajatelj SI-TRUST Root arhivira svoj javni ključ in javne ključe imetnikov, kot je podano v podpogl. 5.5.

6.3.2. Obdobje veljavnosti potrdila in ključev

(1) Veljavnosti digitalnih potrdil, ki jih za izdajatelje znotraj overitelja na MJU izdaja korenski izdajatelj SI-TRUST Root, so sledeče:

- za podrejene izdajatelje: dvajset (20) let oz. do poteka veljavnosti korenskega potrdila SI-TRUST Root,
- za enostransko povezane izdajatelje: do poteka veljavnosti osnovnega potrdila povezanega izdajatelja oz. do poteka veljavnosti korenskega potrdila SI-TRUST Root.

(2) Veljavnost digitalnih potrdil pri povezovanju z zunanjimi izdajatelji je do poteka veljavnosti osnovnega potrdila povezanega izdajatelja oz. do poteka veljavnosti korenskega potrdila SI-TRUST Root.

(3) Zunanji izdajatelj in SI-TRUST Root se lahko z medsebojnim dogovorom oz. pogodbo dogovorita tudi za drugačen čas veljavnosti potrdil.

(4) Veljavnost ključev korenskega izdajatelja SI-TRUST Root je do 19.01.2038.

(5) Veljavnost ključev potrdila za sistem OCSP je tri (3) leta.

6.4. Gesla za dostop do zasebnega ključa

6.4.1. Generiranje gesel

Pooblaščene osebe izdajatelja za dostop do zasebnega ključa SI-TRUST Root uporabljajo močna gesla, s katerimi ravnajo v skladu z Interno politiko overitelja na MJU.

6.4.2. Zaščita gesel

Gesla pooblaščenih oseb korenskega izdajatelja SI-TRUST Root za dostop do zasebnega ključa korenskega

izdajatelja SI-TRUST Root se shranijo v skladu z Interno politiko overitelja na MJU.

6.4.3. Drugi vidiki gesel

Niso predpisani.

6.5. Varnostne zahteve za računalniško opremo izdajatelja

6.5.1. Specifične tehnične varnostne zahteve

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

6.5.2. Nivo varnostne zaščite

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

6.6. Tehnični nadzor življenjskega cikla izdajatelja

6.6.1. Nadzor razvoja sistema

(1) Korenski izdajatelj SI-TRUST Root uporablja programsko opremo proizvajalca Entrust, ki je certificirana v skladu s Common Criteria EAL4+.

(2) Podrobne tehnične zahteve so določene v Interni politiki overitelja na MJU.

(3) Imetniki morajo uporabljati programsko opremo, ki je certificirana v skladu s Common Criteria vsaj EAL4+ ali je vzpostavljena v skladu s standardom ETSI EN 319 401.

6.6.2. Upravljanje varnosti

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

6.6.3. Nadzor življenjskega cikla

V skladu z veljavno zakonodajo je to določeno v Interni politiki overitelja na MJU.

6.7. Varnostna kontrola računalniške mreže

(1) Sistem korenskega izdajatelja SI-TRUST Root je večino časa neaktiven in se aktivira le občasno z namenom izdaje posameznega digitalnega potrdila ali seznama preklicanih potrdil. V času delovanja so omogočeni le mrežni protokoli, ki so nujno potrebni za povezavo sistema do strojnega varnostnega modula in do imenika LDAP v notranjem mrežnem segmentu, ločenim od ostalega omrežja.

(2) V skladu z veljavno zakonodajo je to podrobneje določeno v Interni politiki overitelja na MJU.

6.8. Časovno žigosanje

Ni predpisano.

7. PROFIL POTRDIL, REGISTRA PREKLICANIH POTRDIL IN SPROTNEGA PREVERJANJA STATUSA POTRDIL

7.1. Profil potrdil

7.1.1. Različica potrdil

Digitalna potrdila, ki jih izdaja korenski izdajatelj SI-TRUST Root in tudi njemu podrejeni in povezani izdajatelji, sledijo standardu *X.509*, in sicer različici 3, skladno z RFC 5280.

7.1.2. Profil potrdil z razširitvami

7.1.2.1.Profil potrdila SI-TRUST Root

Profil potrdila SI-TRUST Root je predstavljen v podpogl. 1.

