Državni center za storitve zaupanja
Izdajatelj kvalificiranih digitalnih potrdil
SI-TRUST eID Podpis

SI-TRUST
SI-TRUST eID Podpis

POLITIKA SI-TRUST eID Podpis
za kvalificirana potrdila za elektronski podpis na osebni izkaznici

Javni del notranjih pravil Državnega centra za storitve zaupanja

veljavnost: od 14. marca 2025
verzija: 1.3

CP_{Name}: SI-TRUST eID Podpis
CP_{OID}: 1.3.6.1.4.1.6105.9.1.1

© Državni center za storitve zaupanja

Zgodovina politik

Izdaje politik delovanja SI-TRUST eID Podpis	
verzija: 1.3, veljavnost: od 14. marca 2025	
Politika SI-TRUST eID Podpis za kvalificirana digitalna potrdila za elektronski podpis na osebni izkaznici CP_{OID}: 1.3.6.1.4.1.6105.9.1.1 CP_{Name}: SI-TRUST eID Podpis	*Revizija dokumenta*
verzija: 1.2, veljavnost: od 12. decembra 2023	
Politika SI-TRUST eID Podpis za kvalificirana digitalna potrdila za elektronski podpis na osebni izkaznici CP_{OID}: 1.3.6.1.4.1.6105.9.1.1 CP_{Name}: SI-TRUST eID Podpis	*Spremembe z verzijo 1.2:* • *spremenjeni so kontaktni podatki SI-TRUST,* • *revizija dokumenta.*
verzija: 1.1, veljavnost: od 5. decembra 2022	
Politika SI-TRUST eID Podpis za kvalificirana digitalna potrdila za elektronski podpis na osebni izkaznici CP_{OID}: 1.3.6.1.4.1.6105.9.1.1 CP_{Name}: SI-TRUST eID Podpis	*Revizija dokumenta*
verzija: 1.0, veljavnost: od 28. marca 2022	
Politika SI-TRUST eID Podpis za kvalificirana digitalna potrdila za elektronski podpis na osebni izkaznici CP_{OID}: 1.3.6.1.4.1.6105.9.1.1 CP_{Name}: SI-TRUST eID Podpis	/

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 digitalno preobrazbo (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 elektronsko identifikacijo in avtentikacijo imetnikov v skladu z zakonodajo s področja elektronske identifikacije,
- 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 izdajatelj kvalificiranih digitalnih potrdil SI-TRUST eID Podpis (angl. *Slovenian Trust Service eID Signature Certification Authority*), https://www.si-trust.gov.si/sl/eoi/, ki izdaja kvalificirana digitalna potrdila za elektronski podpis na osebni izkaznici (v nadaljevanju digitalna potrdila).

Izdajatelj SI-TRUST eID Podpis je registriran v skladu z veljavno zakonodajo in priznan s strani korenskega izdajatelja SI-TRUST Root (angl. *Slovenian Trust Service Root Certification Authority*).

Politika delovanja SI-TRUST eID Podpis za kvalificirana digitalna potrdila za elektronski podpis na osebni izkaznici določa notranja pravila delovanja izdajatelja, ki definirajo namen, delovanje in metodologijo upravljanja z digitalnimi potrdili, odgovornosti in zahteve, ki jih morajo izpolnjevati vsi subjekti.

Pričujoči dokument določa politiko izdajatelja SI-TRUST eID Podpis za kvalificirana digitalna potrdila za elektronski podpis na osebni izkaznici. Na podlagi tega dokumenta SI-TRUST eID Podpis izdaja spletna kvalificirana digitalna potrdila, ki izpolnjujejo najvišje varnostne zahteve, po politiki CP_{OID}: 1.3.6.1.4.1.6105.9.1.1.

Digitalna potrdila SI-TRUST eID Podpis so nameščena na osebni izkaznici, ki jo Republika Slovenija izdaja svojim državljanom. Osebna izkaznica državljana od dopolnjenega 12. leta starosti vsebuje sredstvo elektronske identifikacije visoke ravni zanesljivosti, sredstvo elektronske identifikacije nizke ravni zanesljivosti in kvalificirano potrdilo za elektronski podpis. Organ, pristojen za izdajo osebne izkaznice, je upravna enota ali diplomatsko-konzularno predstavništvo Republike Slovenije.

Čip osebne izkaznice je naprava za ustvarjanje kvalificiranega elektronskega podpisa. Kvalificirano potrdilo za elektronski podpis je povezano z enim parom eliptičnih asimetričnih ključev, ki se v postopku personalizacije, skupaj s sredstvom elektronske identifikacije visoke ravni zanesljivosti in sredstvom elektronske identifikacije nizke ravni zanesljivosti, zapiše na čip osebne izkaznice.

Veljavnost kvalificiranega potrdila za elektronski podpis je od datuma veljavnosti osebne izkaznice do datuma, do katerega velja osebna izkaznica ob izdaji, oz. deset let od datuma veljavnosti osebne izkaznice na osebni izkaznici s trajno veljavnostjo.

Podatke za prevzem digitalnega potrdila pripravi SI-TRUST, njegov zapis na čip osebne izkaznice pa v postopku personalizacije osebne izkaznice izvede izbrani izvajalec, odgovoren za izdelavo, personalizacijo in prenos osebnih izkaznic (v nadaljevanju izvajalec personalizacije). Izvajalec personalizacije po zaključku personalizacije onemogoči brisanje shranjenih zapisov (zasebnega ključa in digitalnega potrdila) in dodajanje novih zapisov na čip osebne izkaznice s strani imetnika. Izdelano osebno izkaznico se bodočemu imetniku vroči skladno z določili zakonodaje, ki ureja osebno izkaznico. Bodoči imetnik prejme tudi začetno geslo za dostop do digitalnega potrdila.

Zasebni ključ, shranjen na čipu osebne izkaznice, je zaščiten z uporabniškim geslom, ki ga mora uporabnik vnesti pred vsako uporabo digitalnega potrdila oz. zasebnega ključa. Uporabniško geslo si imetnik nastavi pred prvo uporabo sredstva elektronske identifikacije visoke ravni zanesljivosti ali kvalificiranega potrdila za elektronski podpis, tako da uporabi začetno geslo za dostop do digitalnega potrdila. Če imetnik uporabniškega gesla ne pozna ali je neuporabno zaradi prevelikega števila neuspešnih poskusov vnosa, lahko pridobi kodo za ponastavitev uporabniškega gesla.

SI-TRUST poleg podatkov, ki so vključeni v digitalno potrdilo, hrani ostale potrebne podatke o imetniku za namen elektronskega poslovanja v skladu z veljavnimi predpisi.

Imetnik mora z osebno izkaznico ravnati skrbno in v skladu z navodili, ki jih prejme ob njeni vročitvi. Prav tako mora skrbno varovati zasebni ključ in svoje kvalificirano potrdilo ter ravnati v skladu s politiko, obvestili izdajatelja SI-TRUST eID Podpis in veljavno zakonodajo.

1. UVOD

1.1. Pregled

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

(2) Znotraj SI-TRUST deluje izdajatelj SI-TRUST eID Podpis (angl. *Slovenian Trust Service eID Signature Certification Authority*), https://www.si-trust.gov.si/sl/eoi/, ki izdaja kvalificirana digitalna potrdila za elektronski podpis. Pričujoči dokument določa politike izdajatelja SI-TRUST eID Podpis za kvalificirana potrdila za elektronski podpis na osebni izkaznici.

