IZJAVA O POLITIKI SI-PASS-CA

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

Povzetek javnega dela notranjih pravil Državnega centra za storitve zaupanja

veljavnost: od 28. junija 2016
verzija: 1.0

CP_{Name}: SI-PASS-CA

- **Politika za kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis**
  CP_{OID}: 1.3.6.1.4.1.6105.7.1.1
- **Politika za kvalificirana digitalna potrdila za fizične osebe**
  CP_{OID}: 1.3.6.1.4.1.6105.7.2.1
- **Politika za normalizirana digitalna potrdila za fizične osebe**
  CP_{OID}: 1.3.6.1.4.1.6105.7.3.1

1. Podatki o ponudniku storitev zaupanja[1]

Kontaktni podatki Državnega centra za storitve zaupanja oz. Overitelja na MJU:

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

Kontaktni podatki izdajatelja SI-PASS-CA:

Naslov:	SI-PASS-CA Državni center za storitve zaupanja Ministrstvo za javno upravo Tržaška cesta 21 1000 Ljubljana
E-pošta:	si-pass-ca@gov.si
Telefon:	01 4788 330
Spletna stran:	http://www.si-pass-ca.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.

Oznaka politike je CP_{Name}: SI-PASS-CA, identifikacijske oznake politike SI-PASS-CA pa so različne glede na vrsto potrdila:

- CP_{OID}: 1.3.6.1.4.1.6105.7.1.1 za kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis,
- CP_{OID}: 1.3.6.1.4.1.6105.7.2.1 za kvalificirana digitalna potrdila za fizične osebe in
- CP_{OID}: 1.3.6.1.4.1.6105.7.3.1 za normalizirana digitalna potrdila za fizične osebe.

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

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

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:
- z enkratnim geslom smsPASS,
- s kvalificiranim digitalnim potrdilom na varnem sredstvu za elektronsko podpisovanje,
- 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.

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 overitelja na MJU.

2.3. Uporaba potrdil in ključev[4]

Zasebni ključ imetnika in njegovo potrdilo sta varno shranjena na infrastrukturi izdajatelja SI-PASS-CA.

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:
- z enkratnim geslom smsPASS,
- s kvalificiranim digitalnim potrdilom na varnem sredstvu za elektronsko podpisovanje,
- 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.

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

3. Omejitve pri uporabi[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 overitelja na MJU.

Zasebni ključ imetnika in njegovo potrdilo sta varno shranjena na infrastrukturi izdajatelja SI-PASS-CA.

Dnevniki beleženih dogodkov v zvezi s ključi in digitalnimi potrdili se hranijo vsaj sedem (7) let po poteku potrdila, na katerega se dnevniški zapis nanaša.

Ostali dnevniki beleženih dogodkov se hranijo vsaj sedem (7) 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[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.

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,
- če po oddaji zahtevka za pridobitev enkratnega gesla smsPASS od izdajatelja SI-PASS-CA ne prejme obvestila po e-pošti oz. s poštno pošiljko na naslov stalnega bivališča, se mora obrniti na pooblaščene osebe izdajatelja SI-PASS-CA,
- 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. **Napaka! Vira sklicevanja ni bilo mogoče najti.**), 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,
- 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,

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

- 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[7]

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

Zaradi verodostojnosti in celovitosti je vedno potrebno preveriti tudi 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:
- po vsakem 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[8]

Overitelj na MJU ni odgovoren za škodo, ki bi nastala zaradi:
- nepravilnega ali pomanjkljivega varovanja gesel, izdajanja zaupnih podatkov tretjim osebam in neodgovornega ravnanja imetnika,
- zlorabe oz. vdora v informacijski sistem imetnika potrdila in s tem do podatkov za dostop do potrdila 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 in drugimi predpisi,
- omogočene uporabe oz. zlorabe imetnikovega potrdila nepooblaščenim osebam,
- izdanega potrdila z napačnimi podatki in neverodostojnimi podatki ali drugih dejanj imetnika,
- uporabe potrdil ter veljavnosti potrdil ob spremembah podatkov iz potrdila ali spremembah imen imetnikov,
- izpada infrastrukture, ki ni v domeni upravljanja overitelja na MJU,
- podatkov, ki se podpisujejo z uporabo potrdil,
- ravnanja imetnikov pri uporabi potrdil, in sicer tudi v primeru, če je imetnik ali tretja oseba spoštoval vsa določila te politike, obvestila izdajatelja SI-PASS-CA ali druge veljavne predpise,
- uporabe in zanesljivosti delovanja strojne in programske opreme imetnikov potrdil.

Izdajatelj SI-PASS-CA oz. overitelj na MJU jamči za vrednost posameznega pravnega posla glede na vrsto potrdila do vrednosti:

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

- 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[9]

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}: 1.3.6.1.4.1.6105.7.1.1 za kvalificirana digitalna potrdila za fizične osebe za kvalificiran elektronski podpis,
- CP_{OID}: 1.3.6.1.4.1.6105.7.2.1 za kvalificirana digitalna potrdila za fizične osebe in
- CP_{OID}: 1.3.6.1.4.1.6105.7.3.1 za normalizirana digitalna potrdila za fizične osebe.

Overitelj na MJU in izdajatelj SI-PASS-CA delujeta v skladu z:

- Zakonom o elektronskem poslovanju in elektronskem podpisu,
- Uredbo eIDAS,
- evropskimi direktivami,
- Zakonom o varstvu osebnih podatkov,
- Zakonom o tajnih podatkih,
- priporočili ETSI s področja kvalificiranih potrdil in storitev zaupanja,
- priporočili RFC s področja potrdil X.509,
- in drugimi veljavnimi predpisi in priporočili.

8. Varovanje osebnih podatkov in čas hrambe

8.1. Varovanje osebnih podatkov[10]

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 ustreznih registrih za dokazovanje istovetnosti imetnika.

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

Overitelj na MJU je odgovoren v skladu z Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo) in drugo veljavno zakonodajo glede varovanja osebnih podatkov.

Imetnik pooblasti overitelja na MJU oz. izdajatelja SI-PASS-CA za uporabo osebnih podatkov na zahtevku za pridobitev potrdila ali kasneje v pisni obliki.

Overitelj na MJU 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 overitelja na MJU imetnik pooblastil za to (glej prejšnje podpoglavje), ali na zahtevo pristojnega sodišča ali upravnega organa.

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

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

8.2. Čas hrambe[11]

Arhivirani podatki v zvezi s ključi in digitalnimi potrdili se hranijo vsaj sedem (7) let po poteku potrdila, na katerega se podatek nanaša.

Ostali arhivirani podatki se hranijo vsaj sedem (7) let po njihovem nastanku.

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

9. Povrnitev stroškov[12]

Stroški upravljanja s potrdili se obračunavajo po objavljenem ceniku na spletni strani http://www.si-pass-ca.gov.si/cenik.php. Povrnitev stroškov imetniku ni predpisana.

10. Postopek v primeru sporov[13]

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[14]

Nadzor nad skladnostjo delovanja overitelja na MJU 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 določb ZEPEP overitelja na MJU skladno z ZEPEP opravlja pristojna inšpekcijska služba v skladu z veljavno zakonodajo za inšpekcijski nadzor.

Notranje preverjanje skladnosti delovanja izvaja notranji revizor in ostale pooblaščene osebe v okviru overitelja na MJU.

Inšpekcijska služba je 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. overitelj na MJU prizadeva za odpravo le-teh v najkrajšem možnem času.

Overitelj na MJU javno objavi povzetek sklepov inšpekcijskega nadzora na svojih spletnih straneh.

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