Državni center za storitve zaupanja

Izdajatelj kvalificiranih digitalnih potrdil za storitev za spletno prijavo in e-podpis SI-PASS-CA

SI-TRUST SI-PASS-CA

POLITIKA SI-PASS-CA

za kvalificirana digitalna potrdila storitve za spletno prijavo in e-podpis

Javni del notranjih pravil Državnega centra za storitve zaupanja

veljavnost: od 20. maja 2026
verzija: 3.0

CP_{Name}: SI-PASS-CA

- **Politika za kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis**
  CP_{OID}: 1.3.6.1.4.1.6105.7.1.2
- **Politika za kvalificirana digitalna potrdila za fizične osebe**
  CP_{OID}: 1.3.6.1.4.1.6105.7.2.2
- **Politika za normalizirana digitalna potrdila za fizične osebe**
  CP_{OID}: 1.3.6.1.4.1.6105.7.3.2

Zgodovina politik

Izdaje politik delovanja SI-PASS-CA	
verzija: 3.0, veljavnost: od 20. maja 2026	
• Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis, CP_{OID}: 1.3.6.1.4.1.6105.7.1.2 • Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.2.2 • Politika SI-PASS-CA za normalizirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.3.2 CP_{Name}: SI-PASS-CA	*Spremembe z verzijo 3.0:* • *dokument je dopolnjen z elementi politike kvalificirane storitve zaupanja za upravljanje oddaljenih naprav za ustvarjanje kvalificiranega elektronskega podpisa.*
verzija: 2.7, veljavnost: od 31. decembra 2025	
• Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis, CP_{OID}: 1.3.6.1.4.1.6105.7.1.2 • Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.2.2 • Politika SI-PASS-CA za normalizirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.3.2 CP_{Name}: SI-PASS-CA	*Spremembe z verzijo 2.7:* • *spremenjena je najmanjša dovoljena dolžina ključa v potrdilu uporabnika,* • *v kvalificiranem potrdilu uporabnika sta vključeni razširitvi za pridobivanje in preverjanje EŠEI posameznika,* • *CRL je dostopen le še prek protokola HTTP,* • *spremenjeni so naslovi URL v razširitvah CP, CDP, AIA in QcStatement,* • *revizija dokumenta.*
verzija: 2.6, veljavnost: od 14. marca 2025	
• Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis, CP_{OID}: 1.3.6.1.4.1.6105.7.1.1 • Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.2.1 • Politika SI-PASS-CA za normalizirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.3.1 CP_{Name}: SI-PASS-CA	*Revizija dokumenta*
verzija: 2.5, veljavnost: od 12. decembra 2023	
• Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis, CP_{OID}: 1.3.6.1.4.1.6105.7.1.1 • Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.2.1 • Politika SI-PASS-CA za normalizirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.3.1 CP_{Name}: SI-PASS-CA	*Spremembe z verzijo 2.5:* • *spremenjeni so kontaktni podatki SI-TRUST,* • *enkratno geslo smsPASS se nadomesti s sredstvom elektronske identifikacije ravni zanesljivosti »srednja« ali »visoka« v skladu z ZEISZ,* • *revizija dokumenta.*
verzija: 2.4, veljavnost: od 5. decembra 2022	
• Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis, CP_{OID}: 1.3.6.1.4.1.6105.7.1.1 • Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.2.1 • Politika SI-PASS-CA za normalizirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.3.1 CP_{Name}: SI-PASS-CA	*Revizija dokumenta*
verzija: 2.3, veljavnost: od 24. decembra 2021	
• Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis, CP_{OID}: 1.3.6.1.4.1.6105.7.1.1 • Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.2.1 • Politika SI-PASS-CA za normalizirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.3.1 CP_{Name}: SI-PASS-CA	*Revizija dokumenta*

verzija: 2.2, veljavnost: od 20. oktobra 2020	
• Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis, CP_{OID}: 1.3.6.1.4.1.6105.7.1.1 • Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.2.1 • Politika SI-PASS-CA za normalizirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.3.1 CP_{Name}: SI-PASS-CA	*Revizija dokumenta*
verzija: 2.1, veljavnost: od 1. oktobra 2019	
• Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis, CP_{OID}: 1.3.6.1.4.1.6105.7.1.1 • Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.2.1 • Politika SI-PASS-CA za normalizirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.3.1 CP_{Name}: SI-PASS-CA	*Revizija dokumenta*
verzija: 2.0, veljavnost: od 28. maja 2018	
• Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis, CP_{OID}: 1.3.6.1.4.1.6105.7.1.1 • Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.2.1 • Politika SI-PASS-CA za normalizirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.3.1 CP_{Name}: SI-PASS-CA	*Spremembe z verzijo 2.0:* • *izvedene so redakcijske spremembe politike,* • *ukinjen je poseben način pridobitve enkratnega gesla smsPASS na osnovi prijave v storitev SI-PASS s kvalificiranim digitalnim potrdilom na varnem sredstvu za elektronsko podpisovanje, izdanim v Sloveniji,* • *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 28. junija 2016	
• Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis, CP_{OID}: 1.3.6.1.4.1.6105.7.1.1 • Politika SI-PASS-CA za kvalificirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.2.1 • Politika SI-PASS-CA za normalizirana digitalna potrdila za fizične osebe, CPOID: 1.3.6.1.4.1.6105.7.3.1 CP_{Name}: SI-PASS-CA	/

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 veljavno zakonodajo s področja storitev zaupanja, standardi ETSI ter drugimi veljavnimi predpisi in priporočili.

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

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

Kvalificirana digitalna potrdila, ki jih izdaja SI-TRUST, so namenjena:
- ustvarjanju elektronskih podpisov in elektronskih žigov 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-PASS-CA (angl. *Slovenian Authentication and e-Signature Service Certification Authority*), https://www.si-trust.gov.si/sl/si-pass/, ki izdaja potrdila za fizične osebe za potrebe storitve za spletno prijavo in e-podpis SI-PASS.

Izdajatelj SI-PASS-CA 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-PASS-CA 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-PASS-CA za kvalificirana digitalna potrdila, ki se izdajajo za potrebe storitve za spletno prijavo in e-podpis SI-PASS, ter politiko kvalificirane storitve zaupanja SI-PASS za upravljanje oddaljenih naprav za ustvarjanje kvalificiranega elektronskega podpisa (v nadaljevanju: storitev SI-PASS za oddaljeni e-podpis). Storitev SI-PASS za oddaljeni e-podpis zagotavlja storitev za strežniško podpisovanje in upravlja življenjski cikel podpisnih ključev v imenu podpisnikov. Zagotavlja, da se podpisni ključi tvorijo, aktivirajo in uporabljajo izključno znotraj naprave za ustvarjanje kvalificiranega elektronskega podpisa pod izključnim nadzorom podpisnika. Na podlagi tega dokumenta SI-PASS-CA izdaja digitalna potrdila, ki izpolnjujejo

najvišje varnostne zahteve, po naslednjih politikah: CP_{OID}: 1.3.6.1.4.1.6105.7.1.1, CP_{OID}: 1.3.6.1.4.1.6105.7.2.1 in CP_{OID}: 1.3.6.1.4.1.6105.7.3.1.