(3) Izdajatelj SI-TRUST eID Podpis je registriran v skladu z veljavno zakonodajo in priznan s strani korenskega izdajatelja SI-TRUST Root (angl. *Slovenian Trust Service Root Certification Authority*).

(4) Po pričujoči politiki SI-TRUST eID Podpis izdaja kvalificirana potrdila za elektronski podpis po CP_{OID}: 1.3.6.1.4.1.6105.9.1.1.

(5) Digitalna potrdila SI-TRUST eID Podpis se lahko uporabljajo za:
- overjanje digitalno podpisanih podatkov v elektronski obliki ter izkazovanje istovetnosti imetnika,
- storitve oz. aplikacije, za katere se zahteva uporaba kvalificiranih digitalnih potrdil SI-TRUST.

(6) Za potrdila, izdana na podlagi te politike, je potrebno upoštevati priporočila izdajatelja SI-TRUST eID Podpis za zaščito zasebnih ključev oz. uporabo varnih kriptografskih modulov.

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

(8) Medsebojna razmerja med tretjimi osebami, ki se zanašajo na potrdila izdajatelja SI-TRUST eID Podpis, in SI-TRUST se izvajajo tudi na podlagi morebitnega pisnega dogovora.

(9) SI-TRUST se preko korenskega izdajatelja SI-TRUST Root lahko povezuje z drugimi ponudniki storitev zaupanja, kar se ureja z medsebojnim dogovorom oz. pogodbo.

1.2. Identifikacijski podatki politike delovanja

(1) Pričujoči dokument je Politika SI-TRUST eID Podpis za kvalificirana potrdila za elektronski podpis na osebni izkaznici (v nadaljevanju *politika SI-TRUST eID Podpis*).

(2) Oznaka pričujoče politike je CP_{Name}: SI-TRUST eID Podpis, identifikacijska oznaka politike SI-TRUST eID Podpis pa CP_{OID}: 1.3.6.1.4.1.6105.9.1.1.

(3) V vsakem potrdilu je navedba ustrezne politike v obliki oznake CP_{OID}, glej podpogl. 7.1.2.

1.3. Udeleženci infrastrukture javnih ključev

1.3.1 Ponudnik storitev zaupanja

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

(2) V okviru SI-TRUST deluje izdajatelj kvalificiranih digitalnih potrdil SI-TRUST eID Podpis.

(3) Kontaktni podatki izdajatelja SI-TRUST eID Podpis so:

Naslov:	SI-TRUST eID Podpis Državni center za storitve zaupanja Ministrstvo za digitalno preobrazbo Tržaška cesta 21 1000 Ljubljana
E-pošta:	si-trust@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
Enotni kontaktni center:	080 2002, 01 4788 590 ekc@gov.si

(4) Izdajatelj SI-TRUST eID Podpis opravlja naslednje naloge:
- izdaja kvalificirana digitalna potrdila za elektronski podpis,
- določa in objavlja svojo politiko delovanja,
- določa obrazce za zahtevke za svoje storitve,
- določa in objavlja navodila in priporočila za varno uporabo svojih storitev,
- objavlja register preklicanih potrdil,
- skrbi za nemoteno delovanje svojih storitev v skladu s politiko in ostalimi predpisi,
- obvešča svoje uporabnike,
- skrbi za delovanje svoje prijavne službe in,
- opravlja vse ostale storitve v skladu s to politiko in ostalimi predpisi.

(5) Izdajatelj SI-TRUST eID Podpis je ob začetku svojega produkcijskega delovanja generiral svoje lastno digitalno potrdilo, ki je namenjeno overjanju potrdil, ki jih je SI-TRUST eID Podpis izdal imetnikom.

Potrdilo SI-TRUST eID Podpis vsebuje naslednje podatke[1]:

Naziv polja	Vrednost potrdila izdajatelja SI-TRUST eID Podpis
Osnovna polja v potrdilu	
Različica, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Number*	1158 BC8E 7B87 B50A D8FB 9862 9794 D00A A9DA 3A0C
Algoritem za podpis, angl. *Signature Algorithm*	sha384WithECDSA (OID 1.2.840.10045.4.3.3)

[1] Pomen je podan v podpogl. 3.1 in 7.1.

Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST eID Podpis
Imetnik, angl. *Subject*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST eID Podpis
Pričetek veljavnosti, angl. *Validity: Not Before*	Mar 15 14:17:58 2022 GMT
Konec veljavnosti, angl. *Validity: Not After*	Jun 15 23:59:59 2042 GMT
Algoritem za javni ključ, angl. *Public Key Algorithm*	P-384/secp384r1 (OID 1.3.132.0.34)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, angl. *ECC Public Key*	*ključ dolžine 384 bitov*
Razširitve X.509v3	
Uporaba ključa, OID 2.5.29.15, angl. *Key Usage*	Kritično (Critical) Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)
Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. *Authority Key Identifier*	F5C2 0034 9406 C208 AC6B 7D6D 1DAA 35A8 2441 16E9
Identifikator imetnikovega ključa, OID 2.5.29.14, angl. *Subject Key Identifier*	F5C2 0034 9406 C208 AC6B 7D6D 1DAA 35A8 2441 16E9
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA-1*	8BF2 514A 65A9 4D91 4ED7 EBF4 0CD3 E689 8714 2014
Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA-256*	0FAE DB67 8A08 D7E1 0D46 BC26 7602 7BF2 8232 AD80 D600 FAE9 8A36 4028 4C3F 59DC

(7) Korenski izdajatelj SI-TRUST Root je izdajatelju SI-TRUST eID Podpis izdal povezovalno potrdilo z naslednjimi podatki:

Nazivi polja Osnovna polja v potrdilu	Vrednost oz. pomen
Različica, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Number*	60cc e65c 0000 0000 571d d226
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 eID Podpis
Pričetek veljavnosti, angl. *Validity: Not Before*	Mar 21 10:01:16 2022 GMT
Konec veljavnosti, angl. *Validity: Not After*	Dec 21 10:31:16 2037 GMT

Algoritem za javni ključ, angl. *Subject Public Key Algorithm*	P-384/secp384r1 (OID 1.3.132.0.34)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, angl. *ECC Public Key*	*ključ dolžine 384 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 Root, oi=VATSI-17659957, o=Republika Slovenija, c=SI?certificateRevocationList c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root, cn=CRL1
Dostop do podatkov o izdajatelju, OID 1.3.6.1.5.5.7.1.1, angl. *Authority Information Access*	Access Method=OCSP http://ocsp.ca.gov.si Access Method=CA Issuers http://www.ca.gov.si/crt/si-trust-root.crt
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)
Politika, pod katero je bilo izdano potrdilo, OID 2.5.29.32, angl. *certificatePolicies*	Certificate Policy: PolicyIdentifier=2.5.29.32.0 (»anyPolicy«) [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.si-trust.gov.si/cps/
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. Author*ity Key Identifier*	4CA3 C368 5E08 0263
Identifikator imetnikovega ključa, OID 2.5.*29.14, angl. Subject Key Identifier*	F5C2 0034 9406 C208 AC6B 7D6D 1DAA 35A8 2441 16E9
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA-1*	B820 71FA CB59 BC58 D418 0E9E 2460 7DE9 A35A 8A6D
Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA-256*	0228 7E94 B50D 1FDA 51A0 B91B C3B2 E928 8B04 D174 BE0B E416 C06A 35BC 2792 F51C

1.3.2 Prijavna služba

(1) Naloge prijavne službe opravljajo upravne enote in diplomatsko-konzularna predstavništva Republike Slovenije kot organi, pristojni za izdajo osebne izkaznice. Prijavne službe morajo izpolnjevati pogoje za opravljanje nalog prijavnih služb SI-TRUST eID Podpis ter delovati v skladu z veljavnimi predpisi in poslovniki za delo prijavnih služb SI-TRUST eID Podpis.

