Državni center za storitve zaupanja

SI-TRUST
Državni center za storitve zaupanja

KROVNA POLITIKA SI-TRUST za izdajatelje, ki delujejo v okviru ponudnika storitev zaupanja SI-TRUST

Javni del notranjih pravil Državnega centra za storitve zaupanja

veljavnost: od 24. decembra 2021
verzija: 1.3

CP_{Name}: SI-TRUST
CP_{OID}: 1.3.6.1.4.1.6105.8.1.1

Zgodovina politik

Izdaje krovne politike SI-TRUST	
verzija: 1.3, veljavnost: od 24. decembra 2021	
Krovna politika SI-TRUST za izdajatelje, ki delujejo v okviru ponudnika storitev zaupanja SI-TRUST CPOID: 1.3.6.1.4.1.6105.8.1.1 CPName: SI-TRUST	*Spremembe z verzijo 1.3:* • *ažuriranje skladnosti z zakonodajo,* • *revizija dokumenta.*
verzija: 1.2, veljavnost: od 20. oktobra 2020	
Krovna politika SI-TRUST za izdajatelje, ki delujejo v okviru ponudnika storitev zaupanja SI-TRUST CPOID: 1.3.6.1.4.1.6105.8.1.1 CPName: SI-TRUST	*Spremembe z verzijo 1.2:* • *pred prenehanjem delovanja izdajatelja se objavi register preklicanih potrdil z daljšo veljavnostjo,* • *sporočila OCSP podpirajo razširitev ArchiveCutOff v skladu s priporočilom ETSI EN 319 411-2,* • *revizija dokumenta.*
verzija: 1.1, veljavnost: od 1. oktobra 2019	
Krovna politika SI-TRUST za izdajatelje, ki delujejo v okviru ponudnika storitev zaupanja SI-TRUST CPOID: 1.3.6.1.4.1.6105.8.1.1 CPName: SI-TRUST	*Revizija dokumenta*
verzija: 1.0, veljavnost: od 28. maja 2018	
Krovna politika SI-TRUST za izdajatelje, ki delujejo v okviru ponudnika storitev zaupanja SI-TRUST CP_{OID}: 1.3.6.1.4.1.6105.8.1.1 CP_{Name}: SI-TRUST	/

VSEBINA

POVZETEK

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

SI-TRUST izdaja kvalificirana digitalna potrdila ter kvalificirane elektronske časovne žige, za katera velja najvišja stopnja varovanja ter deluje v skladu z veljavno zakonodajo s področja storitev zaupanja, standardi ETSI ter drugimi veljavnimi predpisi in priporočili.

SI-TRUST 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 SI-TRUST, so namenjena:
- izdajateljem potrdil, izdajateljem časovnih žigov, sistemom OCSP, informacijskim sistemom, 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 SI-TRUST, so namenjena:
- ustvarjanju elektronskih podpisov in elektronskih žig ter avtentikaciji spletišč,
- 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.

Kvalificirani elektronski časovni žigi SI-TRUST 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 kvalificirani elektronski časovni žig.

Podrobnosti o svojem delovanju posamezni izdajatelji določijo v svoji politiki delovanja.

Pričujoči dokument nadomešča prejšnjo objavljeno krovno politiko SI-TRUST. Vsa digitalna potrdila, izdana po datumu veljavnosti nove politike, se obravnavajo po novi politiki, za vsa ostala pa velja, da se obravnavajo po novi politiki glede tistih določil, ki lahko smiselno nadomestijo oz. dopolnijo določila iz politike, po kateri je bilo digitalno potrdilo izdano (na primer postopek za preklic velja po novi politiki).

Spremembi pričujočega dokumenta sta sledeči:
- pred prenehanjem delovanja izdajatelja se objavi register preklicanih potrdil z daljšo veljavnostjo,
- sporočila OCSP podpirajo razširitev ArchiveCutOff v skladu s priporočilom ETSI EN 319 411-2.

Ker spremembe, ki jih prinaša nova politika, ne vplivajo na namen uporabe ali postopke upravljanja, ki lahko spremenijo nivo zaupanja, se identifikacijska oznaka politike (CP_{OID}), ne spremeni.

1. UVOD

1.1. Pregled

(1) V okviru Ministrstva za javno upravo (v nadaljevanju *MJU*) deluje Državni center za storitve zaupanja (v nadaljevanju *SI-TRUST*).

(2) Politike ponudnika storitev zaupanja predstavljajo celoten javni del notranjih pravil SI-TRUST in določajo namen, delovanje in metodologijo upravljanja s kvalificiranimi in normaliziranimi digitalnimi potrdili, dodeljevanje kvalificiranih elektronskih časovnih žigov, odgovornost SI-TRUST ter zahteve, ki jih morajo izpolnjevati imetniki, uporabniki in tretje osebe, ki se zanašajo na kvalificirana in normalizirana digitalna potrdila ter na kvalificirane elektronske časovne žige, in drugi ponudniki storitev zaupanja, ki želijo uporabljati storitve SI-TRUST.

(3) SI-TRUST izdaja kvalificirana digitalna potrdila in kvalificirane elektronske časovne žige, za katera velja najvišja stopnja varovanja ter deluje v skladu z veljavno zakonodajo s področja storitev zaupanja, standardi ETSI ter drugimi veljavnimi predpisi in priporočili.

(4) SI-TRUST 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 SI-TRUST, so namenjena:
- izdajateljem potrdil, izdajateljem časovnih žigov, sistemom OCSP, informacijskim sistemom, 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 SI-TRUST, so namenjena:
- ustvarjanju elektronskih podpisov in elektronskih žig ter avtentikaciji spletišč,
- 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) Kvalificirani elektronski časovni žigi SI-TRUST 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 kvalificirani elektronski časovni žig.

(8) Podrobnosti o svojem delovanju posamezni izdajatelji določijo v svoji politiki delovanja.

1.2. Identifikacijski podatki politike delovanja

Določbe so opredeljene v posamezni politiki delovanja.

1.3. Udeleženci infrastrukture javnih ključev

1.3.1. Ponudnik storitev zaupanja

(1) Državni center za storitve zaupanja izdaja digitalna potrdila in kvalificirane elektronske 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:	https://www.si-trust.gov.si
Oznaka:	State-institutions

(3) Naloge upravljanja Državnega centra za storitve zaupanja opravlja upravni odbor SI-TRUST (glej podpogl. 5.2).

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

(5) Kontaktni podatki posameznega izdajatelja so navedeni v pripadajoči politiki delovanja.