7.1.2.2.Profil potrdila za podrejene in povezane izdajatelje

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Number*	*enolična interna številka potrdila-celo število (32 bitov entropije)*
Algoritem za podpis, angl. *Signature algorithm*	sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11)
Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Veljavnost, angl. *Validity*	Not Before: <*pričetek veljavnosti po GMT*> Not After: <*konec veljavnosti po GMT*> *v formatu UTCTime* <LLMMDDuummssZ>
Imetnik, angl. *Subject*	*razločevalno ime podrejenega ali povezanega izdajatelja (glej podpogl.3.1), v obliki, primerni za izpis*
Algoritem za javni ključ, angl. *Subject Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. *RSA Public Key*	*dolžina ključa je min 2048 bitov*
Razširitve X.509v3	

Objava registra preklicanih potrdil, OID 2.5.29.31, angl. *CRL Distribution Points*	Url: http://www.ca.gov.si/crl/si-trust-root.crl Url: ldap://x500.gov.si/cn=SI-TRUST%20Root,oi=VATSI-17659957,o=Republika%20Slovenija,c=SI?certificateRevocationList c=SI, o=Republika Slovenija, oid=VATSI-17659957, cn= SI-TRUST Root, cn=CRL<*zaporedna številka registra*>
Uporaba ključa, OID 2.5.29.15, *angl. Key Usage*	Kritično (Critical) Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. *Authority Key Identifier*	*identifikator izdajateljevega ključa*
Identifikator imetnikovega ključa, OID 2.5.*29.14,* *angl. Subject Key Identifier*	*identifikator imetnikovega ključa*
Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Politika, pod katero je bilo izdano potrdilo, OID 2.5.29.32, angl. *certificatePolicies*	V potrdilih, izdanih izdajateljem v okviru Overitelja na MJU: Certificate Policy: PolicyIdentifier=2.5.29.32.0 (»anyPolicy«) [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ca.gov.si/cps/ V potrdilih, izdanih zunanjim izdajateljem: Certificate Policy: PolicyIdentifier= *nabor identifikacijskih oznak politik, ki se uporabljajo v potrdilih, izdanih končnim uporabnikom* [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ca.gov.si/cps/
Dostop do podatkov o izdajatelju, OID 1.3.6.1.5.5.7.1.1, angl. *Authority Information Access*	Access Method:OCSP (1.3.6.1.5.5.7.48.1) Access Location: URL=http://ocsp.ca.gov.si Access Method:CaIssuer (1.3.6.1.5.5.7.48.2) Access Location: URL=http://www.ca.gov.si/crt/si-trust-root.crt
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA-1*	*razpoznavni odtis potrdila po SHA-1*
Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA-256*	*razpoznavni odtis potrdila po SHA-256*

(1) Kot kritični (angl. *critical*) sta v potrdilih označeni polji:
- uporaba ključa (angl. *Key Usage*) in
- osnovne omejitve (angl. *Basic Constraints*).

(2) V polju »osnovne omejitve« (angl. *Basic Constraints*) se določi tudi nastavitev »omejitev dolžine poti« (angl. *Path Length Constraint*), katere vrednost je »none«.

(3) Profili digitalnih potrdil, ki jih izdajajo podrejeni in povezani izdajatelji, so določeni v njihovih politikah delovanja.

7.1.3. Identifikacijske oznake algoritmov

(1) Potrdila, ki jih izdaja SI-TRUST Root, so s strani izdajatelja podpisana z algoritmom, določenim v polju s*ignature algorithm*: vrednost »sha256WithRSAEncryption«, identifikacijska oznaka: OID 1.2.840.113549.1.1.11.

(2) Celoten nabor algoritmov, formatov podatkov in protokolov je na razpolago pri pooblaščenih osebah korenskega izdajatelja SI-TRUST Root.

(3) SI-TRUST Root lahko podpira tudi druge algoritme, če je to sklenjeno v morebitnem medsebojnem dogovoru oz. pogodbi z imetnikom.

7.1.4. Oblika imen

Glej podpogl. 2.

7.1.5. Omejitve glede imen

Omejitve glede imen (polje v potrdilu angl. *nameConstraints*) niso predpisane.

7.1.6. Oznaka politike potrdila

Glej podpogl. 7.1.2.

7.1.7. Uporaba razširitvenega polja za omejitev uporabe politik

Omejitve uporabe politik (angl. *Policy constraints*) se ne uporabljajo.

7.1.8. Oblika in obravnava specifičnih podatkov o politiki

V potrdilih, ki jih izdaja korenski izdajatelj SI-TRUST Root, se uporablja specifični podatek policyQualifiers, ki se obravnava v skladu z RFC 5280.

7.1.9. Obravnava kritičnega razširitvenega polja politike

Razširitveno polje politika (angl. *CertificatePolicies*) ni označeno kot kritično.

7.2. Profil registra preklicanih potrdil

7.2.1. Različica

(1) Register preklicanih potrdil, ki jih izdaja korenski izdajatelj SI-TRUST Root in tudi njemu podrejeni in povezani izdajatelji, ustrezajo priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:1997, vključno z ver. 2.