(2) Naloge prijavne službe so:
- preverjanje istovetnosti imetnikov oz. bodočih imetnikov, njihovih podatkov in drugih potrebnih podatkov,
- sprejemanje zahtevkov za pridobitev kvalificiranih digitalnih potrdil za elektronski podpis na osebnih izkaznicah,
- sprejemanje zahtevkov za pridobitev kode za ponastavitev gesla,
- sprejemanje zahtevkov za preklic potrdil,
- preverjanje podatkov v zahtevkih,
- izdajanje potrebne dokumentacije imetnikom oz. bodočim imetnikom,
- posredovanje zahtevkov in ostalih podatkov na varen način na SI-TRUST.

1.3.3 Imetniki potrdil

Imetniki potrdil po tej politiki so državljani Republike Slovenije, ki so ob pridobitvi osebne izkaznice starejši od 12 let (angl. *subject*), glej definicijo v pogl. 1.6.

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 SI-TRUST eID Podpis, izdana po pričujoči politiki, se lahko uporabljajo za:
- overjanje digitalno podpisanih podatkov v elektronski obliki ter izkazovanje istovetnosti podpisnika,
- storitve oz. aplikacije, za katere se zahteva uporaba kvalificiranih digitalnih potrdil SI-TRUST.

(2) Uporaba potrdil je povezana z namenom pripadajočih ključev. Ločimo naslednji možnosti:
- zasebni ključ za podpisovanje in dešifriranje (v nadaljevanju *zasebni ključ*) ter
- javni ključ za overjanje podpisa in šifriranje (v nadaljevanju *javni ključ*).

(3) Izdajatelj SI-TRUST eID Podpis izdaja tudi potrdila za sistem OCSP za preverjanje veljavnosti potrdil, ki jih je izdal SI-TRUST eID Podpis.

1.4.1 Pravilna uporaba potrdil in ključev

(1) Namen potrdil oz. pripadajočih ključev je podan v potrdilu v polju *uporaba ključa* (angl. *Key Usage*).

(2) Vsakemu imetniku potrdila pripada en par ključev, ki ga sestavljata zasebni in javni ključ, ki sta namenjena za podpisovanje/overjanje podpisa.

1.4.2 Nedovoljena uporaba potrdil in ključev

Določbe so opredeljene v Krovni politiki SI-TRUST.

1.5. Upravljanje s politiko

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 izdajatelja SI-TRUST eID Podpis:

- politike delovanja izdajatelja,
- zahtevke za storitve izdajatelja,
- navodila za varno uporabo digitalnih potrdil,
- informacije o veljavni zakonodaji v zvezi z delovanjem SI-TRUST ter
- ostale informacije v zvezi z delovanjem SI-TRUST eID Podpis.

(2) Na spletni strani SI-TRUST, ki je dostopna na strežniku www.si-trust.gov.si, se objavlja register preklicanih digitalnih potrdil (podrobneje podan v podpogl. 7.2).

(3) Ostali dokumenti oz. ključni podatki o delovanju izdajatelja SI-TRUST eID Podpis ter splošna obvestila imetnikom in tretjim osebam se objavijo na spletnih straneh https://www.si-trust.gov.si.

(4) Zaupni del notranjih pravil SI-TRUST, znotraj katerega deluje izdajatelj SI-TRUST eID Podpis, ni javno dostopen dokument.

(5) SI-TRUST je odgovoren za pravočasnost in verodostojnost objavljenih dokumentov in ostalih podatkov.

2.3. Pogostnost javne objave

Določbe so opredeljene v Krovni politiki SI-TRUST.

2.4. Dostop do repozitorijev

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

(2) Če je delovanje SI-TRUST zaradi nepredvidenih dogodkov bistveno okrnjeno, bo SI-TRUST izvedel vse potrebne ukrepe, da bo omogočil ponovno dostopnost repozitorijev najkasneje v treh (3) delovnih dneh.

(3) Spletna stran SI-TRUST, ki hrani register preklicanih potrdil, je javno dostopna na strežniku www.si-trust.gov.si po protokolu HTTP oz. HTTPS.

(4) SI-TRUST oz. izdajatelj SI-TRUST eID Podpis v skladu z Interno politiko SI-TRUST skrbi za pooblaščeno in varno dodajanje, spreminjanje ali brisanje podatkov v registru preklicanih potrdil.

3. ISTOVETNOST IN VERODOSTOJNOST

3.1. Določanje imen

3.1.1 Oblika imen

(1) 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.

(2) V vsakem izdanem potrdilu je naveden izdajatelj le-tega, in sicer v polju *izdajatelj* (angl. *issuer*), glej tabelo v nadaljevanju.

(3) Razločevalno ime imetnikov vsebuje osnovne podatke o imetniku, in sicer v polju *imetnik (*angl. *subject)*, glej tabelo v nadaljevanju.

(4) Vsako razločevalno ime vključuje tudi serijsko številko, ki jo določi izdajatelj SI-TRUST eID Podpis[2] (glej podpogl. 3.1.5).

(5) Razločevalno ime se tvori po naslednjih pravilih[3].

Vrsta potrdila	Naziv polja	Razločevalno ime[4]
potrdilo izdajatelja SI-TRUST eID Podpis	Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST eID Podpis
kvalificirano potrdilo za elektronski podpis	Imetnik, angl. *Subject*	c=SI, st=Slovenija, ou=E-osebna izkaznica, ou=Kvalificirani elektronski podpis, cn=<ime in priimek> (eOI - podpis), gn=<ime>, surname=<priimek>, sn=<serijska številka>

3.1.2 Zahteva po smiselnosti imen

(1) Imetnik potrdila je nedvoumno določen z razločevalnim imenom v skladu s prejšnjim razdelkom.

(2) Podatki o imetniku v razločevalnem imenu vsebujejo znake iz kodne tabele UTF-8.

3.1.3 Uporaba anonimnih imen ali psevdonimov

Ni predvidena.

3.1.4 Pravila za interpretacijo imen

Pravila so navedena v podpogl. 3.1.1 in 3.1.2.

[2] Potrdilo izdajatelja SI-TRUST eID Podpis ne vsebuje serijske številke.
[3] Pravila za tvorbo razločevalnih imen za druge vrste potrdil določi in objavi SI-TRUST eID Podpis.
[4] Pomen posameznih označb: država (»c«), organizacija (»o«), organizacijska enota (»ou«), ime (»cn«), serijska številka (»sn«).