Pričujoči dokument nadomešča prejšnjo objavljeno politiko SI-PASS-CA za kvalificirana digitalna potrdila, ki se izdajajo za potrebe storitve za spletno prijavo in e-podpis SI-PASS. 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).

Spremembe pričujočega dokumenta so sledeče:
- dokument je dopolnjen z elementi politike kvalificirane storitve zaupanja za upravljanje oddaljenih naprav za ustvarjanje kvalificiranega elektronskega podpisa.,

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

Po pričujoči politiki SI-PASS-CA izdaja naslednja digitalna potrdila:
- kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis,
- kvalificirana digitalna potrdila za fizične osebe in
- normalizirana digitalna potrdila za fizične osebe.

Digitalna potrdila se pridobijo na podlagi zahtevka, ki ga bodoči imetnik odda elektronsko na uporabniških straneh SI-PASS na podlagi prijave v storitev SI-PASS.

Za pridobitev kvalificiranega digitalnega potrdila za fizične osebe za kvalificiran elektronski podpis se lahko bodoči imetnik potrdila v storitev SI-PASS prijavi na enega izmed naslednjih načinov:
- s sredstvom elektronske identifikacije ravni zanesljivosti »srednja« ali »visoka« v skladu z ZEISZ,
- s kvalificiranim digitalnim potrdilom za kvalificiran elektronski podpis,
- s sredstvom elektronske identifikacije ravni zanesljivosti »visoka« v skladu z eIDAS.

Za pridobitev kvalificiranega digitalnega potrdila za fizične osebe se lahko bodoči imetnik potrdila v storitev SI-PASS prijavi na enega izmed naslednjih načinov:
- s kvalificiranim digitalnim potrdilom,
- s sredstvom elektronske identifikacije ravni zanesljivosti »srednja« v skladu z eIDAS.

Za pridobitev normaliziranega digitalnega potrdila za fizične osebe se lahko bodoči imetnik potrdila v storitev SI-PASS prijavi na enega izmed ostalih načinov prijave, podprtih v storitvi SI-PASS, ki omogočajo pridobitev podatka o imenu in priimku bodočega imetnika.

V primeru odobrenega zahtevka SI-PASS-CA bodočemu imetniku potrdila le-to izda takoj po odobritvi zahtevka.

Digitalno potrdilo imetnika je povezano z enim parom ključev, ki se tvori z namenskim strojnim varnostnim modulom, ki se uporablja kot naprava za ustvarjanje kvalificiranega elektronskega podpisa, s katero upravlja izdajatelj SI-PASS-CA. SI-PASS-CA imetnikov zasebni ključ v šifrirani obliki hrani v namenski zaščiteni podatkovni zbirki in do njega nima dostopa. Zasebni ključ se izven namenskega strojnega varnostnega modula nahaja zgolj v šifrirani obliki. Dostop do zasebnega ključa imetnika v nešifrirani obliki ima samo imetnik.

SI-PASS-CA 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 skrbeti, da ni ogrožen način prijave, ki ga uporablja v storitvi SI-PASS in skrbno varovati geslo za zaščito zasebnega ključa ter ravnati v skladu s politiko, obvestili izdajatelja SI-PASS-CA in veljavno zakonodajo.

1. UVOD

1.1. Pregled

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

(2) Znotraj SI-TRUST deluje izdajatelj kvalificiranih digitalnih potrdil SI-PASS-CA (angl. *Slovenian Authentication and e-Signature Service Certification Authority*), https://www.si-trust.gov.si/sl/si-pass/, ki izdaja potrdila za fizične osebe za potrebe storitve za spletno prijavo in e-podpis SI-PASS.

(3) Izdajatelj SI-PASS-CA 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-PASS-CA za potrebe storitve za spletno prijavo in e-podpis SI-PASS izdaja naslednja digitalna potrdila:
- kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis,
- kvalificirana digitalna potrdila za fizične osebe in
- normalizirana digitalna potrdila za fizične osebe.

.
(5) Digitalna potrdila SI-PASS-CA se lahko uporabljajo za:
- overjanje digitalno podpisanih podatkov v elektronski obliki,
- 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-PASS-CA za zaščito zasebnih ključev.

(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-PASS-CA, ki definirajo namen, delovanje in metodologijo upravljanja z digitalnimi potrdili, odgovornost SI-TRUST ter zahteve, ki jih morajo izpolnjevati imetniki digitalnih potrdil izdajatelja SI-PASS-CA, tretje osebe, ki se zanašajo na digitalna potrdila, in drugi subjekti, ki skladno s predpisi uporabljajo storitve izdajatelja SI-PASS-CA.

(8) Medsebojna razmerja med tretjimi osebami, ki se zanašajo na potrdila izdajatelja SI-PASS-CA, 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.

(10) Pričujoča politika SI-PASS-CA predstavlja tudi politiko kvalificirane storitve zaupanja SI-PASS za upravljanje oddaljenih naprav za ustvarjanje kvalificiranega elektronskega podpisa. Storitev SI-PASS za oddaljeni e-podpis zagotavlja storitev za strežniško podpisovanje v skladu s standardom ETSI TS 119 431-1, Priloga A (politika EUSPv2) in upravlja življenjski cikel podpisnih ključev v imenu podpisnikov. Zagotavlja, da se podpisni ključi tvorijo, aktivirajo in uporabljajo izključno znotraj naprave za ustvarjanje kvalificiranega elektronskega podpisa pod izključnim nadzorom podpisnika.

(11) SI-TRUST izvaja storitev SI-PASS za oddaljeni e-podpis v skladu z Uredbo (EU) št. 910/2014, Izvedbeno uredbo Komisije (EU) 2025/1567 ter standardi ETSI EN 319 421, ETSI EN 319 422 in ETSI EN 391 401.