(2) Register preklicanih potrdil je stalno dostopen v repozitoriju (glej podpogl. 2.1):
- po protokolu LDAP in
- po protokolu HTTP.

7.2.2. Vsebina registra in razširitve

(1) Register preklicanih potrdil poleg ostalih podatkov v skladu s priporočilom *X.509* vsebuje (osnovna polja in razširitve so podrobneje prikazana v tabeli spodaj):
- identifikacijske oznake preklicanih potrdil in
- čas in datum preklica.

Naziv polja	Vrednost oz. pomen
Osnovna polja v CRL	
Različica, angl. *Version*	2
Izdajateljev podpis, angl. *Signature*	*podpis izdajatelja*
Razločevalno ime izdajatelja, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Čas izdaje CRL, angl. *thisUpdate*	Last Update: *čas izdaje po GMT*
Čas izdaje naslednjega CRL, angl. *nextUpdate*	Next Update: *čas naslednje izdaje po GMT*
Identifikacijske oznake preklicanih potrdil in čas preklica, angl. *revokedCertificate*	Serial Number: <*identifikacijska oznaka preklicanega dig. potrdila*> Revocation Date: <*čas preklica po GMT*>
Algoritem za podpis, angl. *Signature Algorithm*	sha256WithRSAEncryption
Razširitve X.509v2 CRL	
Identifikator izdajateljevega ključa, angl. *Authority Key Identifier* *(OID 2.5.29.35)*	*identifikator izdajateljevega ključa*
Številka za posamične registre (CRL1, CRL2,....), angl. *CRLnumber* *(OID 2.5.29.20)*	*zaporedna številka posamičnega registra*
Alternativno ime izdajatelja angl. *issuerAltName* *(OID 2.5.28.18)*	*se ne uporablja*
Oznaka seznama sprememb angl. *deltaCRLindicator* *(OID 2.5.29.27)*	*se ne uporablja*
Objava seznama sprememb angl. *issuingDistribuitionPoint* *(OID 2.5.29.28)*	*se ne uporablja*

(2) Preklicana digitalna potrdila, katerih veljavnost je potekla, ostanejo objavljena v registru preklicanih potrdil.

(3) Polja v CRL niso označena kot kritična.

(4) Register preklicanih digitalnih potrdil je javno objavljen v repozitoriju (glej podpogl. 2).

(5) Izdajatelj objavlja tako posamične registre kot tudi celotni register (na enem mestu).

7.3. Profil sprotnega preverjanja statusa potrdil

(1) Sprotno preverjanje statusa digitalnih potrdil je dostopno na naslovu http://ocsp.ca.gov.si.

(2) Profil sporočil OCSP (zahtevek/odgovor) storitve za sprotno preverjanje statusa potrdil je v skladu s priporočilom RFC 2560.

7.3.1. Različica

Izdajatelj SI-TRUST Root uporablja sporočila OCSP verzije 1 v skladu s priporočilom RFC 2560.

7.3.2. Razširitve sprotnega preverjanje statusa

Sporočila OCSP (zahtevek/odgovor) storitve za sprotno preverjanje statusa potrdil podpirajo razširitev Nonce, ki ni označena kot kritična.

8. INŠPEKCIJSKI NADZOR

8.1. Pogostnost inšpekcijskega nadzora

Pogostnost inšpekcijskega nadzora je v pristojnosti inšpekcijske službe, ki je pristojna v skladu z veljavno zakonodajo.

8.2. Inšpekcijska služba

(1) Izvajanje inšpekcijskega nadzora overitelja na MJU opravlja pristojna inšpekcijska služba v skladu z veljavno zakonodajo za inšpekcijski nadzor.

(2) Notranje preverjanje skladnosti delovanja izvaja notranji revizor in ostale pooblaščene osebe v okviru overitelja na MJU.

8.3. Neodvisnost inšpekcijske službe

Inšpekcijska služba je organ, pristojen v skladu z veljavno zakonodajo.

8.4. Področja inšpekcijskega nadzora

Področja nadzora so določena z veljavno zakonodajo in predpisi.

8.5. Ukrepi overitelja

V primeru ugotovljenih pomanjkljivosti ali napak si korenski izdajatelj SI-TRUST Root oz. overitelj na MJU prizadeva za odpravo le-teh v najkrajšem možnem času.

8.6. Objava rezultatov inšpekcijskega nadzora

Overitelj na MJU javno objavi povzetek sklepov inšpekcijskega nadzora na svojih spletnih straneh.

9. OSTALE POSLOVNE IN PRAVNE ZADEVE

9.1. Cenik storitev

9.1.1. Cena izdaje in obnove potrdil

Cena izdaje in obnove potrdil, ki jih korenski izdajatelj SI-TRUST Root izda zunanjim izdajateljem, se določi z medsebojnim dogovorom oz. pogodbo.