3.1.5 Enoličnost imen

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

(2) Enolična je tudi serijska številka, ki je vključena v razločevalno ime.

(3) Serijska številka je 13-mestno število in enolično določa imetnika oz. izdano potrdilo. Spodnja tabela natančneje določa pomen in vrednosti posameznih mest serijskega števila:

Serijska številka	Pomen	Vrednost
1. mesto	oznaka za potrdilo, ki je shranjeno na osebni izkaznici	4
2.- 8. mesto	enolično število imetnika	/
9. - 10. mesto	oznaka za kvalificirano potrdilo za elektronski podpis	40
11. – 12. mesto	zaporedno število istovrstnega potrdila	/
13. mesto	kontrolna številka	/

3.1.6 Priznavanje, verodostojnost in vloga blagovnih znamk

Določbe so opredeljene v Krovni politiki SI-TRUST.

3.2. Začetno preverjanje istovetnosti

3.2.1 Metoda za dokazovanje lastništva zasebnega ključa

Par ključev se generira z namenskim strojnim varnostnim modulom, s katerim upravlja izvajalec personalizacije, zato dokazovanje s strani bodočega imetnika ni potrebno. V okviru postopkov izdajatelja SI-TRUST eID Podpis ob izdaji potrdila se povezava med zasebnim in javnim ključem preverja z uporabo zahtevka v obliki PKCS#10 v skladu z RSA PKCS#10 Certification Request Syntax Standard.

3.2.2 Preverjanje istovetnosti organizacij

Ni predpisano.

3.2.3 Preverjanje istovetnosti fizičnih oseb

(1) Preverjanje istovetnosti imetnikov se izvede v skladu s postopki za pridobitev osebne izkaznice.

(2) Podatki za pridobitev kvalificiranega potrdila za elektronski podpis se pridobijo iz evidence osebnih izkaznic.

3.2.4 Nepreverjeni podatki pri začetnem preverjanju

Nepreverjenih podatkov v potrdilu ni.

3.2.5 Preverjanje pooblastil

Ni predpisano.

3.2.6 Merila za medsebojno povezovanje

(1) Izdajatelj SI-TRUST eID Podpis je medsebojno priznan s strani korenskega izdajatelja SI-TRUST Root.

(2) Izdajatelj SI-TRUST eID Podpis se medsebojno ne povezuje z drugimi izdajatelji.

(3) SI-TRUST se preko korenskega izdajatelja SI-TRUST Root lahko povezuje z drugimi ponudniki storitev zaupanja, kar se ureja z medsebojnim dogovorom oz. pogodbo.

3.3. Istovetnost in verodostojnost ob obnovi potrdila

3.3.1 Istovetnost in verodostojnost ob obnovi

Preverjanje imetnikov poteka skladno z določili iz podpogl. 3.2.3.

3.3.2 Istovetnost in verodostojnost ob obnovi po preklicu

Preverjanje imetnikov poteka skladno z določili iz podpogl. 3.2.3.

3.4. Istovetnost in verodostojnost ob zahtevi za preklic

(1) Zahtevek za preklic potrdila imetnik odda:
- osebno na prijavno službo, kjer pooblaščene osebe preverijo istovetnost prosilca,
- elektronsko, tako da se pred oddajo zahtevka identificira s sredstvom elektronske identifikacije najmanj srednje ravni zanesljivosti.

(2) Podroben postopek za preklic je podan v podpogl. 4.9.3.

4. UPRAVLJANJE S POTRDILI

4.1. Zahtevek za pridobitev potrdila

4.1.1 Kdo lahko predloži zahtevek za pridobitev potrdila

Bodoči imetniki potrdil so državljani Republike Slovenije, ki vložijo vlogo za izdajo osebne izkaznice in so ob vložitvi vloge starejši od 12 let, glej definicijo v podpogl. 1.3.3.

4.1.2 Postopek za pridobitev potrdila in odgovornosti

(1) Za pridobitev potrdila mora bodoči imetnik vložiti vlogo za izdajo osebne izkaznice v skladu s področno zakonodajo.

(2) Vloga za izdajo osebne izkaznice predstavlja tudi zahtevek za pridobitev potrdila.

4.2. Postopek ob sprejemu zahtevka za pridobitev potrdila

4.2.1 Preverjanje istovetnosti in verodostojnosti bodočega imetnika

(1) Preverjanje istovetnosti in verodostojnosti bodočega imetnika je opravljeno v skladu s postopki za pridobitev osebne izkaznice.

(2) Uradna oseba pristojnega organa ugotovi istovetnost državljana in preveri resničnost podatkov na vlogi za izdajo osebne izkaznice.

(3) Vlogo za izdajo osebne izkaznice lahko vloži državljan, ki je dopolnil 18 let, in tudi državljan, ki še ni star 18 let, pa je sklenil zakonsko zvezo ali je postal roditelj in mu je z odločbo sodišča priznana popolna poslovna sposobnost.

(4) Če vlogo za izdajo osebne izkaznice vloži zakoniti zastopnik, uradna oseba ugotovi tudi istovetnost zakonitega zastopnika. Ob vložitvi vloge mora biti navzoč tudi otrok oziroma državljan, ki ni poslovno sposoben, pa zanj ni upravičenih zdravstvenih razlogov, da ob vložitvi vloge pri pristojnem organu ne bi mogel biti navzoč.

4.2.2 Odobritev/zavrnitev zahtevka

(1) Kvalificirano potrdilo za elektronski podpis je odobreno z sprejemom vloge za izdajo osebne izkaznice.

(2) Ob oddaji vloge je bodoči imetnik potrdila izdajatelja SI-TRUST eID Podpis seznanjen z vso potrebno dokumentacijo v skladu z veljavno zakonodajo.

4.2.3 Čas za izdajo potrdila

Čas za izdajo potrdila je opredeljen v zakonodaji, ki ureja osebno izkaznico.

4.3. Izdaja potrdila

4.3.1 Postopek izdajatelja ob izdaji potrdila

(1) Potrdila se izdajajo izključno na infrastrukturi SI-TRUST.

(3) Na podlagi informacije o vložitvi vloge za izdajo osebne izkaznice izdajatelj SI-TRUST eID Podpis pridobi podatke iz evidence izdanih osebnih izkaznic ter pripravi podatke za izdajo kvalificiranega potrdila za elektronski podpis.

4.4. Prevzem potrdila

4.4.1 Postopek prevzema potrdila

(1) Potrdila se prevzemajo izključno na infrastrukturi izvajalca personalizacije.

(2) Čip osebne izkaznice je naprava za ustvarjanje kvalificiranega elektronskega podpisa.

(3) Potrdilo se na čip osebne izkaznice namesti v postopku personalizacije osebne izkaznice, tako da izvajalec personalizacije na strojnem varnostnem modulu generira par ključev in zahtevek za izdajo potrdila na varen način posreduje izdajatelju. Prejeto potrdilo skupaj z zasebnim ključem shrani na čip osebne izkaznice. Ob zaključku postopka onemogoči brisanje shranjenih zapisov (zasebnega ključa in potrdila) ter dodajanje novih zapisov s strani imetnika.

(4) Izdelano osebno izkaznico se bodočemu imetniku vroči skladno z določili zakonodaje, ki ureja osebno izkaznico.