(6) Naloge, ki jih opravlja posamezni izdajatelj, so navedene v pripadajoči politiki delovanja.

(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)
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	

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

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

(8) Potrdila podrejenih izdajateljev so navedena v posamezni politiki delovanja.

1.3.2. Prijavna služba

Določbe so opredeljene v posamezni politiki delovanja.

1.3.3. Imetniki potrdil

Določbe so opredeljene v posamezni politiki delovanja.

1.3.4. Tretje osebe

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

(2) Tretje osebe se morajo ravnati po navodilih SI-TRUST 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 SI-TRUST se lahko sklene medsebojni pisni dogovor.

1.3.5. Ostali udeleženci

Niso predvideni.

1.4. Namen uporabe potrdil

Določbe so opredeljene v posamezni politiki delovanja.

1.4.1. Pravilna uporaba potrdil in ključev

Določbe so opredeljene v posamezni politiki delovanja.

1.4.2. Nedovoljena uporaba potrdil in ključev

(1) Digitalna potrdila, ki jih izdaja SI-TRUST, se morajo uporabljati v skladu s Krovno politiko SI-TRUST in politiko posameznega izdajatelja, veljavno zakonodajo in medsebojnim dogovorom oz. pogodbo, sicer njihova uporaba ni dovoljena.

(2) Drugih prepovedi v zvezi z uporabo potrdil, ki jih izdaja SI-TRUST, ni.

1.5. Upravljanje s politiko

1.5.1. Upravljavec politike

Upravni odbor SI-TRUST je odgovoren za pripravo, prijavo, objavo, upravljanje in interpretacijo politik delovanja.

1.5.2. Kontaktne osebe

Kontaktne osebe v zvezi s politiko in ostalo dokumentacijo so pooblaščene osebe SI-TRUST (kontaktni podatki so podani v podpogl. 1.3).

1.5.3. Odgovorna oseba glede skladnosti delovanja izdajatelja s politiko

Odgovorne osebe glede skladnosti delovanja posameznega izdajatelja skladno s pripadajočo politiko so pooblaščene osebe SI-TRUST v skladu z nalogami, ki jih opravljajo znotraj organizacijskih skupin (glej podpogl. 5.2).

1.5.4. Postopek za sprejem nove politike

(1) SI-TRUST lahko izda tudi amandmaje k politikam, glej podpogl. 9.12.

(2) Upravni odbor SI-TRUST pripravi predlog nove politike oz. amandmaja.

(3) Skladno z uredbo eIDAS se prijava novosti storitev SI-TRUST posreduje nadzornemu organu po uredbi eIDAS.

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

1.6. Izrazi in okrajšave

1.6.1. Izrazi

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

Digitalni podpis	Napredni elektronski podpis, ki izpolnjuje zahteve iz 26. člena uredbe eIDAS.
Digitalno potrdilo oz. 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).
Elektronski podpis	Niz podatkov v elektronski obliki, ki so dodani k drugim podatkom v elektronski obliki ali so z njimi logično povezani in jih podpisnik uporablja za podpisovanje.
Elektronski žig	Niz podatkov v elektronski obliki, ki so dodani k drugim podatkom v elektronski obliki ali so z njimi logično povezani, da se zagotovita izvor in celovitost povezanih podatkov.
Elektronski časovni žig	Podatki v elektronski obliki, ki druge podatke v elektronski obliki povezujejo z določenim trenutkom in tako zagotavljajo dokaz, da so slednji podatki v tistem trenutku obstajali.
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*).
Kvalificirana storitev zaupanja	Storitev zaupanja, ki izpolnjuje zadevne zahteve iz uredbe eIDAS.
Kvalificirani elektronski podpis	Napredni elektronski podpis, ki se ustvari z napravo za ustvarjanje kvalificiranega elektronskega podpisa in temelji na kvalificiranem potrdilu za elektronske podpise.
Kvalificirani elektronski žig	Napredni elektronski žig, ki se ustvari z napravo za ustvarjanje kvalificiranega elektronskega žiga in temelji na kvalificiranem potrdilu za elektronski žig.
Kvalificirani elektronski časovni žig	Elektronski časovni žig, ki izpolnjuje zahteve iz 42. člena uredbe eIDAS.
Kvalificirano potrdilo za elektronski podpis	Digitalno potrdilo za elektronski podpis, ki ga izda ponudnik kvalificiranih storitev zaupanja in izpolnjuje zahteve iz Priloge I uredbe eIDAS.
Kvalificirano potrdilo za elektronski žig	Digitalno potrdilo za elektronski žig, ki ga izda ponudnik kvalificiranih storitev zaupanja in izpolnjuje zahteve iz Priloge III uredbe eIDAS.
Kvalificirano potrdilo za avtentikacijo spletišč	Digitalno potrdilo za avtentikacijo spletišč, ki ga izda ponudnik kvalificiranih storitev zaupanja in izpolnjuje zahteve iz Priloge IV uredbe eIDAS.
Poslovni subjekt	Pravna ali fizična oseba, registrirana za opravljanje dejavnosti.
Ponudnik storitev zaupanja	Fizična ali pravna oseba, ki zagotavlja eno ali več storitev zaupanja, kot ponudnik kvalificiranih ali nekvalificiranih storitev zaupanja (primerjaj okrajšavo CA).
Ponudnik kvalificiranih storitev zaupanja	Ponudnik storitev zaupanja, ki zagotavlja eno ali več kvalificiranih storitev zaupanja in mu nadzorni organ dodeli kvalificirani status.
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*).
Sredstvo elektronske identifikacije	Materialna in/ali nematerialna enota, ki vsebuje identifikacijske podatke osebe in se uporablja za avtentikacijo pri spletnih storitvah.
Storitev zaupanja	Elektronska storitev, ki se praviloma opravlja za plačilo in vključuje: (a) ustvarjanje, preverjanje in potrjevanje veljavnosti elektronskih

	podpisov, elektronskih žigov ali elektronskih časovnih žigov, storitev elektronske priporočene dostave in potrdil, povezanih s temi storitvami, ali (b) ustvarjanje, preverjanje in potrjevanje veljavnosti potrdil za avtentikacijo spletišč ali (c) hrambo elektronskih podpisov, žigov ali potrdil, povezanih s temi storitvami;
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.
Zanesljivi seznam ponudnikov storitev zaupanja	Zanesljivi seznam države članice Evropske Unije, ki vključuje informacije o ponudnikih kvalificiranih storitev zaupanja, za katere je odgovorna, skupaj z informacijami o kvalificiranih storitvah zaupanja, ki jih ti ponudniki zagotavljajo.

