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

IZJAVA O POLITIKI SI-PASS-CA

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

Povzetek javnega dela 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

VSEBINA:

1. Podatki o ponudniku storitev zaupanja[1]

Kontaktni podatki Državnega centra za storitve zaupanja, ki deluje v okviru Ministrstva za digitalno preobrazbo (v nadaljevanju *SI-TRUST*):

Naslov:	Republika Slovenija Državni center za storitve zaupanja Ministrstvo za digitalno preobrazbo Tržaška cesta 21 1000 Ljubljana
Telefon:	01 4788 330
Spletna stran:	http://www.si-trust.gov.si
Oznaka:	State-institutions

Kontaktni podatki izdajatelja SI-PASS-CA:

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

2. Digitalna potrdila, njihova pridobitev in uporaba

2.1. Vrste potrdil[2]

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.

Po pričujoči politiki 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.

[1] Politika SI-PASS-CA, pogl. 1.3.1
[2] Politika SI-PASS-CA, pogl. 1.1, 1.2

Oznaka 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.

V vsakem potrdilu je navedba ustrezne politike v obliki oznake $CP_{OID.}$

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.

2.2. Pridobitev potrdil[3]

Bodoči imetniki potrdil so vedno fizične osebe.

Zahtevek za pridobitev potrdila 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.

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

Zahtevek za pridobitev potrdila se odobri samodejno na osnovi uspešno izvedenega postopka za pridobitev potrdila.

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

Potrdila se izdajajo izključno na infrastrukturi SI-TRUST.

2.3. Uporaba potrdil in ključev[4]

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.

[3] Politika SI-PASS-CA, pogl. 4.1, 4.2, 4.3
[4] Politika SI-PASS-CA, pogl. 4.5

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

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.

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.

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.

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.

Imetnik mora varovati zasebni ključ pred nepooblaščeno uporabo.

2.4. Uporaba storitve SI-PASS za oddaljeni e-podpis[5]

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.

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.

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.

[5] Politika SI-PASS-CA, pogl. 1.1

- 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.

3. Omejitve pri uporabi[6]

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.

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.

Dnevniki beleženih dogodkov v zvezi s ključi in digitalnimi potrdili se hranijo vsaj deset (10) let po poteku potrdila, na katerega se dnevniški zapis nanaša.

Ostali dnevniki beleženih dogodkov se hranijo vsaj deset (10) let po nastanku dogodka.

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

4. Dolžnosti in odgovornosti imetnika[7]

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.

Imetnik mora varovati zasebni ključ pred nepooblaščeno uporabo.

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, in na način, ki je določen s politiko SI-PASS-CA,
- skrbeti za originalno podpisane dokumente in arhiv teh dokumentov.

Imetnik odgovarja za:
- nastalo škodo v primeru zlorabe potrdila od prijave preklica do preklica,

[6] Politika SI-PASS-CA, pogl. 1.1, 4.5, 5.4.3
[7] Politika SI-PASS-CA, pogl. 4.5.1, 9.6.3

- 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.

5. Zahteve po preverjanju registra preklicanih potrdil za tretje osebe[8]

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

Zaradi verodostojnosti in celovitosti je vedno potrebno preveriti veljavnost in verodostojnost tega registra, ki je digitalno podpisan s strani SI-PASS-CA.

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

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

Register preklicanih potrdil se osvežuje:
- najkasneje dve (2) uri po preklicu potrdila,
- enkrat dnevno, če ni novih zapisov oz. sprememb v registru preklicanih potrdil, in sicer približno štiriindvajset (24) ur po zadnjem osveževanju.