(5) Začetno geslo za dostop do digitalnega potrdila imetnik prejme na enak način kot osebno izkaznico in sicer:
- osebno ob dvigu osebne izkaznice pri prijavni službi oz. izvajalcu personalizacije ali
- s poštno pošiljko na naslov bivališča.

(6) Podrobnosti postopka so določene z Interno politiko SI-TRUST.

(7) Imetnik mora takoj po prevzemu osebne izkaznice, na kateri je že prevzeto potrdilo, preveriti podatke v tem
potrdilu. Če izdajatelja SI-TRUST eID Podpis nemudoma ne obvesti o morebitnih napakah, se smatra, da se z vsebino strinja in da soglaša s pogoji delovanja ter prevzemom obveznosti in odgovornosti.

4.4.2 Objava potrdila

Ni predpisano.

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 oziroma bodoči imetnik potrdila je glede varovanja zasebnega ključa dolžan:
- podatke za uporabo potrdila skrbno varovati pred nepooblaščenimi osebami,
- hraniti zasebni ključ in potrdilo v skladu z obvestili in priporočili SI-TRUST eID Podpis,
- zasebni ključ in vse druge zaupne podatke ščititi s primernim uporabniškim geslom v skladu s priporočili SI-TRUST eID Podpis ali na drug način tako, da ima dostop do njih samo imetnik,
- po preteku veljavnosti oz. preklicu potrdila ravnati v skladu z obvestili SI-TRUST eID

Podpis.

(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

Ni podprto.

4.7.2 Kdo lahko zahteva obnovo potrdila

Ni podprto.

4.7.3 Postopek pri obnovi potrdila

Ni podprto.

4.7.4 Obvestilo imetniku o obnovi potrdila

Ni podprto.

4.7.5 Prevzem obnovljenega potrdila

Ni podprto.

4.7.6 Objava obnovljenega potrdila

Ni podprto.

4.7.7 Obvestilo o izdaji drugim subjektom

Ni podprto.

4.8. Sprememba potrdila

(1) Če pride do spremembe podatkov, ki vplivajo na veljavnost razločevalnega imena oz. drugih podatkov v potrdilu, je potrebno skladno s postopki za ravnanje z osebno izkaznico osebno izkaznico izročiti organu, pristojnemu za izdajo osebne izkaznice, v uničenje najpozneje v 30 dneh. Izdajatelj SI-TRUST eID Podpis v postopku uničenja osebne izkaznice izvede preklic kvalificiranega potrdila za elektronski podpis imetnika izročene osebne izkaznice.

(2) Za pridobitev novega potrdila je potrebno ponoviti postopek za pridobitev osebne izkaznice, kot je naveden v podpogl. 4.1. 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

4.9.1 Razlogi za preklic

(1) Preklic potrdila mora imetnik zahtevati v primeru:
- če je bil zasebni ključ imetnika potrdila ogrožen na način, ki vpliva na zanesljivost uporabe,
- če obstaja nevarnost zlorabe zasebnega ključa ali potrdila imetnika,
- če so se spremenili oz. so napačni ključni podatki, navedeni v potrdilu.

(2) Digitalno potrdilo izdajatelj SI-TRUST eID Podpis prekliče, če:
- izve, da je imetniku prenehala veljavnost osebne izkaznice v skladu z zakonom, ki ureja osebno izkaznico, razen v primeru odvzema osebne izkaznice,
- izve, da je imetnik vložil zahtevek za preklic digitalnega potrdila pri prijavni službi,
- izve, da imetnik v 48 urah po vložitvi zahtevka za začasno razveljavitev digitalnega potrdila zahtevka ni umaknil,
- pridobi informacijo, na podlagi katere mora v skladu z zakonom, ki ureja storitve zaupanja, preklicati digitalno potrdilo,
- izve, da je podatek v potrdilu napačen ali je bilo potrdilo izdano na podlagi napačnih podatkov,

- izve, da je prišlo do napake pri preverjanju istovetnosti podatkov na prijavni službi,
- izve, da so se spremenile druge okoliščine, ki vplivajo na veljavnost potrdila,
- izve, da je bila infrastruktura SI-TRUST ogrožena na način, ki vpliva na zanesljivost potrdila,
- izve, da je bil zasebni ključ imetnika potrdila ogrožen na način, ki vpliva na zanesljivost uporabe,
- izve, da bo SI-TRUST eID Podpis prenehal z izdajanjem potrdil ali da je bilo SI-TRUST prepovedano upravljanje s potrdili in njegove dejavnosti ni prevzel drug ponudnik storitev zaupanja,
- izve, da je preklic odredilo pristojno sodišče ali upravni organ.

4.9.2 Kdo lahko zahteva preklic

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.3 Postopek za preklic

(1) Izdajatelj SI-TRUST eID Podpis izvede preklic na zahtevo imetnika, če imetnik:
- izroči osebno izkaznico v uničenje organu, pristojnemu za izdajo osebne izkaznice,
- poda zahtevek za preklic digitalnega potrdila ali
- v 48 urah po vložitvi zahtevka za začasno razveljavitev digitalnega potrdila zahtevka ne umakne.

(2) Preklic lahko imetnik zahteva osebno v času uradnih ur na prijavni službi.

(3) Imetnik hkrati poda zahtevo za preklic digitalnega potrdila za sredstvo elektronske identifikacije visoke ravni zanesljivosti, digitalnega potrdila za sredstvo elektronske identifikacije nizke ravni zanesljivosti in kvalificiranega potrdila za elektronski podpis na osebni izkaznici. Imetnik ne more podati samo zahtevka za preklic kvalificiranega potrdila za elektronski podpis.

(4) O izvedbi postopka preklica je imetnik seznanjen ob oddaji zahtevka za preklic potrdila.

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

4.9.4 Čas za izdajo zahtevka za preklic

(1) Zahtevek za preklic je potrebno zahtevati nemudoma, če gre za možnost zlorabe ali nezanesljivosti ipd. nujne primere, sicer pa prvi delovni dan v času, ki velja za poslovni čas državnih organov oz. uradnih ur na prijavnih službah (glej naslednje podpoglavje).

(2) Če gre za možnost zlorabe ali nezanesljivosti ipd. nujne primere, lahko imetnik namesto zahtevka za preklic poda zahtevek za začasno razveljavitev (glej podpogl. 4.9.15).

4.9.5 Čas od prejetega zahtevka za preklic do izvedbe preklica

(1) SI-TRUST po prejemu veljavne zahteve za preklic najkasneje v dveh (2) urah prekliče potrdilo.

(2) Če je delovanje SI-TRUST zaradi nepredvidenih dogodkov bistveno okrnjeno, se preklic

izvede najkasneje v štiriindvajsetih (24) urah po prejemu veljavne zahteve za preklic v skladu s postopkom neprekinjenega poslovanja.

(3) Po preklicu je potrdilo takoj dodano v register preklicanih potrdil.

(4) Določila tega podpoglavja se smiselno uporabljajo tudi v primeru prejema zahteve za začasno razveljavitev.