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

Aplikacija oz. informacijski sistem	Računalniški program, s katerim upravlja organizacija in ki za svoje delovanje potrebuje storitve SI-TRUST in ki se lahko izkaže z digitalnim potrdilom SI-TRUST ali na drug varen način, ki ga določi SI-TSA.
Domena	Neodvisna infrastruktura PKI za potrebe povezovanja izdajateljev, 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	Ponudnik storitev 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 ponudnika storitev zaupanja	Vsi prostori ponudnika storitev zaupanja, njegova strojna in programska oprema ter varnostni mehanizmi, ki so potrebni za varno delovanje njegovih izdajateljev.
Interna politika SI-TRUST	Zaupni del notranjih pravil delovanja SI-TRUST, ki jo sestavljajo Krovna varnostna politika ter podrejeni dokumenti in specifične politike za posamezna področja.
Izdajatelj	Izdajatelj digitalnih potrdil, ki deluje v okviru ponudnika storitev zaupanja (primerjaj okrajšavo *CA* in izraza *Ponudnik storitev zaupanja* in *Potrdilo*).
Izdajatelj SIGOV-CA	Izdajatelj potrdil za državne organe, ki deluje znotraj SI-TRUST, angl. *Slovenian Governmental Certification Authority* (primerjaj definicijo *Državni organ*).
Izdajatelj SIGEN-CA	Izdajatelj potrdil za fizične osebe in poslovne subjekte, ki deluje znotraj SI-TRUST, angl. *Slovenian General Certification Authority*.
Izdajatelj SI-PASS-CA	Izdajatelj potrdil, ki izdaja potrdila za fizične osebe za potrebe storitve za spletno prijavo in e-podpis SI-PASS in deluje znotraj SI-TRUST, angl. *Slovenian Authentication and e-Signature Service Certification Authority*.
Izdajatelj SI-TSA	Izdajatelj kvalificiranih časovnih žigov, ki deluje znotraj SI-TRUST, angl. *Slovenian Time Stamping Authority*.
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 SI-TRUST in izdaja digitalna potrdila za podrejene in povezane izdajatelje kvalificiranih digitalnih potrdil (angl. *Slovenian Trust Service Root Certification Authority*).
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).
Naprava za ustvarjanje kvalificiranega elektronskega podpisa	Naprava za ustvarjanje elektronskega podpisa, ki izpolnjuje zahteve iz Priloge II uredbe eIDAS (QSCD, angl. *Qualified Signature Creation Device*). Zasebnega ključa z naprave za ustvarjanje kvalificiranega elektronskega podpisa ni mogoče izvoziti oz. kopirati.
Objava SI-TRUST	Javna objava na spletnih straneh SI-TRUST, https://www.si-trust.gov.si.
Obvestila SI-TRUST	Vsa navodila, pojasnila, seznami, pogoji, posamezna obvestila, priporočila, standardi in drugi dokumenti, ki jih določi ali priporoči SI-TRUST Root oz. SI-TRUST in jih objavi ali kako drugače posreduje imetnikom, organizacijam ali tretjim osebam.
Organizacija	Državni organ, pravna ali fizična oseba, ki upravlja z izdajateljem potrdil, kateremu je SI-TRUST Root izdal povezovalno potrdilo (primerjaj izraz *Ponudnik storitev zaupanja*).
Pametna kartica oz. varno sredstvo za elektronsko podpisovanje	Glej izraz *Naprava za ustvarjanje kvalificiranega elektronskega podpisa*.
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 ponudnika storitev zaupanja, ki določajo namen, delovanje in metodologijo upravljanja z digitalnimi potrdili, odgovornost ponudnika storitev zaupanja ter zahteve, ki jih morajo izpolnjevati uporabniki in tretje osebe, ki uporabljajo in se zanašajo na digitalna potrdila ponudnika storitev zaupanja.
Posebno potrdilo	Digitalno potrdilo z dvema paroma ključev, ki povezuje podatke iz potrdila z imetnikovima zasebnima ključema. Posebno potrdilo sestavljata potrdilo za overjanje podpisa in potrdilo za šifriranje.
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.
Prijavna služba	Po pooblastilu izdajatelja prijavna služba sprejema zahtevke za pridobitev, preklic in regeneracijo potrdil ter preverja istovetnosti imetnikov oz. bodočih imetnikov (RA, angl. *Registration Authority*).
smsPASS	Sredstvo elektronske identifikacije, ki omogoča prijavo prek storitve SI-PASS z uporabo enkratnega gesla, poslanega s sporočilom SMS.

Spletno potrdilo	Digitalno potrdilo z enim parom ključev, ki povezuje podatke iz potrdila z imetnikovim zasebnim ključem (angl. *web certificate*).
Storitev SI-PASS	Storitev za spletno prijavo in e-podpis (angl. *Authentication and e-Signature Service)*, https://sicas.gov.si.
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
Zahtevek	Obrazec za pridobitev, preklic ali regeneracijo potrdil, ki je dostopen preko spletne strani SI-TRUST oz. pri pooblaščenih osebah na prijavnih službah.
Zaposlen	Fizična oseba, ki je v delovnem razmerju z organizacijo ali pa na drugačni pravni podlagi dela za organizacijo in za katero želi odgovorna oseba te organizacije pridobiti potrdilo, ki ga ta oseba potrebuje za opravljanje dela za to organizacijo.

1.6.2. Okrajšave

CA	Izdajatelj digitalnih potrdil, angl. *Certification Authority*
CP_{Name}	Ime politike delovanja ponudnika storitev zaupanja 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*)
DCF77	Dolgovalovni radijski oddajnik, ki stoji v Mainflingenu pri Frankfurtu in oddaja uradno časovno referenco 77.5 kHz
eIDAS	Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES
ETSI	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*
GPS	Satelitski sistem za določanje položaja, angl. *Global Positioning System*
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

NTP	Protokol za sinhronizacijo časa, angl. *Network Time Protocol*, http://www.ntp.org
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. SI-TRUST 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 ponudnika storitev zaupanja. 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*«.
QSCD	Naprava za ustvarjanje kvalificiranega elektronskega podpisa, ki izpolnjuje zahteve iz Priloge II uredbe eIDAS, angl. *Qualified Signature Creation Device*
QTSP	Ponudnik kvalificiranih storitev zaupanja, angl. *Qualified Trust Service Provider*
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	Glej izraz Državni center za storitve zaupanja.
SI-TRUST Root	Korenski izdajatelj digitalnih potrdil, angl. *Slovenian Trust Service Root Certification Authority*
TSP	Ponudnik storitev zaupanja, angl. *Trust Service Provider*
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 elektronskih časovnih žigov (TSA, angl. *Time Stamping Authority*)
UTC	Koordiniran univerzalni čas, angl. *Coordinated Universal Time,* mednarodni standard za meritve časa, veljaven od. l. 1972

ZEISZ	Zakon o elektronski identifikaciji in storitvah zaupanja

2. OBJAVE IN ODGOVORNOSTI GLEDE REPOZITORIJA

2.1. Repozitoriji

SI-TRUST dokumente oz. podatke posameznega izdajatelja javno objavlja v dveh repozitorijih:
- v javnem imeniku na strežniku x500.gov.si ter
- na spletnih straneh https://www.si-trust.gov.si.

