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 20. oktobra 2020
verzija: 2.2

CP_{Name}: SI-TRUST Root
CP_{OID}: 1.3.6.1.4.1.6105.6.1.2

Zgodovina politik

Izdaje politik delovanja SI-TRUST Root	
verzija: 2.2, veljavnost: od 20. oktobra 2020	
Politika SI-TRUST Root za korenskega izdajatelja digitalnih potrdil za podrejene in povezane izdajatelje kvalificiranih digitalnih potrdil CP_{OID}: 1.3.6.1.4.1.6105.6.1.2 CP_{Name}: SI-TRUST Root	*Revizija dokumenta*
verzija: 2.1, veljavnost: od 1. oktobra 2019	
Politika SI-TRUST Root za korenskega izdajatelja digitalnih potrdil za podrejene in povezane izdajatelje kvalificiranih digitalnih potrdil CP_{OID}: 1.3.6.1.4.1.6105.6.1.2 CP_{Name}: SI-TRUST Root	*Revizija dokumenta*
verzija: 2.0, veljavnost: od 28. maja 2018	
Politika SI-TRUST Root za korenskega izdajatelja digitalnih potrdil za podrejene in povezane izdajatelje kvalificiranih digitalnih potrdil CP_{OID}: 1.3.6.1.4.1.6105.6.1.2 CP_{Name}: SI-TRUST Root	*Spremembe z verzijo 2.0:* • *uvedena je Krovna politika SI-TRUST za izdajatelje, ki delujejo v okviru ponudnika storitev zaupanja SI-TRUST, zato se pričujoča politika v določenih točkah sklicuje nanjo,* • *izrazi in okrajšave so usklajeni z veljavno zakonodajo.*
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

1. UVOD 11

1.1. Pregled 11

1.2. Identifikacijski podatki politike delovanja 11

1.3. Udeleženci infrastrukture javnih ključev 11
1.3.1. Ponudnik storitev zaupanja 12
1.3.2. Prijavna služba 12
1.3.3. Imetniki potrdil 12
1.3.4. Tretje osebe 13
1.3.5. Ostali udeleženci 13

1.4. Namen uporabe potrdil 13
1.4.1. Pravilna uporaba potrdil in ključev 13
1.4.2. Nedovoljena uporaba potrdil in ključev 14

1.5. Upravljanje s politiko 14
1.5.1. Upravljavec politike 14
1.5.2. Kontaktne osebe 14
1.5.3. Odgovorna oseba glede skladnosti delovanja izdajatelja s politiko 14
1.5.4. Postopek za sprejem nove politike 14

1.6. Izrazi in okrajšave 14
1.6.1. Izrazi 14
1.6.2. Okrajšave 14

2. OBJAVE IN ODGOVORNOSTI GLEDE REPOZITORIJA 14

2.1. Repozitoriji 14

2.2. Objava informacij o potrdilih 15

2.3. Pogostnost javne objave 15

2.4. Dostop do repozitorijev 15

3. ISTOVETNOST IN VERODOSTOJNOST 16

3.1. Določanje imen 16
3.1.1. Oblika imen 16
3.1.2. Zahteva po smiselnosti imen 16
3.1.3. Uporaba anonimnih imen ali psevdonimov 16
3.1.4. Pravila za interpretacijo imen 16
3.1.5. Enoličnost imen 16
3.1.6. Priznavanje, verodostojnost in vloga blagovnih znamk 16

3.2. Začetno preverjanje istovetnosti 17
3.2.1. Metoda za dokazovanje lastništva zasebnega ključa 17
3.2.2. Preverjanje istovetnosti organizacij 17
3.2.3. Preverjanje istovetnosti fizičnih oseb 17
3.2.4. Nepreverjeni podatki pri začetnem preverjanju 17
3.2.5. Preverjanje pooblastil 18
3.2.6. Merila za medsebojno povezovanje 18

3.3. Istovetnost in verodostojnost ob obnovi potrdila 18
3.3.1. Istovetnost in verodostojnost ob obnovi 18
3.3.2. Istovetnost in verodostojnost ob obnovi po preklicu 18

3.4. Istovetnost in verodostojnost ob zahtevi za preklic 19

4. UPRAVLJANJE S POTRDILI 19

4.1. Zahtevek za pridobitev potrdila 19
4.1.1. Kdo lahko predloži zahtevek za pridobitev potrdila 19
4.1.2. Postopek za pridobitev potrdila in odgovornosti 19