9.1.2. Cena dostopa do potrdil

(1) Dostop do imenika izdanih digitalnih potrdil korenskega izdajatelja SI-TRUST Root je brezplačen.

(2) Ker se s to politiko zahteva javnost dostopa tudi za imenike digitalnih potrdil, s katerimi upravljajo podrejeni in povezani izdajatelji, le-ti teh storitev ne zaračunavajo.

9.1.3. Cena dostopa do statusa potrdila in registra preklicanih potrdil

(1) Dostop do statusa potrdila in registra preklicanih digitalnih potrdil korenskega izdajatelja SI-TRUST Root je brezplačen.

(2) Ker se s to politiko zahteva javnost dostopa do statusa potrdila in registra preklicanih potrdil tudi za podrejene in povezane izdajatelje, le-ti teh storitev ne zaračunavajo.

9.1.4. Cene drugih storitev

Stroške potrebne strojne ali programske opreme, ki jo zahteva oz. priporoča SI-TRUST Root za varno shranjevanje in uporabo potrdil, krije imetnik potrdila.

9.1.5. Povrnitev stroškov

Ni predpisana.

9.2. Finančna odgovornost

9.2.1. Zavarovalniško kritje

Ministrstvo za javno upravo ima glede delovanja overitelja na MJU ustrezno zavarovano svojo odgovornost v skladu z veljavno zakonodajo.

9.2.2. Drugo kritje

Ni predpisano.

9.2.3. Zavarovanje imetnikov

Ni predpisano.

9.3. Varovanje poslovnih podatkov

9.3.1. Varovani podatki

(1) Korenski izdajatelj SI-TRUST Root kot zaupne obravnava naslednje podatke:
- vse zahtevke za pridobitev potrdila ali druge storitve,
- vse morebitne zaupne podatke v zvezi s finančnimi obveznostmi,
- vse morebitne zaupne podatke, ki so predmet medsebojne pogodbe z organizacijo ali tretjimi osebami ter
- vse ostale zadeve, ki so v skladu z veljavno zakonodajo zavedene v Interni politiki overitelja na MJU.

(2) Z vsemi zaupnimi podatki o organizacijah ali tretjih osebah, ki so nujno potrebni za storitve upravljanja s potrdili, korenski izdajatelj SI-TRUST Root ravna v skladu z veljavno zakonodajo.

9.3.2. Nevarovani podatki

Korenski izdajatelj SI-TRUST Root javno objavlja samo take poslovne podatke, ki v skladu z veljavno zakonodajo niso zaupne narave.

9.3.3. Odgovornost glede varovanja poslovnih podatkov

Korenski izdajatelj SI-TRUST Root posreduje le tiste podatke o organizacijah, ki so navedeni v potrdilu ali morebitnem medsebojnem dogovoru oz. pogodbi. Drugi podatki se lahko posredujejo le v primeru, če se posebej zahtevajo za izvajanje specifičnih storitev oz. aplikacij, povezanih s potrdili, ter je to na zahtevku za pridobitev potrdila ali kasneje v pisni obliki odobril imetnik potrdila, ali na zahtevo pristojnega sodišča ali upravnega organa. Podatki se posredujejo tudi brez pisne privolitve, če to določa zakonodaja oz. veljavni predpisi.

9.4. Varovanje osebnih podatkov

9.4.1. Načrt varovanja osebnih podatkov

Z vsemi osebnimi in zaupnimi podatki o imetnikih potrdil, ki so nujno potrebni za storitve upravljanja s potrdili, korenski izdajatelj SI-TRUST Root ravna v skladu z veljavno zakonodajo.

9.4.2. Varovani osebni podatki

Varovani podatki so vsi osebni podatki, ki jih korenski izdajatelj SI-TRUST Root pridobi na zahtevkih za svoje storitve ali v morebitnem medsebojnem dogovoru oz. pogodbi oz. v ustreznih registrih za dokazovanje istovetnosti imetnika.

9.4.3. Nevarovani osebni podatki

Drugih morebitnih nevarovanih osebnih podatkov, razen teh, ki so navedeni v potrdilu in registru preklicanih potrdil, ni.

9.4.4. Odgovornost glede varovanja osebnih podatkov

Overitelj na MJU je odgovoren v skladu z Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo) in drugo veljavno zakonodajo glede varovanja osebnih podatkov.

9.4.5. Pooblastilo glede uporabe osebnih podatkov

Ni predpisano.

9.4.6. Posredovanje osebnih podatkov na uradno zahtevo

Korenski izdajatelj SI-TRUST Root ne posreduje osebnih podatkov, razen na zahtevo pristojnega sodišča ali upravnega organa.