(12) Storitev SI-PASS za oddaljeni e-podpis vključuje sledeče komponente, kot jih določa ETSI TS 119 431-1:
- storitev tvorjenja podpisnih ključev: tvori podpisne ključe znotraj naprave za ustvarjanje kvalificiranega elektronskega podpisa,

- storitev povezovanja potrdil: poveže potrdila, izdana s strani SI-PASS-CA, z ustreznimi podpisnimi ključi,
- storitev povezovanja sredstev elektronske identifikacije oz. identitete podpisnika: poveže avtentikacijo podpisnika (prek storitve SI-PASS za spletno prijavo) z ustreznimi podpisnimi ključi,
- storitev aktivacije podpisa: preveri podatke za ustvarjanje podpisa (Signature Activation Data, SAD) in aktivira podpisne ključe za ustvarjanje podpisa,
- storitev brisanja podpisnih ključev: uniči podpisne ključe, ko je to potrebno.

(13) Storitev SI-PASS za oddaljeni e-podpis podpira dva modela namestitve aplikacije za ustvarjanje podpisa (Signature Creation Application, SCA):
- zunanja aplikacija SCA: ponudnik lastne storitve upravlja lastno aplikacijo SCA. Na vmesnik SI-PASS pošlje pred-izračunano vrednost predstavitve podatkov za podpis (Data To Be Signed Representation, DTBS/R) in prejme surovo vrednost podpisa.
- aplikacija SCA SI-PASS: ponudnik lastne storitve pošlje dokument na vmesnik SI-PASS. Aplikacija SCA SI-PASS izračuna podatke DTBS/R, orkestrira podpisovanje prek aplikacije za strežniško podpisovanje (Server Signing Application, SSA) in vrne podpisan dokument.

(14) Aplikacija SCA je dodatna storitvena plast nad aplikacijo SSA. Ocena skladnosti storitve za strežniško podpisovanje (Server Signing Application Service, SSAS) je neodvisna od modela namestitve aplikacije SCA.

1.2. Identifikacijski podatki politike delovanja

(1) Pričujoči dokument je Politika SI-PASS-CA za kvalificirana digitalna potrdila storitve za spletno prijavo in e-podpis (v nadaljevanju *politika SI-PASS-CA*).

(2) Oznaka pričujoče politike je CP_{Name}: SI-PASS-CA, identifikacijske oznake politike SI-PASS-CA pa so različne glede na vrsto potrdila:
- CP_{OID}: 1.3.6.1.4.1.6105.7.1.2 za kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis,
- CP_{OID}: 1.3.6.1.4.1.6105.7.2.2 za kvalificirana digitalna potrdila za fizične osebe in
- CP_{OID}: 1.3.6.1.4.1.6105.7.3.2 za normalizirana digitalna potrdila za fizične osebe.

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

(4) Identifikacijska oznaka politike kvalificirane storitve zaupanja SI-PASS za upravljanje oddaljenih naprav za ustvarjanje kvalificiranega elektronskega podpisa je 0.4.0.19431.1.1.4.

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-PASS-CA.

(3) Kontaktni podatki izdajatelja SI-PASS-CA so:

Naslov:	SI-PASS-CA Državni center za storitve zaupanja Ministrstvo za digitalno preobrazbo Tržaška cesta 21

	1000 Ljubljana
E-pošta:	si-pass-ca@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-PASS-CA opravlja naslednje naloge:
- izdaja kvalificirana in normalizirana digitalna potrdila,
- 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-PASS-CA je ob začetku svojega produkcijskega delovanja generiral svoje lastno digitalno potrdilo, ki je namenjeno overjanju potrdil, ki jih je SI-PASS-CA izdal imetnikom.

Potrdilo SI-PASS-CA vsebuje naslednje podatke[1]:

Naziv polja	Vrednost potrdila izdajatelja SI-PASS-CA
Različica, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Number*	5AF3 C2BA 0000 0000 574E AE10
Algoritem za podpis, angl. *Signature Algorithm*	sha256WithRSAEncryption
Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-PASS-CA
Imetnik, angl. *Subject*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-PASS-CA
Pričetek veljavnosti, angl. *Validity: Not Before*	Jun 1 09:12:41 2016 GMT
Konec veljavnosti, angl. *Validity: Not After*	Jun 1 09:42:41 2036 GMT
Algoritem za javni ključ, angl. *Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. *RSA Public Key*	*ključ dolžine 3072 bitov*
Razširitve X.509v3	
Uporaba ključa, OID 2.5.29.15, *angl. Key Usage*	Kritično (Critical) Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)

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

Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. Auth*ority Key Identifier*	4832 CA46 4E33 CB0A
Identifikator imetnikovega ključa, OID 2.5.*29.14, angl. Subject Key Identifier*	4832 CA46 4E33 CB0A
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA-1*	271E 1C16 BC2C 72DE 1243 9F79 CD9B 3FAE FECA 2E78
Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA-256*	10D4 20E2 C8BF E438 D696 7038 16E1 58E4 79C8 D825 82AC 691B 29B9 ACD4 51B7 4986

(6) Korenski izdajatelj SI-TRUST Root je izdajatelju SI-PASS-CA izdal povezovalno potrdilo z naslednjimi podatki:

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Number*	9D0E 9E3A 0000 0000 571D D10C
Algoritem za podpis, angl. *Signature Algorithm*	sha256WithRSAEncryption
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-PASS-CA
Pričetek veljavnosti, angl. *Validity: Not Before*	Jun 10 10:24:15 2016 GMT
Konec veljavnosti, angl. *Validity: Not After*	May 30 22:00:00 2036 GMT
Algoritem za javni ključ, angl. *Subject Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. *RSA Public Key*	*ključ dolžine 3072 bitov*
Razširitve X.509v3	
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: http://www.ca.gov.si/cps/
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. Auth*ority Key Identifier*	4CA3 C368 5E08 0263
Identifikator imetnikovega ključa, OID 2.5.*29.14, angl. Subject Key Identifier*	4832 CA46 4E33 CB0A
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SH*A-1	4FAE 2C20 DED9 3559 4D57 D544 19D5 0D3A 496B B8D7
Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SH*A-256	B394 3BD0 C0FF B4B4 1CD9 E1AD E986 ABE3 3583 12D6 AA6C 5DD2 45BB 7B0D 63A5 F851

1.3.2 Prijavna služba

(1) Organizacije, ki opravljajo naloge prijavne službe, pooblasti SI-TRUST. Izpolnjevati morajo pogoje za opravljanje nalog prijavnih služb SI-TRUST ter delovati v skladu z veljavnimi predpisi in poslovniki za delo prijavnih služb SI-TRUST.

(2) Naloge prijavne službe so:
- preverjanje istovetnosti imetnikov oz. bodočih imetnikov, njihovih podatkov in drugih potrebnih podatkov,
- sprejemanje zahtevkov za pridobitev potrdil,
- preverjanje podatkov v zahtevkih,
- izdajanje potrebne dokumentacije imetnikom oz. bodočim imetnikom,
- posredovanje zahtevkov in ostalih podatkov na varen način na SI-PASS-CA.