4.2. Postopek ob sprejemu zahtevka za pridobitev potrdila 19
4.2.1. Postopek preverjanja istovetnosti in verodostojnosti bodočega imetnika 20
4.2.2. Odobritev/zavrnitev zahtevka 20
4.2.3. Čas za izdajo potrdila 20

4.3. Izdaja potrdila 20
4.3.1. Postopek izdajatelja ob izdaji potrdila 20
4.3.2. Obvestilo imetniku o izdaji potrdila 20

4.4. Prevzem potrdila 20
4.4.1. Postopek prevzema potrdila 21
4.4.2. Objava potrdila 21
4.4.3. Obvestilo o izdaji tretjim osebam 21

4.5. Uporaba potrdil in ključev 21
4.5.1. Uporaba potrdila in zasebnega ključa imetnika 21
4.5.2. Uporaba potrdila in javnega ključa za tretje osebe 21

4.6. Ponovna izdaja potrdila brez spremembe javnega ključa 21
4.6.1. Razlogi za ponovno izdajo potrdila 22
4.6.2. Kdo lahko zahteva ponovno izdajo 22
4.6.3. Postopek ob ponovni izdaji potrdila 22
4.6.4. Obvestilo imetniku o izdaji novega potrdila 22
4.6.5. Prevzem ponovno izdanega potrdila 22
4.6.6. Objava ponovno izdanega potrdila 22
4.6.7. Obvestilo o izdaji drugim subjektom 22

4.7. Obnova potrdila 22
4.7.1. Razlogi za obnovo potrdila 22
4.7.2. Kdo lahko zahteva obnovo potrdila 22
4.7.3. Postopek pri obnovi potrdila 23
4.7.4. Obvestilo imetniku o obnovi potrdila 23
4.7.5. Prevzem obnovljenega potrdila 23
4.7.6. Objava obnovljenega potrdila 23
4.7.7. Obvestilo o izdaji drugim subjektom 23

4.8. Sprememba potrdila 23
4.8.1. Razlogi za spremembo potrdila 23
4.8.2. Kdo lahko zahteva spremembo 23
4.8.3. Postopek ob spremembi potrdila 23
4.8.4. Obvestilo imetniku o izdaji novega potrdila 23
4.8.5. Prevzem spremenjenega potrdila 24
4.8.6. Objava spremenjenega potrdila 24
4.8.7. Obvestilo o izdaji drugim subjektom 24

4.9. Preklic in začasna razveljavitev potrdila 24
4.9.1. Razlogi za preklic 24
4.9.2. Kdo lahko zahteva preklic 24
4.9.3. Postopek za preklic 25
4.9.4. Čas za izdajo zahtevka za preklic 25
4.9.5. Čas od prejetega zahtevka za preklic do izvedbe preklica 25
4.9.6. Zahteve po preverjanju registra preklicanih potrdil za tretje osebe 25
4.9.7. Pogostnost objave registra preklicanih potrdil 25

4.9.8. Čas do objave registra preklicanih potrdil 25
4.9.9. Sprotno preverjanje statusa potrdil 26
4.9.10. Zahteve za sprotno preverjanje statusa potrdil 26
4.9.11. Drugi načini za dostop do statusa potrdil 26
4.9.12. Druge zahteve pri zlorabi zasebnega ključa 26
4.9.13. Razlogi za začasno razveljavitev 26
4.9.14. Kdo lahko zahteva začasno razveljavitev 26
4.9.15. Postopek za začasno razveljavitev 26
4.9.16. Čas začasne razveljavitve 26

4.10. Preverjanje statusa potrdil 26
4.10.1. Dostop za preverjanje 26
4.10.2. Razpoložljivost 27
4.10.3. Druge možnosti 27

4.11. Prekinitev razmerja med imetnikom in ponudnikom storitev zaupanja 27

4.12. Odkrivanje kopije ključev za dešifriranje 27
4.12.1. Postopek za odkrivanje ključev za dešifriranje 27
4.12.2. Postopek za odkrivanje ključa seje 27

5. UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE 27

5.1. Fizično varovanje 27
5.1.1. Lokacija in zgradba ponudnika storitev zaupanja 27
5.1.2. Fizični dostop do infrastrukture ponudnika storitev zaupanja 27
5.1.3. Napajanje in prezračevanje 28
5.1.4. Zaščita pred poplavo 28
5.1.5. Zaščita pred požari 28
5.1.6. Hramba nosilcev podatkov 28
5.1.7. Odstranjevanje odpadkov 28
5.1.8. Hramba na oddaljeni lokaciji 28