2.2. Objava informacij o potrdilih

Določbe so opredeljene v posamezni politiki delovanja.

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) Potrdila se skladno z določili posamezne politike objavijo v javnem imeniku takoj po njihovi izdaji, evidenčni podatki o potrdilu (imetnikov naziv, naslov e-pošte, serijska številka ...) pa že ob sami rezervaciji potrdila.

(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

Določbe so opredeljene v posamezni politiki delovanja.

3. ISTOVETNOST IN VERODOSTOJNOST

3.1. Določanje imen

Določbe so opredeljene v posamezni politiki delovanja.

3.1.1. Oblika imen

Določbe so opredeljene v posamezni politiki delovanja.

3.1.2. Zahteva po smiselnosti imen

Določbe so opredeljene v posamezni politiki delovanja.

3.1.3. Uporaba anonimnih imen ali psevdonimov

Določbe so opredeljene v posamezni politiki delovanja.

3.1.4. Pravila za interpretacijo imen

Določbe so opredeljene v posamezni politiki delovanja.

3.1.5. Enoličnost imen

Določbe so opredeljene v posamezni politiki delovanja.

3.1.6. Priznavanje, verodostojnost in vloga blagovnih znamk

(1) Imetnik oz. organizacija 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. SI-TRUST ni dolžan preverjati in/ali na to opozoriti imetnika oz. organizacijo.

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

3.2. Začetno preverjanje istovetnosti

Določbe so opredeljene v posamezni politiki delovanja.

3.2.1. Metoda za dokazovanje lastništva zasebnega ključa

Določbe so opredeljene v posamezni politiki delovanja.

3.2.2. Preverjanje istovetnosti organizacij

Določbe so opredeljene v posamezni politiki delovanja.

3.2.3. Preverjanje istovetnosti fizičnih oseb

Določbe so opredeljene v posamezni politiki delovanja.

3.2.4. Nepreverjeni podatki pri začetnem preverjanju

Določbe so opredeljene v posamezni politiki delovanja.

3.2.5. Preverjanje pooblastil

Določbe so opredeljene v posamezni politiki delovanja.

3.2.6. Merila za medsebojno povezovanje

Določbe so opredeljene v posamezni politiki delovanja.

3.3. Istovetnost in verodostojnost ob obnovi potrdila

Določbe so opredeljene v posamezni politiki delovanja.

3.3.1. Istovetnost in verodostojnost ob obnovi

Določbe so opredeljene v posamezni politiki delovanja.

3.3.2. Istovetnost in verodostojnost ob obnovi po preklicu

Določbe so opredeljene v posamezni politiki delovanja.

3.4. Istovetnost in verodostojnost ob zahtevi za preklic

Določbe so opredeljene v posamezni politiki delovanja.

4. UPRAVLJANJE S POTRDILI

4.1. Zahtevek za pridobitev potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.1.1. Kdo lahko predloži zahtevek za pridobitev potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.1.2. Postopek za pridobitev potrdila in odgovornosti

Določbe so opredeljene v posamezni politiki delovanja.

4.2. Postopek ob sprejemu zahtevka za pridobitev potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.2.1. Postopek preverjanja istovetnosti in verodostojnosti bodočega imetnika

Določbe so opredeljene v posamezni politiki delovanja.

4.2.2. Odobritev/zavrnitev zahtevka

Določbe so opredeljene v posamezni politiki delovanja.

4.2.3. Čas za izdajo potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.3. Izdaja potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.3.1. Postopek izdajatelja ob izdaji potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.3.2. Obvestilo imetniku o izdaji potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.4. Prevzem potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.4.1. Postopek prevzema potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.4.2. Objava potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.4.3. Obvestilo o izdaji tretjim osebam

Določbe so opredeljene v posamezni politiki delovanja.

4.5. Uporaba potrdil in ključev

4.5.1. Uporaba potrdila in zasebnega ključa imetnika

Določbe so opredeljene v posamezni politiki delovanja.

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 posameznega izdajatelja:

- 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 izdajatelja potrdila, ki je objavljen v tej politiki in tudi na morebiten drug način posredovan tretjim osebam,
- upoštevati druge določbe, če je s SI-TRUST sklenila dogovor o uporabi potrdil.

(4) Tretja oseba mora za overjanje podpisa oz. druge kriptografske operacije uporabljati programsko in strojno opremo, s katero lahko na verodostojen način preveri vse zgoraj navedene zahteve za varno uporabo potrdil.

(5) 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

Določbe so opredeljene v posamezni politiki delovanja.

4.7.1. Razlogi za obnovo potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.7.2. Kdo lahko zahteva obnovo potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.7.3. Postopek pri obnovi potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.7.4. Obvestilo imetniku o obnovi potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.7.5. Prevzem obnovljenega potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.7.6. Objava obnovljenega potrdila

Določbe so opredeljene v posamezni politiki delovanja.

4.7.7. Obvestilo o izdaji drugim subjektom

Določbe so opredeljene v posamezni politiki delovanja.

4.8. Sprememba potrdila

Določbe so opredeljene v posamezni politiki delovanja.

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[2]

4.9.1. Razlogi za preklic

Določbe so opredeljene v posamezni politiki delovanja.

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

4.9.2. Kdo lahko zahteva preklic

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

(2) V primeru, da SI-TRUST informacijo o zlorabi potrdila pridobi s strani tretje osebe, pred preklicem potrdila pridobi soglasje njegovega imetnika.

4.9.3. Postopek za preklic

Določbe so opredeljene v posamezni politiki delovanja.