(3) Izdajatelj SI-PASS-CA ima vzpostavljene prijavne službe na različnih lokacijah, podatki o tem pa so objavljeni na spletnih straneh SI-PASS-CA.

1.3.3 Imetniki potrdil

Imetniki potrdil po tej politiki so vedno fizične osebe (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) Potrdila SI-PASS-CA izdana po pričujoči politiki se lahko uporabljajo za:
- overjanje digitalno podpisanih podatkov v elektronski obliki,
- storitve oz. aplikacije, za katere se zahteva uporaba kvalificiranih digitalnih potrdil SI-TRUST.

(2) Digitalno potrdilo imetnika je povezano z enim parom ključev, ki se tvori z namenskim strojnim varnostnim modulom, ki se uporablja kot naprava za ustvarjanje kvalificiranega elektronskega podpisa, s katero upravlja izdajatelj SI-PASS-CA.

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

(4) Izdajatelj SI-PASS-CA izdaja tudi potrdila za sistem OCSP za preverjanje veljavnosti potrdil, ki jih je izdal SI-PASS-CA.

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-PASS-CA:
- 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-PASS-CA.

(2) Na spletnih straneh https://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-PASS-CA 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-PASS-CA, 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) SI-TRUST oz. izdajatelj SI-PASS-CA v skladu z Interno politiko SI-TRUST skrbi za pooblaščeno in varno upravljanje podatkov v repozitorijih.

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-PASS-CA[2] (glej podpogl. 3.1.5).

(5) Razločevalno ime se glede na vrsto identitete oz. potrdila tvori po naslednjih pravilih[3].

Vrsta potrdila	Naziv polja	Razločevalno ime[4]
potrdilo izdajatelja SI-PASS-CA	Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-PASS-CA
kvalificirano potrdilo za fizične osebe za kvalificiran elektronski podpis	Imetnik, angl. *Subject*	c=SI, st=Slovenija, ou=individuals, ou=QcQscd, cn=<ime in priimek>, gn=<ime>, surname=<priimek>, sn=<serijska številka>
kvalificirano potrdilo za fizične osebe	Imetnik, angl. *Subject*	c=SI, st=Slovenija, ou=individuals,

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

		ou=Qc, cn=<ime in priimek>, gn=<ime>, surname=<priimek>, sn=<serijska številka>
normalizirano potrdilo za fizične osebe	Imetnik, angl. *Subject*	c=SI, st=Slovenija, ou=individuals, ou=Nc, cn=<ime in priimek>, 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 oz. nazivu 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.

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 ga je izdal izdajatelj SI-PASS-CA	3	
2.- 8. mesto	enolično število imetnika	/	
9. - 10. mesto	oznaka za potrdilo storitve za spletno prijavo in e-podpis	potrdilo za kvalificiran elektronski podpis	31
		kvalificirano potrdilo	32
		normalizirano potrdilo	33
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, ki se uporablja kot naprava za ustvarjanje kvalificiranega elektronskega podpisa, s katero upravlja izdajatelj SI-PASS-CA, zato dokazovanje s strani bodočega imetnika ni potrebno. V okviru postopkov izdajatelja SI-PASS-CA 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 opravi bodisi prijavna služba SI-TRUST ali pa se ugotavlja na podlagi prijave v storitev SI-PASS z veljavnim kvalificiranim digitalnim potrdilom oz. drugim ustreznim sredstvom elektronske identifikacije.

(2) Izdajatelj SI-PASS-CA preveri osebne podatke o imetniku v ustreznih registrih ali veljavnih kvalificiranih potrdilih oz. drugih sredstvih elektronske identifikacije.

3.2.4 Nepreverjeni podatki pri začetnem preverjanju

Nepreverjenih podatkov v kvalificiranem potrdilu ni. Podatki v normaliziranem potrdilu niso preverjeni.

3.2.5 Preverjanje pooblastil

Ni predpisano.

3.2.6 Merila za medsebojno povezovanje

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

(2) Izdajatelj SI-PASS-CA 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 elektronsko na podlagi prijave v storitev SI-PASS, s čimer je izkazana tudi istovetnost prosilca.

(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 vedno fizične osebe, glej definicijo v podpogl. 1.3.3.

4.1.2 Postopek za pridobitev potrdila in odgovornosti

(1) Zahtevek za pridobitev potrdila bodoči imetnik odda elektronsko na uporabniških straneh SI-PASS na podlagi prijave v storitev SI-PASS.

(2) Za pridobitev kvalificiranega digitalnega potrdila za fizične osebe za kvalificiran elektronski podpis se lahko bodoči imetnik potrdila v storitev SI-PASS prijavi na enega izmed naslednjih načinov:
- s sredstvom elektronske identifikacije ravni zanesljivosti »srednja« ali »visoka« v skladu z ZEISZ,
- s kvalificiranim digitalnim potrdilom za kvalificiran elektronski podpis,
- s sredstvom elektronske identifikacije ravni zanesljivosti »visoka« v skladu z eIDAS.

(3) Za pridobitev kvalificiranega digitalnega potrdila za fizične osebe se lahko bodoči imetnik potrdila v storitev SI-PASS prijavi na enega izmed naslednjih načinov:
- s kvalificiranim digitalnim potrdilom,
- s sredstvom elektronske identifikacije ravni zanesljivosti »srednja« v skladu z eIDAS.

(4) Za pridobitev normaliziranega digitalnega potrdila za fizične osebe se lahko bodoči imetnik potrdila v storitev SI-PASS prijavi na enega izmed ostalih načinov prijave, podprtih v storitvi SI-PASS, ki omogočajo pridobitev podatka o imenu in priimku bodočega imetnika.

4.2. Postopek ob sprejemu zahtevka za pridobitev potrdila

4.2.1 Preverjanje istovetnosti in verodostojnosti bodočega imetnika

Bodoči imetnik potrdila svojo istovetnost izkaže na podlagi prijave v storitev SI-PASS z veljavnim kvalificiranim digitalnim potrdilom oz. drugim ustreznim sredstvom elektronske identifikacije.

4.2.2 Odobritev/zavrnitev zahtevka

(1) Pred oddajo zahtevka izdajatelj SI-PASS-CA seznani bodočega imetnika z vso potrebno dokumentacijo v skladu z veljavno zakonodajo.

(2) Zahtevek za pridobitev potrdila se odobri samodejno na osnovi uspešno izvedenega postopka za pridobitev potrdila (glej podpogl. 4.1.2).

4.2.3 Čas za izdajo potrdila

SI-PASS-CA na podlagi odobrenega zahtevka bodočemu imetniku digitalnega potrdila le-to izda takoj po odobritvi zahtevka.