5.2. Organizacijska struktura izdajatelja oz. ponudnika storitev zaupanja 28
5.2.1. Organizacija ponudnika storitev zaupanja in zaupanja vredne vloge 28
5.2.2. Število oseb za posamezne vloge 28
5.2.3. Izkazovanje istovetnosti za opravljanje posameznih vlog 28
5.2.4. Nezdružljivost vlog 28

5.3. Nadzor nad osebjem 29
5.3.1. Potrebne kvalifikacije in izkušnje osebja ter njegova primernost 29
5.3.2. Preverjanje primernosti osebja 29
5.3.3. Izobraževanje osebja 29
5.3.4. Zahteve za redna usposabljanja 29
5.3.5. Menjava nalog 29
5.3.6. Sankcije 29
5.3.7. Zahteve za zunanje izvajalce 29
5.3.8. Dostop osebja do dokumentacije 29

5.4. Varnostni pregledi sistema 29
5.4.1. Vrste beleženih dogodkov 29
5.4.2. Pogostost pregledov dnevnikov beleženih dogodkov 30
5.4.3. Čas hrambe dnevnikov beleženih dogodkov 30
5.4.4. Zaščita dnevnikov beleženih dogodkov 30
5.4.5. Varnostne kopije dnevnikov beleženih dogodkov 30
5.4.6. Zbiranje podatkov za dnevnike beleženih dogodkov 30
5.4.7. Obveščanje povzročitelja dogodka 30
5.4.8. Ocena ranljivosti sistema 30

5.5. Arhiviranje podatkov 30
5.5.1. Vrste arhiviranih podatkov 30
5.5.2. Čas hrambe 30
5.5.3. Zaščita arhiviranih podatkov 31
5.5.4. Varnostno kopiranje arhiviranih podatkov 31
5.5.5. Zahteva po časovnem žigosanju 31
5.5.6. Način zbiranja arhiviranih podatkov 31
5.5.7. Postopek za dostop do arhiviranih podatkov in njihova verifikacija 31

5.6. Obnova izdajateljevega potrdila 31

5.7. Okrevalni načrt 31
5.7.1. Postopek v primeru vdorov in zlorabe 31
5.7.2. Postopek v primeru okvare strojne in programske opreme ali podatkov 31
5.7.3. Postopek v primeru ogroženega zasebnega ključa izdajatelja 31
5.7.4. Okrevalni načrt 31

5.8. Prenehanje delovanja izdajatelja 32

6. TEHNIČNE VARNOSTNE ZAHTEVE 32

6.1. Generiranje in namestitev ključev 32
6.1.1. Generiranje ključev 32
6.1.2. Dostava zasebnega ključa imetnikom 32
6.1.3. Dostava javnega ključa izdajatelju potrdil 32
6.1.4. Dostava izdajateljevega javnega ključa tretjim osebam 32
6.1.5. Dolžina ključev 32
6.1.6. Generiranje in kakovost parametrov javnih ključev 33
6.1.7. Namen ključev in potrdil 33

6.2. Zaščita zasebnega ključa in varnostni moduli 33
6.2.1. Standardi za kriptografski modul 33
6.2.2. Nadzor zasebnega ključa s strani pooblaščenih oseb 33
6.2.3. Odkrivanje kopije zasebnega ključa 33
6.2.4. Varnostna kopija zasebnega ključa 33
6.2.5. Arhiviranje zasebnega ključa 33
6.2.6. Prenos zasebnega ključa iz/v kriptografski modul 33
6.2.7. Zapis zasebnega ključa v kriptografskem modulu 34
6.2.8. Postopek za aktiviranje zasebnega ključa 34
6.2.9. Postopek za deaktiviranje zasebnega ključa 34
6.2.10. Postopek za uničenje zasebnega ključa 34
6.2.11. Lastnosti kriptografskega modula 34

6.3. Ostali vidiki upravljanja ključev 34
6.3.1. Arhiviranje javnega ključa 34
6.3.2. Obdobje veljavnosti potrdila in ključev 34

6.4. Gesla za dostop do zasebnega ključa 35
6.4.1. Generiranje gesel 35
6.4.2. Zaščita gesel 35
6.4.3. Drugi vidiki gesel 35