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

6. Zanikanje in omejitev odgovornosti[9]

SI-TRUST ni odgovoren za škodo, ki bi nastala zaradi:
- uporabe potrdil za namen in na način, ki ni izrecno predviden v politiki izdajatelja SI-PASS-CA oz. morebitnem dogovoru med imetnikom oz. organizacijo in SI-TRUST,
- nepravilnega ali pomanjkljivega varovanja gesel ali zasebnih ključev imetnikov, izdajanja zaupnih podatkov ali ključev tretjim osebam in neodgovornega ravnanja imetnika,
- zlorabe oz. vdora v informacijski sistem imetnika potrdila in s tem do podatkov o potrdilih s strani nepooblaščenih oseb,
- nedelovanja ali slabega delovanja informacijske infrastrukture imetnika potrdila ali tretjih oseb,
- nepreverjanja podatkov in veljavnosti potrdil,
- nepreverjanja časa veljavnosti potrdila,
- ravnanja imetnika potrdila ali tretje osebe v nasprotju z obvestili izdajatelja SI-PASS-CA, politiko, morebitnim dogovorom oz. pogodbo in drugimi predpisi,
- omogočene uporabe oz. zlorabe imetnikovega potrdila nepooblaščenim osebam,
- izdanega potrdila z napačnimi podatki in neverodostojnimi podatki ali drugih dejanj imetnika ali organizacije,
- uporabe potrdil ter veljavnosti potrdil ob spremembah podatkov iz potrdila ali spremembah podatkov o imetniku ali organizaciji,
- izpada infrastrukture, ki ni v domeni upravljanja SI-TRUST,
- podatkov, ki se šifrirajo ali podpisujejo z uporabo pripadajočih potrdil oz. zasebnih ključev,

[8] Politika SI-PASS-CA, pogl. 4.9.6, 4.9.7, 4.9.9
[9] Politika SI-PASS-CA, pogl. 9.7, 9.8

- ravnanja imetnikov pri uporabi potrdil, in sicer tudi v primeru, če je imetnik ali tretja oseba spoštoval vsa določila te politike in dogovora ter obvestila izdajatelja SI-PASS-CA ali druge veljavne predpise,
- uporabe in zanesljivosti delovanja strojne in programske opreme imetnikov potrdil.

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.

7. Politika in veljavna zakonodaja[10]

Izhodiščni dokument je Politika SI-PASS-CA za kvalificirana digitalna potrdila za storitev za spletno prijavo in e-podpis.

Oznaka 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.

SI-TRUST in izdajatelj SI-PASS-CA delujeta v skladu z:
- Uredbo (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES,
- Uredbo (EU) št. 679/2016 Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 1995/46/ES,
- Zakonom o elektronski identifikaciji in storitvah zaupanja,
- Zakonom o osebni izkaznici,
- Zakonom o varstvu osebnih podatkov,
- Zakonom o tajnih podatkih,
- Zakonom o varstvu dokumentarnega in arhivskega gradiva ter arhivih,
- Uredbo o določitvi sredstev elektronske identifikacije in uporabi centralne storitve za spletno prijavo in elektronski podpis,
- priporočili ETSI s področja kvalificiranih potrdil in storitev zaupanja,
- priporočili RFC s področja potrdil X.509,
- zahtevami organizacije CA/Browser Forum (»Baseline Requirements« in »EV SSL Certificate Guidelines«),
- in drugimi veljavnimi predpisi in priporočili.

8. Varovanje osebnih podatkov in čas hrambe

8.1. Varovanje osebnih podatkov[11]

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

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

[10] Politika SI-PASS-CA, pogl. 1.2, 9.14
[11] Politika SI-PASS-CA, pogl. 9.4

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

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

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, ali na zahtevo pristojnega sodišča ali upravnega organa

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

8.2. Čas hrambe[12]

Arhivirani podatki v zvezi s ključi in digitalnimi potrdili se hranijo vsaj deset (10) let po poteku potrdila, na katerega se podatek nanaša.

Ostali arhivirani podatki se hranijo vsaj deset (10) let po njihovem nastanku.

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

9. Povrnitev stroškov[13]

Stroški upravljanja s potrdili se imetnikom ne obračunavajo.

10. Postopek v primeru sporov[14]

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

11. Skladnost z veljavno zakonodajo[15]

Nadzor nad skladnostjo delovanja SI-TRUST oz. izdajatelja SI-PASS-CA z veljavno zakonodajo in predpisi izvaja pristojna inšpekcijska služba.

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

Izvajanje inšpekcijskega nadzora SI-TRUST opravlja pristojna inšpekcijska služba v skladu z veljavno zakonodajo.

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

[12] Politika SI-PASS-CA, pogl. 5.5.2
[13] Politika SI-PASS-CA, pogl. 9.1
[14] Politika SI-PASS-CA, pogl. 9.13
[15] Politika SI-PASS-CA, pogl. 9.15, 8

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

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

Področja nadzora so določena z veljavno zakonodajo in predpisi.

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

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

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