4.3. Izdaja potrdila

4.3.1 Postopek izdajatelja ob izdaji potrdila

(1) V primeru odobrenega zahtevka SI-PASS-CA bodočemu imetniku potrdila le-to izda takoj po odobritvi zahtevka.

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

4.3.2 Obvestilo imetniku o izdaji potrdila

Imetnik potrdila je o izdaji digitalnega potrdila obveščen na uporabniških straneh SI-PASS.

4.4. Prevzem potrdila

4.4.1 Postopek prevzema potrdila

(1) V primeru odobrenega zahtevka SI-PASS-CA bodočemu imetniku potrdila le-to izda takoj po odobritvi zahtevka.

(2) Način in podrobna navodila za prevzem potrdil po tej politiki so opisana na uporabniških straneh SI-PASS.

(3) Imetnik mora takoj po prevzemu potrdila preveriti podatke v tem potrdilu. Če izdajatelja SI-PASS-CA ne obvesti o morebitnih napakah, se smatra, da se z vsebino strinja in da soglaša s pogoji delovanja in 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) Zasebni ključ imetnika in njegovo potrdilo sta varno shranjena na infrastrukturi izdajatelja SI-PASS-CA, kar zagotavlja, da je v času uporabe zasebnega ključa imetnika pripadajoče potrdilo veljavno.

(2) Pred uporabo potrdila se mora imetnik na ustrezen način prijaviti v storitev SI-PASS ter vnesti geslo, s katerim je zaščiten njegov zasebni ključ.

(3) Imetnik kvalificiranega digitalnega potrdila za fizične osebe za kvalificiran elektronski podpis se lahko v storitev SI-PASS prijavi na enega izmed naslednjih načinov:
- s sredstvom elektronske identifikacije ravni zanesljivosti »srednja« ali »visoka« v skladu z ZEISZ,
- s kvalificiranim digitalnim potrdilom za kvalificiran elektronski podpis,
- s sredstvom elektronske identifikacije ravni zanesljivosti »visoka« v skladu z eIDAS.

(4) Imetnik kvalificiranega digitalnega potrdila za fizične osebe se lahko v storitev SI-PASS prijavi na enega izmed naslednjih načinov:
- s kvalificiranim digitalnim potrdilom,
- s sredstvom elektronske identifikacije ravni zanesljivosti »srednja« v skladu z eIDAS.

(5) Imetnik normaliziranega digitalnega potrdila za fizične osebe se lahko v storitev SI-PASS prijavi na enega izmed ostalih načinov prijave, podprtih v storitvi SI-PASS, ki omogočajo pridobitev podatka o imenu in priimku bodočega imetnika.

(6) Imetnik oziroma bodoči imetnik potrdila je glede varovanja zasebnega ključa dolžan:
- skrbeti, da ni ogrožen način prijave, ki ga uporablja v storitvi SI-PASS,
- zasebni ključ ščititi s primernim geslom v skladu s priporočili SI-PASS-CA tako, da ima dostop do njega samo imetnik,
- skrbno varovati geslo za zaščito zasebnega ključa,
- po preteku veljavnosti oz. preklicu potrdila ravnati v skladu z obvestili SI-PASS-CA.

(7) Imetnik mora varovati zasebni ključ pred nepooblaščeno uporabo.

(8) 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 potrdilo preklicati.

(2) Za pridobitev novega potrdila je potrebno ponoviti postopek za pridobitev novega potrdila, 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[5]

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) Izdajatelj SI-PASS-CA 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 je prišlo do napake pri preverjanju istovetnosti podatkov na prijavni službi,
- da so se spremenile druge okoliščine, ki vplivajo na veljavnost potrdila,
- za neizpolnjevanje obveznosti imetnika,
- da niso poravnani morebitni 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-PASS-CA 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

Določbe so opredeljene v Krovni politiki SI-TRUST.

4.9.3 Postopek za preklic

(1) Preklic lahko imetnik zahteva elektronsko štiriindvajset (24) ur na dan vse dni v letu na uporabniških straneh SI-PASS na podlagi prijave v storitev SI-PASS.

(2) Če gre za možnost zlorabe ali nezanesljivosti potrdila, lahko imetnik za pomoč pri preklicu pokliče na dežurno telefonsko številko izdajatelja SI-PASS-CA štiriindvajset (24) ur na dan vse dni v letu.

(3) Če je delovanje SI-TRUST zaradi nepredvidenih dogodkov bistveno okrnjeno in prijava v storitev SI-PASS ni mogoča, imetnik preklica sicer ne more zahtevati, vendar v tem primeru tudi ni možnosti zlorabe njegovega potrdila.

[5] Po priporočilu RFC 3647 to podpoglavje vključuje tudi postopek za storitev suspenza, ki jo izdajatelj SI-PASS-CA ne omogoča.

(4) O datumu ter času preklica, izdajatelju zahtevka za preklic ter vzrokih za preklic je imetnik obveščen na uporabniških straneh SI-PASS.

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

4.9.4 Čas za izdajo zahtevka za preklic

Zahtevek za preklic je potrebno zahtevati nemudoma, če gre za možnost zlorabe ali nezanesljivosti ipd. nujne primere, sicer pa čim prej oz. pred prvo nadaljnjo uporabo potrdila.

4.9.5 Čas od prejetega zahtevka za preklic do izvedbe preklica

(1) SI-TRUST po prejemu veljavne zahteve za preklic potrdilo prekliče najkasneje v štirih (4) urah.

(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 prejemu veljavne zahteve za preklic v skladu s postopkom neprekinjenega poslovanja.

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

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/digitalna-potrdila-si-pass-ca/, sprotno preverjanje statusa potrdila je dostopno na naslovu http://si-trust-ocsp.gov.si/sipass, 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
- imetnikovo potrdilo preteče in ga le-ta ne podaljša,
- 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.

4.13. Inicializacija podpisnih ključev uporabnikov storitve SI-PASS za oddaljeni e-podpis

4.13.1 Tvorjenje podpisnih ključev

(1) Storitev SI-PASS za oddaljeni e-podpis podpira dolgotrajne ključe za večkratno uporabo, ki se lahko uporabijo za več podpisov v več sejah.

(2) Podpisni ključi se tvorijo znotraj namenskega strojnega varnostnega modula, ki deluje v certificirani konfiguraciji in se zato uporablja kot naprava za ustvarjanje kvalificiranega elektronskega podpisa. Namenski strojni varnostni modul izvede kriptografsko tvorjenje para ključev, pri čemer veljajo naslednje zahteve iz standarda ETSI EN 419 241-1:

- podpisni ključi se tvorijo in uporabljajo v okolju, zaščitenem pred posegi,
- kriptografski algoritmi in dolžine ključev so skladni z dogovorjenimi kriptografskimi mehanizmi ENISA,
- podpisni ključi so zaščiteni z infrastrukturnim ključem v strojnem varnostnem modulu,
- inicializacija naprave je izvedena skladno s smernicami iz certifikacijske dokumentacije namenskega strojnega varnostnega modula,
- parametri algoritma se nastavijo ob tvorjenju ključa,
- čas tvorjenja ključa se zabeleži v revizijski dnevnik.