6.5. Varnostne zahteve za računalniško opremo izdajatelja 35
6.5.1. Specifične tehnične varnostne zahteve 35
6.5.2. Nivo varnostne zaščite 35

6.6. Tehnični nadzor življenjskega cikla izdajatelja 35
6.6.1. Nadzor razvoja sistema 35
6.6.2. Upravljanje varnosti 35

6.6.3. Nadzor življenjskega cikla ... 36
6.7. Varnostna kontrola računalniške mreže ... 36
6.8. Časovno žigosanje ... 36
7. PROFIL POTRDIL, REGISTRA PREKLICANIH POTRDIL IN SPROTNEGA PREVERJANJA STATUSA POTRDIL ... 36
7.1. Profil potrdil ... 36
7.1.1. Različica potrdil ... 36
7.1.2. Profil potrdil z razširitvami ... 36
7.1.3. Identifikacijske oznake algoritmov ... 38
7.1.4. Oblika imen ... 38
7.1.5. Omejitve glede imen ... 38
7.1.6. Oznaka politike potrdila ... 38
7.1.7. Uporaba razširitvenega polja za omejitev uporabe politik ... 38
7.1.8. Oblika in obravnava specifičnih podatkov o politiki ... 38
7.1.9. Obravnava kritičnega razširitvenega polja politike ... 38
7.2. Profil registra preklicanih potrdil ... 38
7.2.1. Različica ... 39
7.2.2. Vsebina registra in razširitve ... 39
7.3. Profil sprotnega preverjanja statusa potrdil ... 40
7.3.1. Različica ... 40
7.3.2. Razširitve sprotnega preverjanje statusa ... 40
8. INŠPEKCIJSKI NADZOR ... 40
8.1. Pogostnost inšpekcijskega nadzora ... 40
8.2. Inšpekcijska služba ... 40
8.3. Neodvisnost inšpekcijske službe ... 40
8.4. Področja inšpekcijskega nadzora ... 40
8.5. Ukrepi ponudnika storitev zaupanja ... 40
8.6. Objava rezultatov inšpekcijskega nadzora ... 40
9. OSTALE POSLOVNE IN PRAVNE ZADEVE ... 41
9.1. Cenik storitev ... 41
9.1.1. Cena izdaje in obnove potrdil ... 41
9.1.2. Cena dostopa do potrdil ... 41
9.1.3. Cena dostopa do statusa potrdila in registra preklicanih potrdil ... 41
9.1.4. Cene drugih storitev ... 41
9.1.5. Povrnitev stroškov ... 41
9.2. Finančna odgovornost ... 41
9.2.1. Zavarovalniško kritje ... 41
9.2.2. Drugo kritje ... 41
9.2.3. Zavarovanje imetnikov ... 41
9.3. Varovanje poslovnih podatkov ... 42
9.3.1. Varovani podatki ... 42
9.3.2. Nevarovani podatki ... 42
9.3.3. Odgovornost glede varovanja poslovnih podatkov ... 42
9.4. Varovanje osebnih podatkov ... 42
9.4.1. Načrt varovanja osebnih podatkov ... 42
9.4.2. Varovani osebni podatki ... 42

9.4.3. Nevarovani osebni podatki ... 42
9.4.4. Odgovornost glede varovanja osebnih podatkov ... 42
9.4.5. Pooblastilo glede uporabe osebnih podatkov ... 42
9.4.6. Posredovanje osebnih podatkov na uradno zahtevo ... 42
9.4.7. Druga določila glede posredovanja osebnih podatkov ... 43

9.5. Določbe glede pravic intelektualne lastnine ... 43

9.6. Obveznosti in odgovornosti ... 43
9.6.1. Obveznosti in odgovornosti izdajatelja ... 43
9.6.2. Obveznosti in odgovornosti prijavne službe ... 43
9.6.3. Obveznosti in odgovornosti imetnika ... 43
9.6.4. Obveznosti in odgovornosti tretjih oseb ... 44
9.6.5. Obveznosti in odgovornosti drugih subjektov ... 44

9.7. Zanikanje odgovornosti ... 44

9.8. Omejitev odgovornosti ... 44

9.9. Poravnava škode ... 44

9.10. Veljavnost politike ... 44
9.10.1. Čas veljavnosti ... 44
9.10.2. Konec veljavnosti politike ... 44
9.10.3. Učinek poteka veljavnosti politike ... 44