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

(1) Začasno razveljavitev potrdila lahko imetnik zahteva v primeru:
- če je bil zasebni ključ imetnika potrdila ogrožen na način, ki vpliva na zanesljivost uporabe ali
- če obstaja nevarnost zlorabe zasebnega ključa ali potrdila imetnika,

2) Digitalno potrdilo izdajatelj SI-TRUST eID Podpis začasno razveljavi, če:

- izve, da je imetnik naznanil pogrešitev, izgubo ali krajo osebne izkaznice pri organu, pristojen za izdajo osebne izkaznice,
- izve, da je imetnik vložil zahtevek za začasno razveljavitev digitalnega potrdila pri prijavni službi, ali
- pridobi informacijo, da osebno izkaznico v skladu s predpisi, ki urejajo osebno izkaznico, hrani pristojni organ in ne imetnik, kar obravnava kot zahtevo za začasno razveljavitev digitalnega potrdila zaradi neposesti.

4.9.14 Kdo lahko zahteva začasno razveljavitev

Začasno razveljavitev lahko zahteva:
- imetnik ali
- upravni organ.

4.9.15 Postopek za začasno razveljavitev

(1) Izdajatelj SI-TRUST eID Podpis izvede začasno razveljavitev na zahtevo imetnika, če imetnik:
- naznani pogrešitev, izgubo ali krajo osebne izkaznice pri organu, pristojnem za izdajo osebne izkaznice ali
- poda zahtevek za začasno razveljavitev digitalnega potrdila.

(2) Imetnik zahtevek za začasno razveljavitev poda:
- osebno v času uradnih ur na prijavni službi,
- elektronsko štiriindvajset (24) ur na dan vse dni v letu, tako da se pri tem avtenticira s sredstvom elektronske identifikacije najmanj srednje ravni zanesljivosti.

(3) Če je delovanje SI-TRUST zaradi nepredvidenih dogodkov bistveno okrnjeno, lahko imetnik poda zahtevek za začasno razveljavitev zgolj osebno v času uradnih ur na prijavni službi.

(4) Imetnik hkrati poda zahtevo za začasno razveljavitev digitalnega potrdila za sredstvo elektronske identifikacije visoke ravni zanesljivosti, digitalnega potrdila za sredstvo elektronske identifikacije nizke ravni zanesljivosti in kvalificiranega potrdila za elektronski podpis na osebni izkaznici. Imetnik ne more podati samo zahtevka za začasno razveljavitev kvalificiranega potrdila za elektronski podpis.

(5) O izvedbi postopka začasne razveljavitve je imetnik seznanjen ob oddaji zahtevka za začasno razveljavitev potrdila.

(6) Imetnik lahko zahtevek za začasno razveljavitev umakne v času 48 ur od oddaje zahtevka, tako da:
- prekliče naznanitev pogrešitve, izgube ali kraje osebne izkaznice pri organu, pristojnem za izdajo osebne izkaznice ali
- poda zahtevek za umik začasne razveljavitve digitalnega potrdila.

(7) Imetnik zahtevek za umik začasne razveljavitve poda:
- osebno v času uradnih ur na prijavni službi,
- elektronsko štiriindvajset (24) ur na dan vse dni v letu, tako da se pri tem avtenticira s sredstvom elektronske identifikacije visoke ravni zanesljivosti, pri čemer ne more uporabiti sredstva elektronske identifikacije visoke ravni zanesljivosti na osebni izkaznici.

4.9.16 Čas začasne razveljavitve

(1) Čas začasne razvaljevitve je 48 ur. Če imetnik v 48 urah po vložitvi zahtevka za začasno razveljavitev digitalnega zahtevka ne umakne, izdajatelj SI-TRUST eID Podpis izvede preklic.

(2) Če izdajatelj SI-TRUST eID Podpis začasno razveljavitev izvede zaradi neposesti digitalnega potrdila, je začasna razveljavitev v veljavi do vrnitve osebne izkaznice v posest imetnika.

4.10. Preverjanje statusa potrdil

4.10.1 Dostop za preverjanje

Register preklicanih potrdil je objavljen na spletni strani http://si-trust-data.gov.si/crl/si-trust-eid-podpis.crl, sprotno preverjanje statusa potrdila je dostopno na naslovu http://si-trust-ocsp.gov.si/eid, 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 izdajateljem

Razmerje med imetnikom in SI-TRUST se prekine, če
- potrdilo preteče, imetnik pa ne zaprosi za novega,
- je potrdilo preklicano, imetnik pa ne zaprosi za novega.

4.12. Odkrivanje kopije ključev za dešifriranje

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 dnevnikov

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

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

(2) Zahtevke za pridobitev in preklic digitalnih potrdil, ki se nanašajo na pridobitev, naznanitev pogrešitve ali izročitev osebne izkaznice v uničenje, hranijo organi, pristojni za izdajo osebne izkaznice.

(3) Arhivirani podatki, ki se nanašajo na dokumente iz prejšnjega odstavka, se hranijo in arhivirajo v skladu s postopki dela z dokumentarnim gradivom na organih, pristojnih za izdajo osebne izkaznice.

5.5.4 Varnostno kopiranje arhiviranih podatkov

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

(2) Varnostno kopiranje arhiviranih podatkov, ki se nanašajo na dokumente iz drugega odstavka podpogl. 5.5.3, se hranijo in arhivirajo v skladu s postopki dela z dokumentarnim gradivom na organih, pristojnih za izdajo osebne izkaznice.

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

V primeru obnove potrdila izdajatelja SI-TRUST eID Podpis se postopek objavi na spletnih

straneh SI-TRUST.

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 izdajatelja SI-TRUST eID Podpis za podpisovanje in overjanje je formalen in kontroliran postopek ob namestitvi programske opreme SI-TRUST eID Podpis, o katerem se vodi poseben zapisnik (dokument »eID Sub CA key generation Script Template for Slovenian eID sub CAs«). 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 eID Podpis, ki so opravljene ob vzpostavitvi sistema, se dokumentirajo v posebnem zapisniku oz. v ustreznem dnevniku.

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

(5) Za generiranje parov ključev imetnikov se uporabi namenski strojni varnostni modul, s

katerim upravlja izvajalec personalizacije. V postopku personalizacije izvajalec personalizacije par ključev na varen način prenese iz strojnega varnostnega modula na čip osebne izkaznice.

6.1.2 Dostava zasebnega ključa imetnikom

Pri generiranju digitalnega potrdila ni prenosa zasebnega ključa do imetnika. Osebna izkaznica z digitalnim potrdilom in zasebnim ključem se vroči imetniku v skladu s predpisi, ki urejajo osebno izkaznico.

6.1.3 Dostava javnega ključa izdajatelju potrdil[5]

Izvajalec personalizacije pripravi zahtevek za izdajo potrdila po protokolu PKCS#10, ki vključuje javni ključ digitalnega potrdila, ter ga posreduje izdajatelju SI-TRUST eID Podpis.

6.1.4 Dostava izdajateljevega javnega ključa tretjim osebam

(1) Potrdilo z javnim ključem izdajatelja SI-TRUST eID Podpis je objavljeno v repozitoriju SI-TRUST (glej podpogl. 2.1).

(2) Potrdilo z javnim ključem izdajatelja SI-TRUST eID Podpis je imetniku dostavljeno oz. tretjim osebam dostopno:

- v obliki PEM na naslovu https://www.si-trust.gov.si/assets/si-trust-root/povezovalni-podrejeni/si-trust-eid podpis/si-trust-eid-podpis.xcert.pem,
- na čipu osebne izkaznice.