(3) Strojni varnostni modul ne hrani trajno vseh podpisnih ključev uporabnikov. Po tvorjenju ključa strojni varnostni modul vrne objekt (BLOB) s šifriranim ključem. Zasebni ključ znotraj objekta je šifriran z infrastrukturnim ključem, shranjenim v strojnem varnostnem modulu. Objekt se shrani v podatkovni bazi ključev aplikacije SSA.

(4) Ob vsakem postopku podpisovanja aplikacija SSA pridobi objekt iz podatkovne baze in ga posreduje strojnemu varnostnemu modulu, ki ključ naloži in hrani za čas operacije. Po podpisu se ključ odstrani iz strojnega varnostnega modula.

(5) Uporabljeni model je skladen z zahtevo standarda ETSI EN 419 241-1, člen 5.13.3.1. Objekt ključa je zaščiten z infrastrukturnim ključem v strojnem varnostnem modulu in ga ni mogoče uporabiti zunaj naprave za ustvarjanje kvalificiranega elektronskega podpisa.

4.13.2 Povezovanje potrdil, ključev in sredstev

(1) Podpisni ključ se poveže s sredstvom .

(2) Storitev SI-PASS za oddaljeni e-podpis ščiti celovitost povezave med podpisnim ključem in sredstvom elektronske identifikacije oziroma identiteto uporabnika.

(3) Podatki za identifikacijo osebe, povezani s sredstvom elektronske identifikacije, so enaki podatkom, povezanim z imetnikom pripadajočega potrdila.

(4) Potrdila, ki jih izda SI-PASS-CA, se povežejo z ustreznimi podpisnimi ključi znotraj storitve za strežniško podpisovanje, pri čemer velja sledeče:
- potrdilo se poveže s podpisnim ključem,
- povezava potrdila se preveri,
- celovitost povezave med ključem in potrdilom je zaščitena.

4.14. Življenjski cikel podpisnih ključev

4.14.1 Aktivacija podpisa

Storitev aktivacije podpisa preveri podatke SAD in aktivira podpisni ključ za ustvarjanje vrednosti digitalnega podpisa, pri čemer velja sledeče:
- avtentikacija podpisnika je zahtevana pred aktivacijo podpisnega ključa,
- nadzor dostopa preprečuje nepooblaščeno uporabo podpisnih ključev,
- aktivacija podpisnega ključa sledi zahtevam za izključni nadzor,
- podpisni ključi se uporabljajo v napravi za ustvarjanje kvalificiranega elektronskega podpisa,
- naprava za ustvarjanje kvalificiranega elektronskega podpisa deluje v certificirani konfiguraciji.

4.14.2 Dodatni elementi ob aktivaciji in ustvarjanju podpisa

(1) Podpisni ključi se lahko uporabijo samo v primerih, za katere je podpisnik dal privolitev. Podpisnik poda privolite z vpisom svojega gesla za zaščito zasebnega ključa.

(2) Storitev SI-PASS za oddaljeni e-podpis pred uporabo podpisnega ključa preveri, da je pripadajoče digitalno potrdilo veljavno (ni preteklo, ni preklicano).

4.14.3 Brisanje podpisnih ključev

(1) Podpisni ključi se uničijo:
- ob preklicu pripadajočega potrdila,
- ob ponastavitvi imetnikovega gesla za zaščito zasebnega ključa.

(2) Brisanje ključa se izvede z odstranitvijo objekta ključa iz podatkovne baze aplikacija SSA. Po izvedenem brisanju ključa ni mogoče rekonstruirati.

4.14.4 Varnostno kopiranje in obnovitev podpisnih ključev

Za varnostno kopiranje ključev velja:
- število podvojenih naborov podatkov ne presega minimuma, potrebnega za zagotavljanje neprekinjenosti storitve,
- varnost varnostnih kopij je na enaki ravni kot varnost izvirnih naborov podatkov.

4.15. Modeli namestitve aplikacije SCA

(1) Aplikacija SCA je komponenta, ki upravlja dokument za podpis, izračuna podatke DTBS/R in vgradi vrednost podpisa v podpisan dokument. Aplikacija SCA deluje nad storitvijo za strežniško podpisovanje in ni del naprave za ustvarjanje kvalificiranega elektronskega podpisa.

(2) Storitev SI-PASS podpira dva modela namestitve aplikacije SCA:
- zunanja aplikacija SCA,
- aplikacija SCA SI-PASS.

(3) V modelu zunanje aplikacije SCA ponudnik lastne storitve upravlja lastno aplikacijo SCA, storitev SI-PASS za oddaljeni e-podpis pa zagotavlja samo storitev za strežniško podpisovanje (aplikacijo SSA in napravo za ustvarjanje kvalificiranega elektronskega podpisa). Ponudnik lastne storitve je odgovoren za oblikovanje elektronskega podpisa v ustrezni obliki (PAdES, XAdES, CAdES, JAdES) in za celovitost dokumenta. Potek elektronskega podpisovanja je naslednji:
- aplikacija SCA ponudnika lastne storitve izračuna podatke DTBS/R iz dokumenta za podpis,
- aplikacija SCA ponudnika lastne storitve pošlje podatke DTBS/R na vmesnik SI-PASS,
- aplikacija SCA ponudnika lastne storitve orkestrira avtentikacijo podpisnika (prek storitve SI-PASS za prijavo) in aktivacijo podpisa (prek naprave za ustvarjanje kvalificiranega elektronskega podpisa),
- aplikacija SSA vrne surovo vrednost digitalnega podpisa aplikaciji SCA ponudnika lastne storitve,
- aplikacija SCA ponudnika lastne storitve vrednost podpisa vgradi v podpisan dokument.

(4) V modelu aplikacije SCA SI-PASS storitev SI-PASS za oddaljeni e-podpis upravlja aplikacijo SCA. Storitev SI-PASS za oddaljeni e-podpis podpira elektronske podpise v oblikah PAdES, XAdES in CAdES. Potek elektronskega podpisovanja je naslednji:
- ponudnik lastne storitve pošlje dokument (PDF, XML ipd.) na vmesnik SI-PASS,
- aplikacija SCA SI-PASS izračuna podatke DTBS/R,
- aplikacija SCA SI-PASS prek aplikacije SSA orkestrira avtentikacijo (prek storitve SI-PASS za prijavo) in aktivacijo podpisa (prek naprave za ustvarjanje kvalificiranega elektronskega podpisa),
- aplikacija SCA vrednost podpisa vgradi v dokument,
- aplikacija SCA celoten podpisan dokument vrne ponudniku lastne storitve.