9.4.7. Druga določila glede posredovanja osebnih podatkov

Niso predpisana.

9.5. Določbe glede pravic intelektualne lastnine

Določbe glede avtorskih, sorodnih in drugih pravic intelektualne lastnine v zvezi s korenskim izdajateljem SI-TRUST Root:

- na pričujoči politiki pripadajo vse pravice overitelju na MJU,
- na imeniku potrdil in registru preklicanih potrdil pripadajo vse pravice overitelju na MJU,
- na vseh podatkih v potrdilih pripadajo vse pravice overitelju na MJU,
- na zasebnem ključu za podpisovanje pripadajo vse pravice imetniku.

9.6. Obveznosti in odgovornosti

9.6.1. Obveznosti in odgovornosti izdajatelja

(1) Korenski izdajatelj SI-TRUST Root oz. overitelj na MJU je dolžan:
- delovati v skladu s svojimi notranjimi pravili in ostalimi veljavnimi predpisi in zakonodajo,
- delovati v skladu z mednarodnimi priporočili,
- objavljati vse pomembne dokumente, ki določajo njegovo delovanje (politike delovanja, zahtevke ipd.),
- objavljati na svojih spletnih straneh vse informacije o tistih spremembah glede dejavnosti overitelja na MJU, ki kakorkoli vplivajo na imetnike potrdil in tretje osebe,
- spoštovati določila glede varnega ravnanja z osebnimi, poslovnimi in zaupnimi podatki o overitelju, imetnikih potrdil ali tretjih osebah,
- preklicati potrdilo in objaviti preklicano potrdilo v registru preklicanih potrdil, ko ugotovi, da so podani razlogi po tej politiki ali drugih veljavnih predpisih,
- izdajati potrdila v skladu s to politiko in ostalimi predpisi ter priporočili.

(2) Korenski izdajatelj SI-TRUST Root oz. overitelj na MJU je dolžan:
- zagotoviti pravilnost podatkov izdanih potrdil,
- pred izdajo potrdila preveriti, da ima imetnik potrdila zasebni ključ, ki pripada v potrdilu navedenemu javnemu ključu (glej podpogl. 3.2),
- zagotoviti pravilnost registra preklicanih potrdil,
- zagotoviti pravilnost delovanja sprotnega preverjanja statusa potrdil,
- zagotoviti enoličnost razločevalnih imen,
- zagotoviti primerno fizično varnost prostorov in dostopov do samih prostorov izdajatelja,
- kot dober gospodar skrbeti za nemoteno delovanje in čim večjo razpoložljivost storitev,
- kot dober gospodar skrbeti za čim večjo dostopnost storitev,
- kot dober gospodar skrbeti za nemoteno delovanje vseh ostalih spremljajočih storitev,
- poskušati odpraviti nastale probleme po najboljših močeh in v najkrajšem času,
- skrbeti za optimizacijo strojne in programske opreme in
- obveščati vse ustrezne subjekte o pomembnih zadevah ter
- izpolnjevati vse druge zahteve v skladu s to politiko.

(3) Korenski izdajatelj SI-TRUST Root *oz. o*veritelj na MJU zagotavlja čim večjo dostopnost svojih storitev, in sicer 24ur/7dni/365dni, pri čemer pa se ne upošteva naslednjih primerov:
- načrtovanih in vnaprej napovedanih tehničnih ali servisnih posegov na infrastrukturi,
- nenačrtovanih tehničnih ali servisnih posegov na infrastrukturi kot posledica nepredvidenih okvar,
- tehničnih ali servisnih posegov zaradi okvare infrastrukture izven pristojnosti korenskega izdajatelja SI-TRUST Root oz overitelja na MJU in
- nedostopnosti kot posledico višje sile ali izrednih dogodkov.

(4) Vzdrževalna dela ali nadgradnje infrastrukture mora overitelj na MJU oz. SI-TRUST Root najaviti vsaj tri (3) dni pred pričetkom del.

(5) Overitelj na MJU je odgovoren za vse navedbe v tem dokumentu in za izvajanje vseh določil iz te politike.

(6) Ostale obveznosti oz. odgovornosti korenskega izdajatelja SI-TRUST Root oz. overitelja na MJU so določene v interni politiki overitelja na MJU in morebitnem medsebojnem dogovoru oz. pogodbi z imetnikom.

9.6.2. Obveznosti in odgovornosti prijavne službe

(1) Korenski izdajatelj SI-TRUST Root nima vzpostavljene prijavne službe.

(2) Upravni odbor overitelja na MJU je odgovoren za ustreznost identifikacijskih postopkov in točnost podatkov v zahtevkih.