4.9.4. Čas za izdajo zahtevka za preklic

Določbe so opredeljene v posamezni politiki delovanja.

4.9.5. Čas od prejetega zahtevka za preklic do izvedbe preklica

Določbe so opredeljene v posamezni politiki delovanja.

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 posameznega izdajatelja .

(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

(1) 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 pri korenskem izdajatelju SI-TRUST Root,
- enkrat dnevno, če ni novih zapisov oz. sprememb v registru preklicanih potrdil, in sicer približno štiriindvajset (24) ur po zadnjem osveževanju pri ostalih izdajateljih.

(2) Pred prenehanjem delovanja izdajatelja SI-TRUST objavi pripadajoči register preklicanih potrdil na naslednji način:

- obdobje veljavnosti registra preklicanih potrdil znaša 3000 mesecev,
- register preklicanih potrdil je dostopen najmanj 7 let po prenehanju delovanja izdajatelja.

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 pri korenskem izdajatelju SI-TRUST Root oz. z zakasnitvijo največ desetih (10) minut pri ostalih izdajateljih.

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

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

Določbe so opredeljene v posamezni politiki delovanja.

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 ponudnikom storitev zaupanja

Določbe so opredeljene v posamezni politiki delovanja.

4.12. Odkrivanje kopije ključev za dešifriranje

Določbe so opredeljene v posamezni politiki delovanja.

4.12.1. Postopek za odkrivanje ključev za dešifriranje

Določbe so opredeljene v posamezni politiki delovanja.

4.12.2. Postopek za odkrivanje ključa seje

Ni podprto.

5. UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE

5.1. Fizično varovanje

(1) Oprema SI-TRUST je varovana z večnivojskim sistemom fizičnega in elektronskega varovanja.

(2) Varovanje infrastrukture SI-TRUST se izvaja v skladu s priporočili stroke za najvišji nivo varovanja.

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

5.1.1. Lokacija in zgradba ponudnika storitev zaupanja

(1) Oprema SI-TRUST 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 SI-TRUST.

5.1.2. Fizični dostop do infrastrukture ponudnika storitev zaupanja

(1) Dostop do infrastrukture SI-TRUST je omogočen samo pooblaščenim osebam SI-TRUST 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 SI-TRUST.

5.1.3. Napajanje in prezračevanje

(1) Infrastruktura SI-TRUST ima zagotovljeno neprekinjeno napajanje in ustrezne klimatske sisteme.

(2) Podrobno o tem je določeno v Interni politiki SI-TRUST.

5.1.4. Zaščita pred poplavo

(1) Infrastruktura SI-TRUST ni izpostavljena nevarnosti poplav.

(2) Podrobno o tem je določeno v Interni politiki SI-TRUST.

5.1.5. Zaščita pred požari

(1) Prostori SI-TRUST so varovani pred morebitnim izbruhom požara.

(2) Podrobno o tem je določeno v Interni politiki SI-TRUST.

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 SI-TRUST se redno obnavljajo in shranjujejo v dveh ločenih in fizično varovanih prostorih, na različnih lokacijah.

(3) Podrobno o tem je določeno v Interni politiki SI-TRUST.

5.1.7. Odstranjevanje odpadkov

(1) SI-TRUST zagotavlja varno odstranjevanje in uničevanje dokumentov v fizični in elektronski obliki.

(2) Odstranjevanje odpadkov izvaja posebna komisija v skladu z Interno politiko SI-TRUST.

5.1.8. Hramba na oddaljeni lokaciji

Glej podpogl. 5.1.6.

5.2. Organizacijska struktura ponudnika storitev zaupanja

5.2.1. Organizacija ponudnika storitev zaupanja in zaupanja vredne vloge

(1) Operativno, organizacijsko in strokovno pravilno delovanje SI-TRUST vodi pooblaščena oseba SI-TRUST, 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 SI-TRUST spadajo:
- zaposleni pri SI-TRUST in
- prijavne službe.

(3) Zaposleni pri SI-TRUST so razporejeni v šest organizacijskih skupin, ki pokrivajo naslednja vsebinska področja:
- upravljanje ponudnika storitev zaupanja,
- 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 ponudnika storitev zaupanja,
- upravljanje s potrdili,
- upravljanje z infrastrukturo,
- varovanje in kontrola.

Organizacijska skupina	Vloga	Osnovne naloge	Število oseb
Upravljanje ponudnika storitev zaupanja	Upravljavec sistema	– Strategija delovanja SI-TRUST – Določevanje prvega varnostnega inženirja – Operativno vodenje SI-TRUST	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	2

		delovanja sistema za podeljevanje potrdil	
	Administratorji potrdil	– Upravljanje s potrdili*	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 – Vzdrževanje varnostnih kopij	1
Notranje preverjanje skladnosti	Notranji revizor		1
Pravno-administrativno	Pravnik		1

* Zaradi posebnosti izdajatelja SI-TRUST Root vlogo administratorjev potrdil pri njem opravljajo varnostni inženirji.

(5) Upravni odbor SI-TRUST sestavljajo upravljavec sistema, varnostni inženir, pravnik in vodja NOE.

(6) Naloge upravnega odbora SI-TRUST 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 SI-TRUST opravljati več oseb hkrati. Med te spadajo:
- regeneriranje ključev,
- odkrivanje kopije ključev za dešifriranje ter
- druge naloge, določene z Interno politiko SI-TRUST.

(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 SI-TRUST.

5.2.4. Nezdružljivost vlog

(1) Vse organizacijske skupine SI-TRUST, 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) Ne glede na določbe prejšnjega člena so pri kritičnih opravilih, katerih izvedba ima za posledico porast tveganj, vloge med seboj nezdružljive.

(3) Vloge posameznih organizacijskih skupin so določene z Interno politiko SI-TRUST.

5.3. Nadzor nad osebjem

V skladu z veljavno zakonodajo so podrobnejša določila glede nadzora osebja določena v Interni politiki SI-TRUST.

5.3.1. Potrebne kvalifikacije in izkušnje osebja ter njegova primernost

(1) Osebje SI-TRUST 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 SI-TRUST pred pričetkom opravljanja nalog za potrebe SI-TRUST podpišejo izjavo o opravljanju nalog s posebnimi odgovornostmi.