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

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

V primeru obnove potrdila izdajatelja SI-PASS-CA se postopek objavi na spletnih straneh SI-PASS-CA.

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-PASS-CA za podpisovanje in overjanje je formalen in kontroliran postopek ob namestitvi programske opreme SI-PASS-CA, o katerem se vodi poseben zapisnik (dokument »Zapisnik postopka generiranja ključev izdajatelja SI-PASS-CA«). 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-PASS-CA, ki so opravljene ob vzpostavitvi sistema, se dokumentirajo v posebnem zapisniku oz. v ustreznem dnevniku.

(4) Za generiranje para ključev izdajatelja SI-PASS-CA se uporabi strojni varnostni modul (glej podpogl. 6.2.1).

(5) Za generiranje parov ključev imetnikov se uporabi namenski strojni varnostni modul, ki se uporablja kot naprava za ustvarjanje kvalificiranega elektronskega podpisa, s katero upravlja izdajatelj SI-PASS-CA (glej podpogl. 6.2.1).

(6) Za generiranje infrastrukturnih kontrolnih ključev, ki se uporabljata za aktiviranje uporabniških zasebnih ključev na strojni opremi za varno shranjevanje zasebnih ključev imetnikov, se uporabi strojni varnostni modul (glej podpogl. 6.2.1). Postopek generiranja se izvede vsaka tri (3) leta oziroma po potrebi tudi prej in je podrobneje opisan v Interni politiki SI-TRUST.

6.1.2 Dostava zasebnega ključa imetnikom

Zasebni ključ se generira na namenskem strojnem varnostnem modulu, hrani pa v namenski zaščiteni podatkovni zbirki, s katero upravlja izdajatelj SI-PASS-CA, zato se imetniku ne dostavi.

6.1.3 Dostava javnega ključa izdajatelju potrdil[6]

Javni ključ se generira na namenskem strojnem varnostnem modulu, hrani pa v namenski zaščiteni podatkovni zbirki, zato dostava izdajatelju ni potrebna.

6.1.4 Dostava izdajateljevega javnega ključa tretjim osebam

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

(2) Potrdilo z javnim ključem izdajatelja SI-PASS-CA je imetniku dostavljeno oz. tretjim osebam dostopno:
- v javnem imeniku x500.gov.si po protokolu LDAP (glej podpogl. 2.3),
- v obliki PEM na naslovu https://www.si-trust.gov.si/assets/si-trust-root/povezovalni-podrejeni/si-pass-ca/si-pass-ca.xcert.pem.

6.1.5 Dolžina ključev

(1) Potrdila izdajatelja SI-PASS-CA uporabljajo kriptografski algoritem RSA z naslednjimi dolžinami ključev:

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

Potrdilo	Dolžina ključa po RSA [bit]
potrdilo izdajatelja SI-PASS-CA	3072
potrdilo za imetnike	3072[7]
potrdilo za sistem OCSP	3072

(2) Za zagotavljanje storitve SI-PASS za oddaljeni e-podpis se uporabljajo naslednji kriptografski algoritmi in dolžine ključev:

Namen	Algoritem	Dolžina ključa
Ustvarjanje digitalnega podpisa	RSA-SHA256, RSA-SHA384, RSA-SHA512, ECDSA	Po vrsti ključa
Infrastrukturni ključi	RSA	3072 ali 4096
HMAC (celovitost dnevnikov)	SHA-256, SHA-384, SHA-512	256, 384 ali 512 bitov
AES (izvoz zasebne konfiguracije)	AES	128, 192 ali 256 bitov

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

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

(2) Zasebni ključi imetnikov se generirajo in uporabljajo na strojni opremi za varno shranjevanje zasebnih ključev, ki izpolnjuje zahteve v skladu s standardom FIPS 140-2 Level 3 ter zahteve za napravo za ustvarjanje kvalificiranega elektronskega podpisa v skladu z veljavno zakonodajo. S tem v zvezi SI-TRUST zagotavlja tudi naslednje ukrepe:

- storitev SI-PASS za oddaljeni e-podpis izpolnjuje zahteve, določene v certifikacijskem poročilu naprave za ustvarjanje kvalificiranega elektronskega podpisa,
- naprava za ustvarjanje kvalificiranega elektronskega podpisa deluje v konfiguraciji, kot je opisana v certifikacijski dokumentaciji,
- različica programske opreme naprave za ustvarjanje kvalificiranega elektronskega podpisa se vzdržuje na certificirani različici.

(3) Infrastrukturna kontrolna ključa, ki se uporabljata za aktiviranje uporabniških zasebnih ključev na strojni opremi za varno shranjevanje zasebnih ključev imetnikov, se generirata, uporabljata in hranita na strojni opremi za varno shranjevanje zasebnih ključev, ki izpolnjuje zahteve v skladu s standardom FIPS 140-2 Level 3.

[7] Vrednost pomeni minimalno predpisano dolžino.

6.2.2 Nadzor zasebnega ključa s strani pooblaščenih oseb

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

(2) Dostop do zasebnega ključa imetnika v nešifrirani obliki ima samo imetnik.

6.2.3 Odkrivanje kopije zasebnega ključa

Ni podprto.

6.2.4 Varnostna kopija zasebnega ključa

(1) Izdajatelj SI-PASS-CA zagotavlja varnostno kopijo svojega zasebnega ključa. Podrobnosti so določene v Interni politiki SI-TRUST.

(2) Izdajatelj SI-PASS-CA zagotavlja varnostno kopijo zasebnih ključev imetnikov. 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.

(4) Zasebni ključ imetnika se generira na namenskem strojnem varnostnem modulu, ki se uporablja kot naprava za ustvarjanje kvalificiranega elektronskega podpisa, s katero upravlja izdajatelj SI-PASS-CA. Prenos zasebnega ključa imetnika iz strojnega varnostnega modula se izvede v šifrirani obliki po generiranju para ključev z namenom varne hrambe zasebnega ključa v namenski zaščiteni podatkovni zbirki ter izdelave njegove varnostne kopije (glej podpogl. 6.2.4). Prenos zasebnega ključa v strojni varnostni modul se izvede v šifrirani obliki pred vsako uporabo zasebnega ključa imetnika. Zasebni ključ se izven namenskega strojnega varnostnega modula nahaja zgolj v šifrirani obliki.