6.1.5 Dolžina ključev

Potrdilo	Dolžina ključa ECC [bit]
potrdilo izdajatelja SI-TRUST eID Podpis	384
potrdilo za imetnike	384
potrdilo za sistem OCSP	384

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

[5] RFC 3647 ne predvideva opisa načina dostave potrdil imetnikom.

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

Izdajatelj SI-TRUST eID Podpis zagotavlja varnostno kopijo svojega zasebnega ključa. Podrobnosti so določene v Interni politiki SI-TRUST.

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) Zasebni ključ imetnika se generira na namenskem strojnem varnostnem modulu, s katerim upravlja izvajalec personalizacije. V postopku personalizacije izvajalec personalizacije par ključev na varen način prenese iz strojnega varnostnega modula na čip osebne izkaznice.

6.2.7 Zapis zasebnega ključa v kriptografskem modulu

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

(2) Imetniki imajo dostop do svojega zasebnega ključa z geslom z ustreznimi aplikacijami.

6.2.8 Postopek za aktiviranje zasebnega ključa

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

(2) Aktiviranje zasebnega ključa imetnika se izvede pred vsako uporabo zasebnega ključa z namenom kreiranja
elektronskega podpisa. Pred aktiviranjem zasebnega ključa mora imetnik uporabiti uporabniško geslo, s katerim je zaščiten njegov zasebni ključ.

6.2.9 Postopek za deaktiviranje zasebnega ključa

Določbe so opredeljene v Krovni politiki SI-TRUST.

6.2.10 Postopek za uničenje zasebnega ključa

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

(2) Uničenje zasebnega ključa imetnika je izvedeno skladno s postopki za uničenje osebne izkaznice.

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) Veljavnost potrdil in ključev je podana po spodnji tabeli.

Tip potrdila	Par ključev	Ključi	Veljavnost
kvalificirano digitalno potrdilo za elektronski podpis	par za digitalno podpisovanje/overjanje	zasebni ključ	do konca veljavnosti osebne izkaznice oz. največ 10 let
		javni ključ	do konca veljavnosti osebne izkaznice oz. največ 10 let

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

6.4. Gesla za dostop do zasebnega ključa

6.4.1 Generiranje gesel

(1) Pooblaščene osebe izdajatelja za dostop do zasebnega ključa SI-TRUST eID Podpis uporabljajo močna gesla, s katerimi ravnajo v skladu z Interno politiko SI-TRUST.

(2) Imetniki za zaščito zasebnega ključa uporabljajo začetno geslo, uporabniško geslo in kodo za odklepanje uporabniškega gesla.

(4) Začetno geslo uporabi imetnik pred prvo uporabo sredstva elektronske identifikacije visoke ravni zanesljivosti ali kvalificiranega potrdila za elektronski podpis za določitev uporabniškega

gesla. Začetno geslo določi izvajalec personalizacije v postopku personalizacije osebne izkaznice.

(5) Uporabniško geslo uporabi imetnik pred vsako uporabo kvalificiranega potrdila za elektronski podpis. Uporabniško geslo določi imetnik pred prvo uporabo sredstva elektronske identifikacije visoke ravni zanesljivosti ali kvalificiranega potrdila za elektronski podpis, tako da uporabi začetno geslo. Uporabniško geslo je sestavljeno iz številk in je dolgo najmanj 6 in največ 12 znakov.

(6) Kodo za ponastavitev uporabniškega gesla uporabi imetnik v primeru, če ne pozna začetnega ali uporabniškega gesla ali je geslo neuporabno zaradi prevelikega števila neuspešnih poskusov vnosa. Kodo za ponastavitev uporabniškega gesla izračuna izdajatelj SI-TRUST eID Podpis v postopku personalizacije osebne izkaznice in v primeru, da imetnik poda zahtevek za pridobitev kode za ponastavitev uporabniškega gesla.

6.4.2 Zaščita gesel

(1) Gesla pooblaščenih oseb izdajatelja SI-TRUST eID Podpis za dostop do zasebnega ključa izdajatelja SI-TRUST eID Podpis se shranijo v skladu z Interno politiko SI-TRUST.

(2) Začetno geslo izvajalec personalizacije uporabi le v postopku personalizacije osebne izkaznice in ga ne hrani. Začetno geslo je mogoče uporabiti le enkrat in zgolj za nastavitev uporabniškega gesla. Začetno geslo imetnik prejme v ovojnici v skladu s postopkom za vročitev osebne izkaznice.

(3) SI-TRUST eID Podpis priporoča, da se uporabniško geslo ne shranjuje oz. se shrani na varno mesto in da ima do njega dostop le imetnik. SI-TRUST eID Podpis imetnikom priporoča, da sami poskrbijo za zamenjavo uporabniškega gesla vsaj vsakih šest (6) mesecev.

(4) Kodo za ponastavitev uporabniškega gesla izdajatelj SI-TRUST eID Podpis izračuna iz podatkov uporabnika v postopku personalizacije osebne izkaznice in v primeru, da imetnik poda zahtevek za pridobitev kode za ponastavitev uporabniškega gesla. Izdajatelj SI-TRUST eID Podpis kode za ponastavitev uporabniškega gesla in podatkov za njen izračun ne hrani.

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) Omogočeni so le mrežni protokoli, ki so nujno potrebni za delovanje sistema.

(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

(1) Na podlagi pričujoče politike SI-TRUST eID Podpis izdaja digitalna potrdila za elektronski podpis na osebni izkaznici.

(2) Vsa kvalificirana potrdila vključujejo podatke, ki so skladno z veljavno zakonodajo določeni za kvalificirana potrdila.

(3) Potrdila izdajatelja SI-TRUST eID Podpis sledijo standardu *X.509.*

7.1.1 Različica potrdil

Vsa potrdila izdajatelja SI-TRUST eID Podpis 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 eID Podpis

Profil potrdila SI-TRUST eID Podpis je predstavljen v podpogl. 1.3.1.

7.1.2.2 Profil potrdil za imetnike

(1) Podatki v potrdilu so navedeni spodaj.