9.6.3. Obveznosti in odgovornosti imetnika

(1) Imetnik oziroma bodoči imetnik potrdila je dolžan:
- seznaniti se s to politiko pred izdajo potrdila,
- ravnati v skladu s to politiko in določili iz morebitnega medsebojnega dogovora oz. pogodbe ter ostalimi veljavnimi predpisi,
- po prejemu oz. po prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti SI-TRUST Root oziroma zahtevati preklic potrdila,
- spremljati vsa obvestila SI-TRUST Root in ravnati v skladu z njimi,
- vse spremembe, ki so povezane s potrdilom, nemudoma sporočiti SI-TRUST Root,
- zahtevati preklic potrdila, če je bil zasebni ključ ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe,
- uporabljati potrdilo izključno za namen, določen s to politiko in morebitnim medsebojnim dogovorom oz. pogodbo,
- skrbeti za originalno podpisane dokumente in arhiv teh dokumentov.

(2) Za imetnika potrdila veljajo naslednje zahteve:
- podrejeni izdajatelj se ne sme povezovati z drugimi izdajatelji,
- povezani izdajatelj se medsebojno ne sme povezovati z drugimi povezanimi izdajatelji; ob predhodni presoji in odobritvi s strani SI-TRUST Root se izjemoma lahko povezuje z zunanjimi izdajatelji, če s tem ni ogrožena integriteta povezanega sistema.

(3) V primeru kršitve pogojev povezovanja iz prejšnjega odstavka lahko SI-TRUST Root takoj nepreklicno prekine povezavo s podrejenim oz. povezanim izdajateljem.

(4) Vsak izdajatelj, ki se povezuje preko SI-TRUST Root, ohranja vse odgovornosti v zvezi z izdajanjem digitalnih potrdil za svoje imetnike.

(5) Imetnik odgovarja za:
- nastalo škodo v primeru zlorabe potrdila od prijave preklica do preklica,
- vsako škodo, ki je bodisi posredno ali neposredno povzročena zato, ker je bila omogočena uporaba oz. zloraba potrdila s strani nepooblaščenih oseb,
- vsako drugo škodo, ki izvira iz neupoštevanja določil te politike in drugih obvestil korenskega izdajatelja SI-TRUST Root ter veljavnih predpisov.

9.6.4. Obveznosti in odgovornosti tretjih oseb

(1) Tretje osebe morajo proučiti vse zahteve in okoliščine, preden se odločijo za zanašanje na potrdila, ki jih izda SI-TRUST Root.

(2) Tretje osebe, ki se zanašajo na izdana potrdila SI-TRUST Root, morajo:
- skrbno proučiti vse možnosti tveganja in odgovornosti pri uporabi potrdil in določiti politiko za način uporabe,
- za overjanje podpisa oz. druge kriptografske operacije uporabljati programsko in strojno opremo, s katero lahko na verodostojen način preverijo vse zahteve za varno uporabo potrdil,
- obvestiti korenskega izdajatelja SI-TRUST Root, če izvedo, da so bili zasebni ključi imetnika potrdila, na katerega se zanašajo, ogroženi na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, navedeni v potrdilu,

- skrbeti za arhiv dokumentov,
- upoštevati druge določbe iz morebitnih medsebojnih dogovorov,
- upoštevati vsa navodila oz. priporočila SI-TRUST Root glede zanesljive uporabe,
- ob morebitnih napakah ali problemih takoj obvestiti korenskega izdajatelja SI-TRUST Root,
- seznaniti se s to politiko in upoštevati vsa določila glede njihove obveznosti, odgovornosti ter omejitve glede zaupanja in uporabe potrdil,
- spremljati vsa obvestila in objave korenskega izdajatelja SI-TRUST Root in ravnati v skladu z le-temi,
- upoštevati morebitna druga pravila, ki so izven pristojnosti izdajatelja in so določena drugje.

(3) Tretje osebe nosijo vse posledice, ki bi nastale zaradi morebitnega neupoštevanja določil te politike, morebitnega dogovora z overiteljem na MJU in veljavne zakonodaje.

9.6.5. Obveznosti in odgovornosti drugih subjektov

Niso predpisane.