(3) Zaposleni pri SI-TRUST, ki opravljajo zaupanja vredne vloge:
- morajo biti za opravljanje teh vlog imenovani s strani upravnega odbora SI-TRUST,
- ne smejo opravljati drugih nalog, ki bi bile v nasprotju z opravljanjem nalog pri SI-TRUST,
- 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 SI-TRUST 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 SI-TRUST, ki opravlja zaupanja vredne vloge, se ob pridobitvi dovoljenja za dostop do tajnih podatkov izvaja s strani organa, pristojnega po zakonodaji s področja tajnih podatkov.

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 SI-TRUST.

5.3.5. Menjava nalog

Ni predpisana.

5.3.6. Sankcije

Sankcije v primeru nepooblaščenega ali malomarnega izvajanja nalog se za pooblaščene osebe SI-TRUST 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 SI-TRUST.

5.3.8. Dostop osebja do dokumentacije

Pooblaščenim osebam SI-TRUST je na voljo vsa potrebna dokumentacija skladno z njihovimi zadolžitvami in nalogami.

5.4. Varnostni pregledi sistema

(1) SI-TRUST 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 SI-TRUST.

5.4.1. Vrste beleženih dogodkov

(1) SI-TRUST skladno z veljavno zakonodajo beleži naslednje vrste dogodkov:
- dogodke na operacijskem sistemu, programski in strojni opremi posameznega izdajatelja,
- dogodke na operacijskih sistemih, programski in strojni opremi elementov komunikacijskega sistema,
- dogodke v zvezi s ključi posameznega 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 posameznega izdajatelja,
- dogodke v zvezi z varnostno politiko in upravljanjem komunikacijskega sistema.

(2) SI-TRUST zbira in beleži v elektronski ali pisni obliki tudi podatke, ki vplivajo na varnost, niso pa del informacijsko-komunikacijskega sistema ponudnika storitev zaupanja:
- dogodke v zvezi s fizičnim dostopom do sistemov posameznega izdajatelja ter fizično lokacijo,
- kadrovske spremembe osebja SI-TRUST,
- 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 SI-TRUST.

5.4.2. Pogostost pregledov dnevnikov beleženih dogodkov

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

(2) Osebje SI-TRUST 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 SI-TRUST.

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 SI-TRUST.

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 SI-TRUST.

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 SI-TRUST ali

pa se to izvaja avtomatsko z drugimi varnostnimi mehanizmi na vseh računalniško-komunikacijskih napravah v pristojnosti SI-TRUST.

(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 SI-TRUST.

5.5. Arhiviranje podatkov

5.5.1. Vrste arhiviranih podatkov

SI-TRUST 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 SI-TRUST
- zasebne ključe za dešifriranje v skladu z podpogl. 6 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 SI-TRUST.

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 SI-TRUST.

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 SI-TRUST.

5.5.7. Postopek za dostop do arhiviranih podatkov in njihova verifikacija

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

(2) V skladu z veljavno zakonodajo je to podrobno določeno v Interni politiki SI-TRUST.

5.6. Obnova izdajateljevega potrdila

Določbe so opredeljene v posamezni politiki 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 SI-TRUST.

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

V skladu z veljavno zakonodajo je to določeno v Interni politiki SI-TRUST.

5.7.3. Postopek v primeru ogroženega zasebnega ključa izdajatelja

V skladu z veljavno zakonodajo je to določeno v Interni politiki SI-TRUST.

5.7.4. Okrevalni načrt

V skladu z veljavno zakonodajo je to določeno v Interni politiki SI-TRUST.

5.8. Prenehanje delovanja izdajatelja

Če bo SI-TRUST prenehal z opravljanjem svoje dejavnosti ali posamezni izdajatelj prenehal z izdajanjem potrdil, bo SI-TRUST ukrepal skladno z veljavno zakonodajo ter morebitnim medsebojnim dogovorom oz. pogodbo. Postopek prenehanja je podrobneje določen v Interni politiki SI-TRUST.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev ključev

6.1.1. Generiranje ključev

Določbe so opredeljene v posamezni politiki delovanja.

6.1.2. Dostava zasebnega ključa imetnikom

Določbe so opredeljene v posamezni politiki delovanja.

6.1.3. Dostava javnega ključa izdajatelju potrdil

Določbe so opredeljene v posamezni politiki delovanja.

6.1.4. Dostava izdajateljevega javnega ključa tretjim osebam

Določbe so opredeljene v posamezni politiki delovanja.

6.1.5. Dolžina ključev

Določbe so opredeljene v posamezni politiki delovanja.

6.1.6. Generiranje in kakovost parametrov javnih ključev

Kvaliteta parametrov ključa posameznega izdajatelja 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 posameznega izdajatelja, 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 posameznega izdajatelja 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 potrdil korenskega izdajatelja SI-TRUST Root, 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 posameznega izdajatelja so v skladu z veljavno zakonodajo določena v Interni politiki SI-TRUST.

6.2.3. Odkrivanje kopije zasebnega ključa

Določbe so opredeljene v posamezni politiki delovanja.

6.2.4. Varnostna kopija zasebnega ključa

Določbe so opredeljene v posamezni politiki delovanja.

6.2.5. Arhiviranje zasebnega ključa

Določbe so opredeljene v posamezni politiki delovanja.

6.2.6. Prenos zasebnega ključa iz/v kriptografski modul

(1) Prenos zasebnega ključa posameznega izdajatelja iz strojnega varnostnega modula se izvede v šifrirani obliki po generiranju para ključev izdajatelja 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 SI-TRUST.

(3) Podrobnosti o prenosu izdajateljevega zasebnega ključa so določene v Interni politiki SI-TRUST.

(4) Podrobnosti generiranja zasebnega ključa imetnika posamezni izdajatelji določijo v svoji politiki delovanja.

6.2.7. Zapis zasebnega ključa v kriptografskem modulu

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

(2) Podrobnosti dostopa do zasebnega ključa imetnika posamezni izdajatelji določijo v svoji politiki delovanja.

6.2.8. Postopek za aktiviranje zasebnega ključa

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

(2) Podrobnosti aktiviranja zasebnega ključa imetnika posamezni izdajatelji določijo v svoji politiki delovanja.

6.2.9. Postopek za deaktiviranje zasebnega ključa

(1) Ob zaustavitvi delovanja posameznega izdajatelja programska oprema izdajatelja deaktivira zasebni ključ izdajatelja.

(2) Podrobnosti deaktiviranja zasebnega ključa imetnika posamezni izdajatelji določijo v svoji politiki delovanja.

6.2.10. Postopek za uničenje zasebnega ključa

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

(2) Podrobnosti uničenja zasebnega ključa imetnika posamezni izdajatelji določijo v svoji politiki delovanja.

