



Državni center za storitve zaupanja
Izdajatelj kvalificiranih digitalnih potrdil SIGEN-CA



IZJAVA O POLITIKI SIGEN-CA

za spletna kvalificirana digitalna potrdila za fizične osebe

*Povzetek javnega dela notranjih pravil Državnega centra za
storitve zaupanja*

veljavnost: od 20. oktobra 2020
verzija: 7.2

CP_{Name}: SIGEN-CA-2

CP_{OID}: 1.3.6.1.4.1.6105.2.2.3.5



VSEBINA

1.	PODATKI O PONUDNIKU STORITEV ZAUPANJA	3
2.	DIGITALNA POTRDILA, NJIHOVA PRIDOBITEV IN UPORABA	3
2.1.	Vrste potrdil	3
2.2.	Pridobitev potrdil.....	3
2.3.	Uporaba potrdil in ključev	4
3.	OMEJITVE PRI UPORABI	4
4.	DOLŽ NOSTI IN ODGOVORNOSTI IMETNIKA	5
5.	ZAHTEVE PO PREVERJANJU REGISTRA PREKLICANIH POTRDIL ZA TRETJE OSEBE	5
6.	ZANIKANJE IN OMEJITEV ODGOVORNOSTI	6
7.	POLITIKA IN VELJAVNA ZAKONODAJA	6
8.	VAROVANJE OSEBNIH PODATKOV IN ČAS HRAMBE	7
8.1.	Varovanje osebnih podatkov	7
8.2.	Čas hrambe.....	7
9.	POVRNITEV STROŠKOV	8
10.	POSTOPEK V PRIMERU SPOROV	8
11.	SKLADNOST Z VELJAVNO ZAKONODAJO	8

1. Podatki o ponudniku storitev zaupanja¹

Kontaktne podatke Državnega centra za storitve zaupanja, ki deluje v okviru Ministrstva za javno upravo (v nadaljevanju *SI-TRUST*):

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

Kontaktne podatke izdajatelja SIGEN-CA:

Naslov:	SIGEN-CA Državni center za storitve zaupanja Ministrstvo za javno upravo Tržaška cesta 21 1000 Ljubljana
E-pošta:	sigen-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 potrdil²

Po pričujoči politiki SIGEN-CA izdaja spletna kvalificirana digitalna potrdila za fizične osebe po CP_{OID}: 1.3.6.1.4.1.6105.2.2.3.5.

Oznaka politike je CP_{Name}: SIGEN-CA-2, identifikacijska oznaka politike SIGEN-CA-2 pa CP_{OID}: 1.3.6.1.4.1.6105.2.2.3.5.

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

2.2. Pridobitev potrdil³

Bodoči imetniki potrdil so vedno fizične osebe.

Za pridobitev potrdila mora bodoči imetnik pravilno izpolniti in podpisati zahtevek za pridobitev potrdila. Zahtevek lahko odda procesno sposobna oseba, starejša od 15 let.

¹ Politika SIGEN-CA za fizične osebe, pogl. 1.3.1

² Politika SIGEN-CA za fizične osebe, pogl. 1.1, 1.2

³ Politika SIGEN-CA za fizične osebe, pogl. 4.1, 4.2, 4.3

V primeru, da je bodoči imetnik invalidna oseba, lahko zahtevek za pridobitev potrdila odda v njegovem imenu druga oseba, ki mora priložiti notarsko ali upravno overjeno pooblastilo ter svoj veljavni osebni dokument s sliko.

Bodoči imetnik lahko izdajatelju SIGEN-CA po elektronski poti posreduje zahtevek, digitalno podpisan z njegovim veljavnim kvalificiranim digitalnim potrdilom za fizične osebe, ki mu ga je izdal izdajatelj SIGEN-CA.

V primeru osebne oddaje zahtevka na prijavnih službi pooblaščen oseba na prijavnih službi preveri istovetnost bodočega imetnika v skladu z veljavno zakonodajo. Bodoči imetnik mora izkazati svojo istovetnost z veljavnim osebnim dokumentom.

V primeru oddaje zahtevka na elektronski način pooblaščen oseba izdajatelja SIGEN-CA opravi overjanje elektronskega podpisa. Istovetnost bodočega imetnika se izkaže z veljavnostjo njegovega elektronskega podpisa.

Zahtevek za pridobitev potrdila odobrijo oz. v primeru nepravilnih ali pomanjkljivih podatkov ali neizpolnjevanja obveznosti zavrnejo pooblaščen oseba izdajatelja SIGEN-CA.

SIGEN-CA na podlagi odobrenega zahtevka bodočemu imetniku digitalnega potrdila avtorizacijsko kodo in referenčno številko posreduje najkasneje v desetih (10) dneh od odobritve zahtevka.

V primeru odobrenega zahtevka SIGEN-CA posreduje bodočemu imetniku potrdila referenčno številko in avtorizacijsko kodo po dveh ločenih poteh: referenčno številko po elektronski pošti, avtorizacijsko kodo pa s pošto pošiljko, izjemoma pa ju lahko pooblaščen oseba SIGEN-CA preda tudi osebno. Oba podatka bodoči imetnik potrebuje za prevzem digitalnega potrdila.