9.11. Komuniciranje med subjekti ... 45

9.12. Spreminjanje dokumenta ... 45
9.12.1. Postopek uveljavitve sprememb ... 45
9.12.2. Veljavnost in objava sprememb ... 45
9.12.3. Sprememba identifikacijske oznake politike ... 45

9.13. Postopek v primeru sporov ... 45

9.14. Veljavna zakonodaja ... 45

9.15. Skladnost z veljavno zakonodajo ... 45

9.16. Splošne določbe ... 45
9.16.1. Celovit dogovor ... 45
9.16.2. Prenos pravic ... 45
9.16.3. Neodvisnost določil ... 46
9.16.4. Terjatve ... 46
9.16.5. Višja sila ... 46

9.17. Ostale določbe ... 46
9.17.1. Razumevanje določil ... 46
9.17.2. Nasprotujoča določila ... 46
9.17.3. Odstopanje od določil ... 46
9.17.4. Navzkrižno overjanje ... 46

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 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), 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.

Znotraj SI-TRUST 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 SI-TRUST 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.

Pričujoči dokument določa politiko korenskega izdajatelja SI-TRUST Root za podrejene in povezane izdajatelje kvalificiranih digitalnih potrdil. Na podlagi tega dokumenta SI-TRUST Root izdaja digitalna potrdila, ki izpolnjujejo najvišje varnostne zahteve, po politiki CP_{OID}: 1.3.6.1.4.1.6105.6.1.2.

Pričujoči dokument nadomešča prejšnjo objavljeno politiko SI-TRUST Root. 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).

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) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.

(2) Znotraj SI-TRUST 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 SI-TRUST kot korenski izdajatelj, pri povezovanju z zunanjimi izdajatelji pa kot premostitveni izdajatelj.

(3) Imetniki digitalnih potrdil, ki jih izdaja korenski izdajatelj SI-TRUST Root, so izdajatelji kvalificiranih potrdil. Korenski izdajatelj SI-TRUST Root izdaja:

- izdajateljem v okviru SI-TRUST 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) 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 SI-TRUST 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.

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

(6) 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 SI-TRUST, 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. Ponudnik storitev zaupanja

(1) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.
(2) 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:	https://www.si-trust.gov.si
Dežurna tel. številka za preklice (24 ur vse dni v letu):	01 4788 777

(3) Korenski izdajatelj SI-TRUST Root opravlja naslednje naloge:
- določa in objavlja svojo politiko delovanja,
- v okviru SI-TRUST 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.

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 SI-TRUST oz. upravni odbor SI-TRUST[1].

(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

[1] 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 SI-TRUST 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

Določbe so opredeljene v Krovni politiki SI-TRUST.

1.3.5. Ostali udeleženci

Določbe so opredeljene v Krovni politiki SI-TRUST.

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

Določbe so opredeljene v Krovni politiki SI-TRUST.

1.5. Upravljanje s politiko

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

1.5.1. Upravljavec politike

Določbe so opredeljene v Krovni politiki SI-TRUST.

1.5.2. Kontaktne osebe

Določbe so opredeljene v Krovni politiki SI-TRUST.

1.5.3. Odgovorna oseba glede skladnosti delovanja izdajatelja s politiko

Določbe so opredeljene v Krovni politiki SI-TRUST.

1.5.4. Postopek za sprejem nove politike

Določbe so opredeljene v Krovni politiki SI-TRUST.

1.6. Izrazi in okrajšave

1.6.1. Izrazi

Določbe so opredeljene v Krovni politiki SI-TRUST.

1.6.2. Okrajšave

Določbe so opredeljene v Krovni politiki SI-TRUST.

2. OBJAVE IN ODGOVORNOSTI GLEDE REPOZITORIJA

2.1. Repozitoriji

Določbe so opredeljene v Krovni politiki SI-TRUST.

2.2. Objava informacij o potrdilih

(1) SI-TRUST 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 SI-TRUST 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 https://www.si-trust.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 https://www.si-trust.gov.si.

(5) Zaupni del notranjih pravil SI-TRUST, 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) SI-TRUST 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

Določbe so opredeljene v Krovni politiki SI-TRUST.

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 SI-TRUST, 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 SI-TRUST 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 SI-TRUST 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 SI-TRUST 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

Določbe so opredeljene v Krovni politiki SI-TRUST.