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

Posamezni izdajatelj arhivira svoj javni ključ in javne ključe imetnikov, kot je podano v podpogl. 5.5.

6.3.2. Obdobje veljavnosti potrdila in ključev

Določbe so opredeljene v posamezni politiki delovanja.

6.4. Gesla za dostop do zasebnega ključa

6.4.1. Generiranje gesel

Določbe so opredeljene v posamezni politiki delovanja.

6.4.2. Zaščita gesel

Določbe so opredeljene v posamezni politiki delovanja.

6.4.3. Drugi vidiki gesel

Določbe so opredeljene v posamezni politiki delovanja.

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 SI-TRUST.

6.5.2. Nivo varnostne zaščite

V skladu z veljavno zakonodajo je to določeno v Interni politiki SI-TRUST.

6.6. Tehnični nadzor življenjskega cikla izdajatelja

6.6.1. Nadzor razvoja sistema

(1) Posamezni izdajatelj uporablja programsko opremo proizvajalca Entrust, ki je certificirana v skladu s Common Criteria EAL4+.

(2) Podrobne tehnične zahteve so določene v Interni politiki SI-TRUST.

(3) Imetniki potrdil korenskega izdajatelja 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 SI-TRUST.

6.6.3. Nadzor življenjskega cikla

V skladu z veljavno zakonodajo je to določeno v Interni politiki SI-TRUST.

6.7. Varnostna kontrola računalniške mreže

Določbe so opredeljene v posamezni politiki delovanja.

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

Določbe so opredeljene v posamezni politiki delovanja.

7.1.2. Profil potrdil z razširitvami

Določbe so opredeljene v posamezni politiki delovanja.

7.1.3. Identifikacijske oznake algoritmov

(1) Potrdila, ki jih izdaja posamezni izdajatelj, 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 SI-TRUST.

(3) Korenski izdajatelj 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..3.1.1

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 posamezni izdajatelj, 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 z njim 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

Določbe so opredeljene v posamezni politiki delovanja.

7.3. Profil sprotnega preverjanja statusa potrdil

Določbe so opredeljene v posamezni politiki delovanja.

7.3.1. Različica

Posamezni izdajatelj 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,
- razširitev ArchiveCutOff v skladu s priporočilom ETSI EN 319 411-2, 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 SI-TRUST opravlja pristojna inšpekcijska služba v skladu z veljavno zakonodajo.

(2) Zunanje preverjanje skladnosti delovanja izvaja organ za ugotavljanje skladnosti v skladu z veljavno zakonodajo.

(3) Notranje preverjanje skladnosti delovanja izvaja notranji revizor in ostale pooblaščene osebe v okviru SI-TRUST.

8.3. Neodvisnost inšpekcijske službe

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

8.4. Področja inšpekcijskega nadzora

Področja nadzora so določena z veljavno zakonodajo in predpisi.

8.5. Ukrepi ponudnika storitev zaupanja

V primeru ugotovljenih pomanjkljivosti ali napak si SI-TRUST prizadeva za odpravo le-teh v najkrajšem možnem času.

8.6. Objava rezultatov inšpekcijskega nadzora

(1) SI-TRUST na svojih spletnih straneh javno objavi povzetek sklepov inšpekcijskega nadzora.

(2) SI-TRUST na svojih spletnih straneh javno objavi informacijo o organu za ugotavljanje skladnosti, ki je v skladu z veljavno zakonodajo izvedel zunanje preverjanje skladnosti delovanja SI-TRUST.

9. OSTALE POSLOVNE IN PRAVNE ZADEVE

9.1. Cenik storitev

9.1.1. Cena izdaje in obnove potrdil

Določbe so opredeljene v posamezni politiki delovanja.

9.1.2. Cena dostopa do potrdil

Določbe so opredeljene v posamezni politiki delovanja.

9.1.3. Cena dostopa do statusa potrdila in registra preklicanih potrdil

Določbe so opredeljene v posamezni politiki delovanja.

9.1.4. Cene drugih storitev

Stroške potrebne strojne ali programske opreme, ki jo zahteva oz. priporoča posamezni izdajatelj za varno shranjevanje in uporabo potrdil, krije imetnik potrdila oz. organizacija.

9.1.5. Povrnitev stroškov

Ni predpisana.

9.2. Finančna odgovornost

9.2.1. Zavarovalniško kritje

Ministrstvo za javno upravo ima glede delovanja SI-TRUST 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) SI-TRUST kot zaupne obravnava naslednje podatke:
- vse zahtevke za pridobitev potrdila ali druge storitve,
- zasebne ključe potrdil, če se hranijo pri izdajatelju,
- 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 SI-TRUST.

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

9.3.2. Nevarovani podatki

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

9.3.3. Odgovornost glede varovanja poslovnih podatkov

SI-TRUST 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, SI-TRUST ravna v skladu z veljavno zakonodajo.

9.4.2. Varovani osebni podatki

Varovani podatki so vsi osebni podatki, ki jih posamezni izdajatelj 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

SI-TRUST je odgovoren v skladu z veljavno zakonodajo glede varovanja osebnih podatkov.

9.4.5. Pooblastilo glede uporabe osebnih podatkov

Določbe so opredeljene v posamezni politiki delovanja.

9.4.6. Posredovanje osebnih podatkov na uradno zahtevo

Določbe so opredeljene v posamezni politiki delovanja.

9.4.7. Druga določila glede posredovanja osebnih podatkov

Določbe so opredeljene v posamezni politiki delovanja.

9.5. Določbe glede pravic intelektualne lastnine

Določbe glede avtorskih, sorodnih in drugih pravic intelektualne lastnine v zvezi s posameznim izdajateljem :

- na politiki pripadajo vse pravice SI-TRUST,
- na imeniku potrdil in registru preklicanih potrdil pripadajo vse pravice SI-TRUST,
- na vseh podatkih v potrdilih pripadajo vse pravice SI-TRUST,
- na zasebnem ključu za podpisovanje pripadajo vse pravice imetniku oz. organizaciji.