9.7. Zanikanje odgovornosti

Overitelj na MJU ni odgovoren za škodo, ki bi nastala zaradi:

- uporabe potrdil za namen in na način, ki ni izrecno predviden v tej politiki oz. morebitnem dogovoru med imetnikom in SI-TRUST Root,
- nepravilnega ali pomanjkljivega varovanja gesel ali zasebnih ključev imetnikov, izdajanja zaupnih podatkov ali ključev tretjim osebam in neodgovornega ravnanja imetnika,
- zlorabe oz. vdora v informacijski sistem imetnika potrdila in s tem do podatkov o potrdilih s strani nepooblaščenih oseb,
- nedelovanja ali slabega delovanja informacijske infrastrukture imetnika potrdila ali tretjih oseb,
- nepreverjanja podatkov in veljavnosti potrdil,
- nepreverjanja časa veljavnosti potrdila,
- ravnanja imetnika potrdila ali tretje osebe v nasprotju z obvestili korenskega izdajatelja SI-TRUST Root, politiko, morebitnim dogovorom oz. pogodbo in drugimi predpisi,
- omogočene uporabe oz. zlorabe imetnikovega potrdila nepooblaščenim osebam,
- izdanega potrdila z napačnimi podatki in neverodostojnimi podatki ali drugih dejanj imetnika,
- uporabe potrdil ter veljavnosti potrdil ob spremembah podatkov iz potrdila ali spremembah podatkov o imetniku,
- izpada infrastrukture, ki ni v domeni upravljanja overitelja na MJU,
- podatkov, ki se podpisujejo z uporabo pripadajočih zasebnih ključev,
- ravnanja imetnikov pri uporabi potrdil, in sicer tudi v primeru, če je imetnik ali tretja oseba spoštoval vsa določila te politike in dogovora ter obvestila korenskega izdajatelja SI-TRUST Root ali druge veljavne predpise,
- uporabe in zanesljivosti delovanja strojne in programske opreme imetnikov potrdil.

9.8. Omejitev odgovornosti

Korenski izdajatelj SI-TRUST Root oz. overitelj na MJU ne prevzema odgovornosti za posamezne pravne posle, ki so sklenjeni na podlagi potrdil, izdanih s strani podrejenih oz. povezanih izdajateljev.

9.9. Poravnava škode

Za škodo odgovarja stranka, ki je le-to povzročila zaradi neupoštevanja določil iz te politike, veljavne zakonodaje in morebitnih medsebojnih dogovorov.

9.10. Veljavnost politike

9.10.1. Čas veljavnosti

Nova verzija oz. spremembe politike overitelja na MJU se sedem (7) dni pred veljavo predhodno objavi na spletnih straneh overitelja na MJU z označenim datumom začetka njene veljavnosti.

9.10.2. Konec veljavnosti politike

(1) Konec veljavnosti politike ni določen in povezan z veljavnostjo potrdil, izdanih na podlagi politike.

(2) Ob objavi nove politike ostanejo za vsa potrdila, izdana na podlagi te politike, v veljavi tista določila, ki se smiselno ne morejo nadomestiti z ustreznimi določili po novi politiki (na primer postopek, ki določa način, po katerem je bilo to potrdilo izdano ipd.).

(3) Izdajatelj lahko za posamezna določila veljavne politike izda amandmaje, kot je to podano v podpogl. 9.12.

9.10.3. Učinek poteka veljavnosti politike

(1) Ob izdaji nove politike se vsa digitalna potrdila, izdana oz. podaljšana po tem datumu, obravnavajo po novi politiki.

(2) Nova politika ne vpliva na veljavnost potrdil, ki so bila izdana po prejšnjih politikah. Taka potrdila ostanejo v veljavi do konca preteka veljavnosti, pri čemer se, kjer je to možno, obravnavajo po novi politiki.

9.11. Komuniciranje med subjekti

(1) Kontaktni podatki overitelja oz. izdajatelja so objavljeni na spletnih straneh in podani v podpogl. 1.

(2) Kontaktni podatki imetnikov oz. organizacij so podani v zahtevkih in morebitnem medsebojnem dogovoru oz. pogodbi.

(3) Kontaktni podatki tretjih oseb so podani v morebitnem medsebojnem dogovoru med tretjo osebo in overiteljem na MJU.

(4) Izdajatelj SI-TRUST Root ostale subjekte obvešča preko obvestil, objavljenih na spletnih straneh, ter preko e-pošte.

(5) Korenski izdajatelj SI-TRUST Root ter zunanji izdajatelj lahko določita način komuniciranja z medsebojnim dogovorom oz. pogodbo.

(6) Korenski izdajatelj SI-TRUST Root ter tretja oseba lahko določita način komuniciranja z medsebojnim dogovorom oz. pogodbo.

9.12. Spreminjanje dokumenta

9.12.1. Postopek uveljavitve sprememb

(1) Overitelj na MJU si pridržuje pravico do spremembe tega dokumenta brez predhodnega obveščanja imetnikov in drugih subjektov korenskega izdajatelja SI-TRUST Root, če spremembe ne vplivajo na namen uporabe in postopke upravljanja, ki lahko spremenijo nivo zaupanja.

(2) Spremembe ali dopolnitve k pričujoči politiki lahko izdajatelj objavi v obliki amandmajev k tej politiki, kadar ne gre za bistvene spremembe v delovanju izdajatelja.