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

(1) 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.

(2) Dokazilo o posedovanju sredstva za varno hranjenje zasebnih ključev in potrdil, ki jih podeli izdajatelj imetniku, se hrani pri SI-TRUST Root.

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 SI-TRUST 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 SI-TRUST 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 SI-TRUST 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 ponudnikov storitev zaupanja, 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) SI-TRUST ni dolžan priznati drugih izdajateljev tudi, če izpolnjujejo pogoje iz prvega odstavka. Končno odločitev o medsebojnemu povezovanju sprejme upravni odbor SI-TRUST.

(4) SI-TRUST zagotavlja, da bo izvajal medsebojno priznavanje izključno po podpisu pisne pogodbe oz. dogovora z drugimi ponudniki storitev zaupanja, ki morajo izpolnjevati raven varnostnih zahtev, ki je primerljiva ali višja, kot jo predpiše SI-TRUST.

(5) SI-TRUST 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 SI-TRUST za medsebojno priznavanje, krije drugi ponudnik storitev zaupanja.

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 SI-TRUST 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) SI-TRUST 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 SI-TRUST 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 SI-TRUST 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 SI-TRUST v skladu z odločitvijo upravnega odbora SI-TRUST.

(2) Postopek je podrobnejše opisan v interni politiki SI-TRUST 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 SI-TRUST 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 SI-TRUST 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 SI-TRUST, kot je navedeno v pogl.0.

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

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6. Ponovna izdaja potrdila brez spremembe javnega ključa

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6.1. Razlogi za ponovno izdajo potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6.2. Kdo lahko zahteva ponovno izdajo

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6.3. Postopek ob ponovni izdaji potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6.4. Obvestilo imetniku o izdaji novega potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6.5. Prevzem ponovno izdanega potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6.6. Objava ponovno izdanega potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.6.7. Obvestilo o izdaji drugim subjektom

Določbe so opredeljene v Krovni politiki SI-TRUST.

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

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.8.2. Kdo lahko zahteva spremembo

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.8.3. Postopek ob spremembi potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.8.4. Obvestilo imetniku o izdaji novega potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.8.5. Prevzem spremenjenega potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.8.6. Objava spremenjenega potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.8.7. Obvestilo o izdaji drugim subjektom

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9. Preklic in začasna razveljavitev potrdila[2]

4.9.1. Razlogi za preklic

(1) Preklic se lahko zahteva v primeru razkritja ključa ali drugih razlogov, ki vplivajo na nivo zaupanja in 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 ponudnika storitev zaupanja,
- 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 SI-TRUST 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 SI-TRUST prepovedano upravljanje s potrdili in njegove dejavnosti ni prevzel drug ponudnik storitev zaupanja,
- da je preklic odredilo pristojno sodišče ali upravni organ.

4.9.2. Kdo lahko zahteva preklic

(1) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.

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

(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 SI-TRUST 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 SI-TRUST 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 SI-TRUST 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 SI-TRUST.

(2) Če je delovanje SI-TRUST zaradi nepredvidenih dogodkov bistveno okrnjeno, se preklic zaradi nevarnosti zlorabe ali nezanesljivosti ipd. izvede najkasneje v štiriindvajsetih (24) urah po odločitvi upravnega odbora SI-TRUST.

(3) Po preklicu je 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

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.7. Pogostnost objave registra preklicanih potrdil

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.8. Čas do objave registra preklicanih potrdil

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.9. Sprotno preverjanje statusa potrdil

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.10. Zahteve za sprotno preverjanje statusa potrdil

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.11. Drugi načini za dostop do statusa potrdil

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.12. Druge zahteve pri zlorabi zasebnega ključa

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.13. Razlogi za začasno razveljavitev

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.14. Kdo lahko zahteva začasno razveljavitev

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.15. Postopek za začasno razveljavitev

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.16. Čas začasne razveljavitve

Določbe so opredeljene v Krovni politiki SI-TRUST.

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 https://www.si-trust.gov.si/sl/podpora-uporabnikom/korenski-izdajatelj-si-trust-root/, 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

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.10.3. Druge možnosti

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.11. Prekinitev razmerja med imetnikom in ponudnikom storitev zaupanja

(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

Določbe so opredeljene v Krovni politiki SI-TRUST.

5. UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE

5.1. Fizično varovanje

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.1.1. Lokacija in zgradba ponudnika storitev zaupanja

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.1.2. Fizični dostop do infrastrukture ponudnika storitev zaupanja

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.1.3. Napajanje in prezračevanje

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.1.4. Zaščita pred poplavo

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.1.5. Zaščita pred požari

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.1.6. Hramba nosilcev podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.1.7. Odstranjevanje odpadkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.1.8. Hramba na oddaljeni lokaciji

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.2. Organizacijska struktura izdajatelja oz. ponudnika storitev zaupanja

5.2.1. Organizacija ponudnika storitev zaupanja in zaupanja vredne vloge

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.2.2. Število oseb za posamezne vloge

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.2.3. Izkazovanje istovetnosti za opravljanje posameznih vlog

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.2.4. Nezdružljivost vlog

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3. Nadzor nad osebjem

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3.1. Potrebne kvalifikacije in izkušnje osebja ter njegova primernost

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3.2. Preverjanje primernosti osebja

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3.3. Izobraževanje osebja

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3.4. Zahteve za redna usposabljanja

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3.5. Menjava nalog

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3.6. Sankcije

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3.7. Zahteve za zunanje izvajalce

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.3.8. Dostop osebja do dokumentacije

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4. Varnostni pregledi sistema

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4.1. Vrste beleženih dogodkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4.2. Pogostost pregledov dnevnikov beleženih dogodkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4.3. Čas hrambe dnevnikov beleženih dogodkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4.4. Zaščita dnevnikov beleženih dogodkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4.5. Varnostne kopije dnevnikov beleženih dogodkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4.6. Zbiranje podatkov za dnevnike beleženih dogodkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4.7. Obveščanje povzročitelja dogodka

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.4.8. Ocena ranljivosti sistema

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.5. Arhiviranje podatkov

5.5.1. Vrste arhiviranih podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.5.2. Čas hrambe

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.5.3. Zaščita arhiviranih podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.5.4. Varnostno kopiranje arhiviranih podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.5.5. Zahteva po časovnem žigosanju

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.5.6. Način zbiranja arhiviranih podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.5.7. Postopek za dostop do arhiviranih podatkov in njihova verifikacija

Določbe so opredeljene v Krovni politiki SI-TRUST.

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

Določbe so opredeljene v Krovni politiki SI-TRUST.

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

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.7.3. Postopek v primeru ogroženega zasebnega ključa izdajatelja

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.7.4. Okrevalni načrt

Določbe so opredeljene v Krovni politiki SI-TRUST.

5.8. Prenehanje delovanja izdajatelja

Določbe so opredeljene v Krovni politiki SI-TRUST.

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 SI-TRUST 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 SI-TRUST (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

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.1.7. Namen ključev in potrdil

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.2. Zaščita zasebnega ključa in varnostni moduli

6.2.1. Standardi za kriptografski modul

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.2.2. Nadzor zasebnega ključa s strani pooblaščenih oseb

Določbe so opredeljene v Krovni politiki SI-TRUST.

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 SI-TRUST.

(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) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.

(2) 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

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.2.8. Postopek za aktiviranje zasebnega ključa

(1) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.

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

6.2.9. Postopek za deaktiviranje zasebnega ključa

(1) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.

(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) Skupne določbe so opredeljene v Krovni politiki SI-TRUST.

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

6.2.11. Lastnosti kriptografskega modula

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.3. Ostali vidiki upravljanja ključev

6.3.1. Arhiviranje javnega ključa

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.3.2. Obdobje veljavnosti potrdila in ključev

(1) Veljavnosti digitalnih potrdil, ki jih za izdajatelje znotraj SI-TRUST 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 in 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 SI-TRUST.

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 SI-TRUST.

6.4.3. Drugi vidiki gesel

Niso predpisani.

6.5. Varnostne zahteve za računalniško opremo izdajatelja

6.5.1. Specifične tehnične varnostne zahteve

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.5.2. Nivo varnostne zaščite

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.6. Tehnični nadzor življenjskega cikla izdajatelja

6.6.1. Nadzor razvoja sistema

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.6.2. Upravljanje varnosti

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.6.3. Nadzor življenjskega cikla

Določbe so opredeljene v Krovni politiki SI-TRUST.

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 SI-TRUST.

6.8. Časovno žigosanje

Določbe so opredeljene v Krovni politiki SI-TRUST.

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. **Napaka! Vira sklicevanja ni bilo mogoče najti.**.