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Number*	*enolična interna številka potrdila-celo število*
Algoritem za podpis, angl. *Signature algorithm*	sha384WithECDSA (1.2.840.10045.4.3.3)
Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST eID Podpis
Veljavnost, angl. *Validity*	Not Before: <*pričetek veljavnosti po GMT*> Not After: <*konec veljavnosti po GMT*> *v formatu UTCTime* <LLMMDDuummssZ>
Imetnik, angl. *Subject*	*razločevalno ime imetnika, ki vključuje ime imetnika in serijsko številko (glej podpogl. 3.1.1), v obliki, primerni za izpis*
Algoritem za javni ključ, angl. *Subject Public Key Algorithm*	P-384/secp384r1 (OID 1.3.132.0.34)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, angl. *ECC Public Key*	*dolžina ključa je 384 bitov, glej podpogl. 6.1.5*
Razširitve X.509v3	
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. *CRL Distribution Points*	Url: http://si-trust-data.gov.si/crl/si-trust-eid-podpis.crl
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://si-trust-ocsp.gov.si/eid Access Method: CaIssuer (OID 1.3.6.1.5.5.7.48.2) Access Location: URL=http://si-trust-data.gov.si/crt/si-trust-eid-podpis.cer
Uporaba ključa, OID 2.5.29.15, *angl. Key Usage*	ContentCommitment
Razširjena uporaba ključa, OID 2.5.29.37, angl. *Extended Key Usage*	*se ne uporablja*
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. Auth*ority Key Identifier*	F5C2 0034 9406 C208 AC6B 7D6D 1DAA 35A8

Identifikator imetnikovega ključa, OID 2.5.*29.14*, *angl. Subject Key Identifier*	*identifikator imetnikovega ključa*
Politike, pod katerimi je bilo izdano potrdilo, OID 2.5.29.32, angl. *certificatePolicies*	Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6105.9.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.si-trust.gov.si/cps/ PolicyIdentifier=0.4.0.194112.1.2
Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. *qcStatement*	QcCompliance statement QcSSCD statement QcType: esign PdsLocation: https://www.si-trust.gov.si/cps/, https://www.si-trust.gov.si/cps-en/
Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	CA: FALSE Brez omejitev dolžine (Path Length Constraint: none)
Storitev za pridobitev EŠEI fizične osebe, OID 1.3.6.1.4.1.58536.1.1.1.2.1	https://ws.si-trust.gov.si/esei-get?sn=<serijska številka potrdila>&ca=eid-ca-sign
Storitev za preverjanje EŠEI fizične osebe, OID 1.3.6.1.4.1.58536.1.1.1.3.1	https://ws.si-trust.gov.si/esei-validate?sn=<serijska številka potrdila>&ca=eid-ca-sign&esei=0000000000
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*

(2) Polje *uporaba ključa* (angl. *Key Usage*) je označeno kot kritično (angl. *critical*).

(3) Imetnik ima lahko eno samo veljavno istovrstno potrdilo.

7.1.3 Identifikacijske oznake algoritmov

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

(2) Potrdila, ki jih izdaja izdajatelj SI-TRUST eID Podpis, so s strani izdajatelja podpisana z algoritmom, določenim v polju *signature algorithm*: vrednost »sha384WithECDSA«, identifikacijska oznaka: OID 1.2.840.10045.4.3.3.

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 SI-TRUST eID Podpis*
Razločevalno ime izdajatelja, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST eID Podpis
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*	sha384WithECDSA (OID 1.2.840.10045.4.3.3)

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)*	*se ne uporablja*
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. 2.1).

(5) Izdajatelj objavlja register preklicanih potrdil na spletni strani SI-TRUST. Dostopen je po protokolu HTTP na naslovu http://si-trust-data.gov.si/crl/si-trust-eid-podpis.crl.

7.3. Profil sprotnega preverjanja statusa potrdil

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

(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

Stroški upravljanja s potrdili so zajeti v ceno osebne izkaznice.

9.1.2 Cena dostopa do potrdil

Ni podprto.

9.1.3 Cena dostopa do statusa potrdila in registra preklicanih potrdil

Dostop do statusa potrdila in registra preklicanih potrdil izdajtelja SI-TRUST eID Podpis je brezplačen.

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

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

(2) SI-TRUST posreduje podatke, ki so potrebni za zapis digitalnega potrdila na osebno izkaznico, izvajalcu personalizacije.

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

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

(2) Izvajalec personalizacije je za osebne podatke, ki so potrebni za zapis digitalnega potrdila na osebno izkaznico, odgovoren v skladu z veljavno zakonodajo glede varovanja osebnih podatkov.

9.4.5 Pooblastilo glede uporabe osebnih podatkov

Imetnik pooblasti SI-TRUST oz. izdajatelja SI-TRUST eID Podpis za uporabo osebnih podatkov na zahtevku za pridobitev potrdila ali kasneje v pisni obliki.

9.4.6 Posredovanje osebnih podatkov na uradno zahtevo

(1) SI-TRUST ne posreduje podatkov o imetnikih potrdil, ki niso navedeni v potrdilu, razen če se določeni podatki posebej zahtevajo za izvajanje specifičnih storitev oz. aplikacij, povezanih s potrdili, ter je SI-TRUST imetnik pooblastil za to (glej prejšnje podpoglavje), ali na zahtevo pristojnega sodišča ali upravnega organa.

(2) Podatki se posredujejo tudi brez pisne privolitve, če to določa zakonodaja oz. veljavni predpisi.

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 Obveznost in odgovornost prijavne službe

(1) Prijavna služba je dolžna:
- preverjati istovetnost imetnikov oz. bodočih imetnikov,
- sprejemati zahtevke za storitve SI-TRUST eID Podpis,
- preverjati zahtevke,
- izdajati potrebno dokumentacijo imetnikom oz. bodočim imetnikom,
- posredovati zahtevke in vloge ter ostale podatke na varen način na SI-TRUST eID Podpis.

(2) Prijavna služba je odgovorna za izvajanje vseh določil iz teh politik in drugih zahtev, ki jih dogovorita s SI-TRUST.

9.6.3 Obveznosti in odgovornost imetnika

(1) Imetnik oziroma bodoči imetnik potrdila je dolžan:
- seznaniti se s to politiko pred izdajo potrdila,
- ravnati v skladu s politiko in ostalimi veljavnimi predpisi,
- če po oddaji vloge za osebno izkaznico od izvajalca personalizacije ali pristojnega organa, glede na izbiro načina vročitve osebne izkaznice, imetnik ne prejme osebne izkaznice, se mora imetnik obrniti na pristojni organ, kamor je oddal vlogo za osebno izkaznico,
- če po oddaji vloge za osebno izkaznico od izvajalca personalizacije ali pristojnega organa, glede na izbiro načina vročitve osebne izkaznice, imetnik ne prejme ovojnice z začetnim geslom, mora imetnik na pristojnem organu oddati vlogo za pridobitev kode za ponastavitev uporabniškega gesla,
- po prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti izdajatelja SI-TRUST eID Podpis oziroma zahtevati preklic potrdila,
- spremljati vsa obvestila izdajatelja SI-TRUST eID Podpis in ravnati v skladu z njimi,
- v skladu z obvestili ustrezno posodabljati potrebno strojno in programsko opremo za varno delo s potrdili,
- vse spremembe, ki so povezane s potrdilom, nemudoma sporočiti izdajatelju SI-TRUST eID Podpis,
- zahtevati preklic potrdila, če so bili zasebni ključi ogroženi na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe,
- uporabljati potrdilo za namen, določen v potrdilu (glej podpogl. 7.1), in na način, ki je določen s politiko SI-TRUST eID Podpis,
- skrbeti za originalno podpisane dokumente in arhiv teh dokumentov.

(2) 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 imetnikovega potrdila s strani nepooblaščenih oseb,
- vsako drugo škodo, ki izvira iz neupoštevanja določil te politike in drugih obvestil izdajatelja SI-TRUST eID Podpis ter veljavnih predpisov.

(3) Obveznosti imetnika glede uporabe potrdil so določene v podpogl. 4.5.1.

9.6.4 Obveznosti in odgovornost 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

Izdajatelj SI-TRUST eID Podpis oz. SI-TRUST jamči za vrednost posameznega pravnega posla do vrednosti 5.000 EUR.

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.