(3) Amandmaji se sprejmejo po enakem postopku kot politika.

(4) Imetniki oz. bodoči imetniki lahko na elektronski naslov korenskega izdajatelja SI-TRUST Root podajo svoje pripombe glede vsebine politike, ki jih obravnavajo pooblaščene osebe overitelja na MJU. Overitelj na MJU si pridružuje pravico, da pripombe upošteva po lastni presoji.

9.12.2. Veljavnost in objava sprememb

Spremembe politike overitelja na MJU se sedem (7) dni pred veljavo predhodno objavi na spletnih straneh overitelja na MJU pod novo identifikacijsko oznako dokumenta (CP_{OID}) in z označenim datumom začetka njene veljavnosti.

9.12.3. Sprememba identifikacijske oznake politike

(1) Nova verzija politike korenskega izdajatelja SI-TRUST Root se označi z novo identifikacijsko oznako dokumenta (CP_{OID}).

(2) Povezani in podrejeni izdajatelji ob spremembi svojih politik delovanja presodijo, ali sprejete spremembe zahtevajo dodelitev novih identifikacijskih oznak politik (CP_{OID}), ki se uporabljajo v potrdilih, izdanih končnim uporabnikom. Če spremembe vplivajo na namen uporabe ali postopke upravljanja, ki lahko spremenijo nivo zaupanja, morajo dodeliti nove identifikacijske oznake politik.

9.13. Postopek v primeru sporov

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

(2) V primeru povezovanja korenskega izdajatelja SI-TRUST Root z izdajatelji izven Republike Slovenije, se postopek v primeru sporov določi v medsebojnem dogovoru oz. pogodbi.

9.14. Veljavna zakonodaja

Overitelj na MJU in korenski izdajatelj SI-TRUST Root delujeta v skladu z:

- ZEPEP,
- Uredbo k ZEPEP,

- Uredbo eIDAS,
- evropskimi direktivami,
- Zakonom o varstvu osebnih podatkov,
- Zakonom o tajnih podatkih,
- priporočili ETSI s področja kvalificiranih potrdil in storitev zaupanja,
- priporočili RFC s področja potrdil X.509,
- in drugimi veljavnimi predpisi in priporočili.

9.15. Skladnost z veljavno zakonodajo

Nadzor nad skladnostjo delovanja korenskega izdajatelja SI-TRUST Root z veljavno zakonodajo in predpisi, določenimi v podpogl. 9.14, izvaja pristojna inšpekcijska služba (glej podpogl. 8.2).

9.16. Splošne določbe

9.16.1. Celovit dogovor

Določbe te politike v ničemer ne spreminjajo, omejujejo ali drugače vplivajo na obveznosti, odgovornosti in poroštva, ki overitelja na MJU zavezujejo na podlagi drugih pogodb ali dogovorov oziroma druge veljavne zakonodaje.

9.16.2. Prenos pravic

Potrdilo, ki ga korenski izdajatelj SI-TRUST Root izda podrejenemu oz. poveznemu izdajatelju ter morebitne pravice, povezane z uporabo potrdila, so namenjene izključno imetniku in niso prenosljive na tretje osebe.

9.16.3. Neodvisnost določil

Če katerokoli od določil politike ali morebitnega dogovora oz. pogodbe je ali postane neveljavno, to ne vpliva na ostala določila. Neveljavno določilo se nadomesti z veljavnim, ki mora čim bolj ustrezati namenu, ki ga je želelo doseči neveljavno določilo.

9.16.4. Terjatve

Niso določene.

9.16.5. Višja sila

Overitelj na MJU ni odgovoren za škodo, ki bi nastala zaradi višje sile, na katero overitelj nima možnosti vpliva kot so npr. vojne, teroristična dejanja, nemiri, naravne nesreče ipd.

9.17. Ostale določbe

9.17.1. Razumevanje določil

V besedilu politike se uporablja moška samostalniška oblika, ki pa se nanaša na oba spola. Vsi izrazi, zapisani v ednini, se nanašajo tudi na množino in obratno.

9.17.2. Nasprotujoča določila

Če so določila te politike v nasprotju z določili katerekoli pogodbe ali dogovora med overiteljem na MJU in imetnikom ali tretjo osebo, veljajo določila pogodbe ali dogovora.

9.17.3. Odstopanje od določil

Če korenski izdajatelj SI-TRUST Root v posameznem primeru izjemoma odstopi od upoštevanja posameznega določila te politike, to ne pomeni, da bi ta izjema veljala tudi v bodoče in v vseh ostalih primerih.

9.17.4. Navzkrižno overjanje

Podrobnosti o navzkrižnem overjanju so podane v podpogl. 3.2.6.