9.6. Obveznosti in odgovornosti

9.6.1. Obveznosti in odgovornosti izdajatelja

(1) SI-TRUST 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, cenik, navodila ipd.),
- objavljati na svojih spletnih straneh vse informacije o tistih spremembah glede dejavnosti SI-TRUST, ki kakorkoli vplivajo na imetnike potrdil, organizacije in tretje osebe,
- zagotoviti delovanje prijavnih služb v skladu z določili posameznega izdajatelja in ostalimi veljavnimi predpisi,
- spoštovati določila glede varnega ravnanja z osebnimi, poslovnimi in zaupnimi podatki o ponudniku storitev zaupanja, imetnikih potrdil, organizacijah 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 politiko posameznega izdajatelja in ostalimi predpisi ter priporočili,
- pred nepooblaščenimi dostopi skrbno varovati zasebne ključe potrdil, če se hranijo pri izdajatelju.

(2) SI-TRUST 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 varen prevzem digitalnih potrdil z obvezno uporabo pametnih kartic in poskrbeti za varno posredovanje pametnih kartic z digitalnimi potrdili imetnikom,
- zagotoviti pravilnost objave registra preklicanih potrdil,

- zagotoviti pravilnost delovanja sprotnega preverjanja statusa potrdil,
- zagotoviti enoličnost razločevalnih imen,
- zagotoviti primerno fizično varnost prostorov in dostopov do samih prostorov ponudnika storitev zaupanja,
- najmanj enkrat letno preveriti, ali naprave, ki jih uporablja kot varna sredstva za elektronsko podpisovanje, izpolnjujejo zahteve iz Priloge II uredbe eIDAS,
- 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,
- obveščati vse ustrezne subjekte o pomembnih zadevah in
- izpolnjevati vse druge zahteve v skladu s politiko.

(3) SI-TRUST 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 SI-TRUST in
- nedostopnosti kot posledico višje sile ali izrednih dogodkov.

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

(5) SI-TRUST je odgovoren za vse navedbe v tem dokumentu in za izvajanje vseh določil iz te politike.

(6) Ostale obveznosti oz. odgovornosti SI-TRUST so določene v interni politiki SI-TRUST in morebitnem medsebojnem dogovoru oz. pogodbi z imetnikom, organizacijo ali tretjo osebo.

9.6.2. Obveznosti in odgovornosti prijavne službe

Določbe so opredeljene v posamezni politiki delovanja.

9.6.3. Obveznosti in odgovornosti imetnika

Določbe so opredeljene v posamezni politiki delovanja.

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 posamezni izdajatelj.

(2) Tretje osebe, ki se zanašajo na izdana potrdila posameznega izdajatelja, 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 izdajatelja, 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 izdajatelja glede zanesljive uporabe,
- ob morebitnih napakah ali problemih takoj obvestiti izdajatelja ,
- seznaniti se s to politiko ter upoštevati vsa določila glede njihove obveznosti, odgovornosti ter omejitve glede zaupanja in uporabe potrdil,
- spremljati vsa obvestila in objave izdajatelja 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 s SI-TRUST in veljavne zakonodaje.

9.6.5. Obveznosti in odgovornosti drugih subjektov

Niso predpisane.

9.7. Zanikanje odgovornosti

SI-TRUST ni odgovoren za škodo, ki bi nastala zaradi:

- uporabe potrdil za namen in na način, ki ni izrecno predviden v politiki posameznega izdajatelja oz. morebitnem dogovoru med imetnikom oz. organizacijo in SI-TRUST,
- 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 posameznega izdajatelja, 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 ali organizacije,
- uporabe potrdil ter veljavnosti potrdil ob spremembah podatkov iz potrdila ali spremembah podatkov o imetniku ali organizaciji,
- izpada infrastrukture, ki ni v domeni upravljanja SI-TRUST,
- podatkov, ki se šifrirajo ali podpisujejo z uporabo pripadajočih potrdil oz. 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 posameznega izdajatelja ali druge veljavne predpise,
- uporabe in zanesljivosti delovanja strojne in programske opreme imetnikov potrdil.

9.8. Omejitev odgovornosti

Določbe so opredeljene v posamezni politiki delovanja.

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 SI-TRUST se sedem (7) dni pred veljavo predhodno objavi na spletnih straneh SI-TRUST 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) Posamezni 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 ponudnika storitev zaupanja oz. posameznega izdajatelja so objavljeni na spletnih straneh in podani v podpogl. **Napaka! Vira sklicevanja ni bilo mogoče najti.**.

(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 SI-TRUST.

(4) Posamezni izdajatelj ostale subjekte obvešča preko obvestil, objavljenih na spletnih straneh, ter preko e-pošte.

(5) Posamezni izdajatelj ter tretja oseba lahko določita način komuniciranja z medsebojnim dogovorom oz. pogodbo.

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

9.12. Spreminjanje dokumenta

9.12.1. Postopek uveljavitve sprememb

(1) Pred vsako spremembo pričujoče politike SI-TRUST obvesti nadzorni organ o vseh načrtovanih spremembah pri zagotavljanju svojih kvalificiranih storitev zaupanja, kakor tudi o morebitni nameri prenehanja opravljanja teh storitev.

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

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

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

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

9.12.2. Veljavnost in objava sprememb

Spremembe politike SI-TRUST se sedem (7) dni pred veljavo predhodno objavi na spletnih straneh SI-TRUST 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 posameznega izdajatelja se označi z novo identifikacijsko oznako dokumenta (CP_{OID}).

(2) Korenskemu izdajatelju SI-TRUST Root podrejeni ali z njim povezani 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

SI-TRUST in posamezni izdajatelj delujeta v skladu z:

- 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,
- Uredbo (EU) št. 679/2016 Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih

podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 1995/46/ES,
- Zakonom o elektronski identifikaciji in storitvah zaupanja,
- Zakonom o varstvu osebnih podatkov,
- Zakonom o tajnih podatkih,
- Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih,
- priporočili ETSI s področja kvalificiranih potrdil in storitev zaupanja,
- priporočili RFC s področja potrdil X.509,
- zahtevami organizacije CA/Browser Forum (»Baseline Requirements« in »EV SSL Certificate Guidelines«),
- in drugimi veljavnimi predpisi in priporočili.

9.15. Skladnost z veljavno zakonodajo

Nadzor nad skladnostjo delovanja SI-TRUST 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 SI-TRUST zavezujejo na podlagi drugih pogodb ali dogovorov oziroma druge veljavne zakonodaje.

9.16.2. Prenos pravic

Potrdilo, ki ga posamezni izdajatelj izda imetniku 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

SI-TRUST ni odgovoren za škodo, ki bi nastala zaradi višje sile, na katero ponudnik storitev zaupanja 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 SI-TRUST in imetnikom ali tretjo osebo, veljajo določila pogodbe ali dogovora.

9.17.3. Odstopanje od določil

Če posamezni izdajatelj 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.