6.2.7 Zapis zasebnega ključa v kriptografskem modulu

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

(2) Zasebni ključ imetnika je v strojnem varnostnem modulu varovan z mehanizmi v skladu s standardom FIPS 140-2 Level 3 ter imetnikovim geslom za zaščito zasebnega ključa.

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 se mora imetnik na ustrezen način prijaviti v storitev

SI-PASS ter vnesti geslo, s katerim je zaščiten njegov zasebni ključ (glej podpogl. 4.5.1).

6.2.9 Postopek za deaktiviranje zasebnega ključa

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

(2) Po kreiranju elektronskega podpisa se zasebni ključ imetnika v namenskem strojnem varnostnem modulu trajno briše in na ta način deaktivira.

6.2.10 Postopek za uničenje zasebnega ključa

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

(2) Uničenje zasebnega ključa imetnika se izvede takoj po oddaji zahtevka za preklic potrdila tako, da se zasebni ključ v šifrirani obliki trajno briše iz namenske zaščitene podatkovne zbirke.

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
potrdilo imetnika	par za digitalno podpisovanje/overjanje	zasebni ključ	5 let
		javni ključ	5 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-PASS-CA uporabljajo močna gesla, s katerimi ravnajo v skladu z Interno politiko SI-TRUST.

(2) Imetniki sami določijo geslo, s katerim zaščitijo dostop do svojih zasebnih ključev, pri čemer uporabljajo močna gesla, kar se zagotavlja v okviru storitve SI-PASS.

(3) SI-PASS-CA za imetnike zahteva uporabo varnih gesel:
- mešano uporabo velikih in malih črk ter števil,
- dolžine vsaj 6 znakov,
- odsvetuje se uporaba besed, ki so zapisane v slovarjih.

6.4.2 Zaščita gesel

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

(2) SI-PASS-CA priporoča, da se geslo imetnika za dostop do zasebnega ključa ne shranjuje oz. se shrani na varno mesto in da ima do njega dostop le imetnik.

(3) SI-PASS-CA imetnikom priporoča, da sami poskrbijo za zamenjavo gesla vsaj vsakih šest (6) mesecev.

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-PASS-CA izdaja potrdila za fizične osebe za potrebe storitve za spletno prijavo in e-podpis SI-PASS.

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

(3) Potrdila izdajatelja SI-PASS-CA sledijo standardu *X.509.*

7.1.1 Različica potrdil

Vsa potrdila izdajatelja SI-PASS-CA 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-PASS-CA

Profil potrdila SI-PASS-CA 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*	sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11)
Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-PASS-CA

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*	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 3072 bitov, glej podpogl. 6.1.5*
Razširitve X.509v3	
Alternativno ime OID 2.5.29.17, angl. *Subject Alternative Name*	*se ne uporablja*
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. *CRL Distribution Points*	Url: http://si-trust-data.gov.si/crl/si-pass-ca.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/sipass Access Method: CaIssuer (OID 1.3.6.1.5.5.7.48.2) Access Location: URL=http://si-trust-data.gov.si/crt/si-pass-ca-certs.p7c
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. Author*ity Key Identifier*	4832 CA46 4E33 CB0A
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=*odvisno od vrste potrdila, glej podpogl. 7.1.2.3* [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.si-trust.gov.si/cps/
Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. *qcStatement*	*odvisno od vrste potrdila, glej podpogl. 7.1.2.3*
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=si-pass-ca
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=si-pass-ca&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.

7.1.2.3 Profili posameznih vrst potrdil

Vsa potrdila imetnikov vključujejo podatke, ki so navedeni v tabeli v podpogl. 7.1.2. Vrednosti polj za *politiko ter oznako kvalificiranega potrdila,* ki pa so odvisne od vrste potrdila, so za posamezno vrsto potrdila podane v spodnji tabeli.

Naziv polja	Vrsta potrdila		
	kvalificirano potrdilo za kvalificiran elektronski podpis	kvalificirano potrdilo	normalizirano potrdilo
Politike, pod katerimi je bilo izdano potrdilo (OID), in iz katerih je razvidno tudi, da gre za kvalificirano potrdilo, angl. *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.7.1.2 0.4.0.194112.1.2	Policy: 1.3.6.1.4.1.6105.7.2.2 0.4.0.194112.1.0	Policy: 1.3.6.1.4.1.6105.7.3.2
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-en/, https://www.si-trust.gov.si/cps/	QcCompliance statement QcType: esign PdsLocation: https://www.si-trust.gov.si/cps-en/, https://www.si-trust.gov.si/cps/	/

7.1.3 Identifikacijske oznake algoritmov

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

(2) Infrastrukturna kontrolna ključa, ki se uporabljata za aktiviranje uporabniških zasebnih ključev na strojni opremi za varno shranjevanje zasebnih ključev imetnikov, sta generirana z algoritmom AES256 oz. HASH-MAC-SHA256.

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-PASS-CA*
Razločevalno ime izdajatelja, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-PASS-CA
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 posamičnem registru, v celotnem registru pa so objavljena le do poteka veljavnosti.

(3) Polja v CRL niso označena kot kritična.

(4) Register preklicanih digitalnih potrdil je javno objavljen v repozitoriju (glej podpogl. 2.1).

7.3. Profil sprotnega preverjanja statusa potrdil

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

(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 se imetnikom ne obračunavajo.

9.1.2 Cena dostopa do potrdil

Potrdila imetnikov se ne objavljajo v javnem imeniku (glej pogl. 0).

9.1.3 Cena dostopa do statusa potrdila in registra preklicanih potrdil

Dostop do statusa potrdila in registra preklicanih potrdil izdajatelja SI-PASS-CA 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

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

Imetnik pooblasti SI-TRUST oz. izdajatelja SI-PASS-CA 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-PASS-CA,
- preverjati zahtevke,
- izdajati potrebno dokumentacijo imetnikom oz. bodočim imetnikom,
- posredovati zahtevke in ostale podatke na varen način na SI-PASS-CA.

(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,
- po prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti SI-PASS-CA oziroma zahtevati preklic potrdila,

- spremljati vsa obvestila SI-PASS-CA 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 SI-PASS-CA,
- 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-PASS-CA,
- 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 po krivdi imetnika omogočena uporaba oz. zloraba imetnikovega potrdila s strani nepooblaščenih oseb,
- vsako drugo škodo, ki izvira iz neupoštevanja določil te politike in drugih obvestil SI-PASS-CA 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-PASS-CA oz. SI-TRUST jamči za vrednost posameznega pravnega posla glede na vrsto potrdila do vrednosti:
- za kvalificirana potrdila za kvalificiran elektronski podpis do višine 5.000 EUR ter
- za kvalificirana potrdila do višine 1.000 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.