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 SI-TRUST: 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 (OID 1.3.6.1.5.5.7.48.1) Access Location: URL=http://ocsp.ca.gov.si Access Method: CaIssuer (OID 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

Določbe so opredeljene v Krovni politiki SI-TRUST.

7.1.4. Oblika imen

Določbe so opredeljene v Krovni politiki SI-TRUST.

7.1.5. Omejitve glede imen

Določbe so opredeljene v Krovni politiki SI-TRUST.

7.1.6. Oznaka politike potrdila

Določbe so opredeljene v Krovni politiki SI-TRUST.

7.1.7. Uporaba razširitvenega polja za omejitev uporabe politik

Določbe so opredeljene v Krovni politiki SI-TRUST.

7.1.8. Oblika in obravnava specifičnih podatkov o politiki

Določbe so opredeljene v Krovni politiki SI-TRUST.

7.1.9. Obravnava kritičnega razširitvenega polja politike

Določbe so opredeljene v Krovni politiki SI-TRUST.

7.2. Profil registra preklicanih potrdil

7.2.1. Različica

Določbe so opredeljene v Krovni politiki SI-TRUST.

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

Določbe so opredeljene v Krovni politiki SI-TRUST.

7.3.2. Razširitve sprotnega preverjanje statusa

Določbe so opredeljene v Krovni politiki SI-TRUST.

8. INŠPEKCIJSKI NADZOR

8.1. Pogostnost inšpekcijskega nadzora

Določbe so opredeljene v Krovni politiki SI-TRUST.

8.2. Inšpekcijska služba

Določbe so opredeljene v Krovni politiki SI-TRUST.

8.3. Neodvisnost inšpekcijske službe

Določbe so opredeljene v Krovni politiki SI-TRUST.

8.4. Področja inšpekcijskega nadzora

Določbe so opredeljene v Krovni politiki SI-TRUST.

8.5. Ukrepi ponudnika storitev zaupanja

Določbe so opredeljene v Krovni politiki SI-TRUST.

8.6. Objava rezultatov inšpekcijskega nadzora

Določbe so opredeljene v Krovni politiki SI-TRUST.

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

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.1.5. Povrnitev stroškov

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.2. Finančna odgovornost

9.2.1. Zavarovalniško kritje

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.2.2. Drugo kritje

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.2.3. Zavarovanje imetnikov

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.3. Varovanje poslovnih podatkov

9.3.1. Varovani podatki

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.3.2. Nevarovani podatki

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.3.3. Odgovornost glede varovanja poslovnih podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.4. Varovanje osebnih podatkov

9.4.1. Načrt varovanja osebnih podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.4.2. Varovani osebni podatki

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.4.3. Nevarovani osebni podatki

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.4.4. Odgovornost glede varovanja osebnih podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST.

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 so opredeljene v Krovni politiki SI-TRUST.

9.6. Obveznosti in odgovornosti

9.6.1. Obveznosti in odgovornosti izdajatelja

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.6.2. Obveznosti in odgovornosti prijavne službe

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

(2) Upravni odbor SI-TRUST 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

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.6.5. Obveznosti in odgovornosti drugih subjektov

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.7. Zanikanje odgovornosti

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.8. Omejitev odgovornosti

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

9.9. Poravnava škode

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.10. Veljavnost politike

9.10.1. Čas veljavnosti

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.10.2. Konec veljavnosti politike

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.10.3. Učinek poteka veljavnosti politike

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.11. Komuniciranje med subjekti

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.12. Spreminjanje dokumenta

9.12.1. Postopek uveljavitve sprememb

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.12.2. Veljavnost in objava sprememb

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.12.3. Sprememba identifikacijske oznake politike

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.13. Postopek v primeru sporov

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.14. Veljavna zakonodaja

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.15. Skladnost z veljavno zakonodajo

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.16. Splošne določbe

9.16.1. Celovit dogovor

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.16.2. Prenos pravic

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.16.3. Neodvisnost določil

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.16.4. Terjatve

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.16.5. Višja sila

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.17. Ostale določbe

9.17.1. Razumevanje določil

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.17.2. Nasprotujoča določila

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.17.3. Odstopanje od določil

Določbe so opredeljene v Krovni politiki SI-TRUST.

9.17.4. Navzkrižno overjanje

Določbe so opredeljene v Krovni politiki SI-TRUST.