Potrdila se izdajajo izključno na infrastrukturi SI-TRUST.

2.3. Uporaba potrdil in ključ ev⁴

Imetnik oziroma bodoči imetnik potrdila je glede varovanja zasebnega ključa dolžan:

- podatke za prevzem potrdila skrbno varovati pred nepooblaščenimi osebami,
- hraniti zasebni ključ in potrdilo v skladu z obvestili in priporočili SIGEN-CA,
- zasebni ključ in vse druge zaupne podatke ščititi s primernim geslom v skladu s priporočili SIGEN-CA ali na drug način tako, da ima dostop do njih samo imetnik,
- skrbno varovati gesla za zaščito zasebnega ključa,
- po preteku veljavnosti oz. preklicu potrdila ravnati v skladu z obvestili SIGEN-CA.

Imetnik mora varovati zasebni ključ pred nepooblaščen uporabo.

3. Omejitve pri uporabi⁵

Digitalna potrdila SIGEN-CA se lahko uporabljajo za:

- šifriranje podatkov v elektronski obliki,
- overjanje digitalno podpisanih podatkov v elektronski obliki ter izkazovanje istovetnosti imetnika,
- storitve oz. aplikacije, za katere se zahteva uporaba kvalificiranih digitalnih potrdil SI-TRUST.

Dnevnik 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 dnevnik beleženih dogodkov se hranijo vsaj sedem (7) let po nastanku dogodka.

⁴ Politika SIGEN-CA za fizične osebe, pogl. 4.5

⁵ Politika SIGEN-CA za fizične osebe, pogl. 1.1, 4.5, 5.4.3

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

4. Dolž nosti in odgovornosti imetnika⁶

Imetnik oziroma bodoči imetnik potrdila je glede varovanja zasebnega ključa dolžan:

- podatke za prevzem potrdila skrbno varovati pred nepooblaščenimi osebami,
- hraniti zasebni ključ in potrdilo v skladu z obvestili in priporočili SIGEN-CA,
- zasebni ključ in vse druge zaupne podatke ščititi s primernim geslom v skladu s priporočili SIGEN-CA ali na drug način tako, da ima dostop do njih samo imetnik,
- skrbno varovati gesla za zaščito zasebnega ključa,
- po preteku veljavnosti oz. preklicu potrdila ravnati v skladu z obvestili SIGEN-CA.

Imetnik mora varovati zasebni ključ pred nepooblaščenno 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 potrdila oz. drugo storitev od izdajatelja SIGEN-CA ne prejme obvestila po e-pošti, ki jo je navedel v zahtevku, se mora obrniti na pooblaščen osebo izdajatelja SIGEN-CA,
- po prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti SIGEN-CA oziroma zahtevati preklic potrdila,
- v kolikor po oddaji zahtevka za pridobitev potrdila oz. drugo storitev od izdajatelja SIGEN-CA ne prejme obvestila po e-pošti, ki jo je navedel v zahtevku, potem se mora obrniti na pooblaščen osebo izdajatelja SIGEN-CA,
- spremljati vsa obvestila SIGEN-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 SIGEN-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 SIGEN-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 omogočena uporaba oz. zloraba imetnikovega potrdila s strani nepooblaščenih oseb,
- vsako drugo škodo, ki izvira iz neupoštevanja določil te politike in drugih obvestil SIGEN-CA ter veljavnih predpisov.

5. Zahteve po preverjanju registra preklicanih potrdil za tretje osebe⁷

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

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

⁶ Politika SIGEN-CA za fizične osebe, pogl. 4.5.1, 9.6.3

⁷ Politika SIGEN-CA za fizične osebe, pogl. 4.9.6, 4.9.7, 4.9.9

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 omejitve odgovornosti⁸

SI-TRUST ni odgovoren za škodo, ki bi nastala zaradi:

- uporabe potrdil za namen in na način, ki ni izrecno predviden v politiki izdajatelja SIGEN-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 SIGEN-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,
- 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 SIGEN-CA ali druge veljavne predpise,
- uporabe in zanesljivosti delovanja strojne in programske opreme imetnikov potrdil.

Izdajatelj SIGEN-CA oz. SI-TRUST jamči za vrednost posameznega pravnega posla do vrednosti 1.000 EUR.

7. Politika in veljavna zakonodaja⁹

Izhodiščni dokument je Politika SIGEN-CA za kvalificirana digitalna potrdila za fizične osebe.

Oznaka pričujoče politike je CP_{Name}: SIGEN-CA-2, identifikacijska oznaka politike SIGEN-CA-2 pa CP_{OID}: 1.3.6.1.4.1.6105.2.2.3.5.

⁸ Politika SIGEN-CA za fizične osebe, pogl. 9.7, 9.8

⁹ Politika SIGEN-CA za fizične osebe, pogl. 1.2, 9.14

SI-TRUST in SIGEN-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 o izvajanju Uredbe (EU) o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (Uradni list RS, št. 46/16),
- 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 (Uradni list EU, št. L 119/1),
- 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,
- 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 podatkov¹⁰

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

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

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 SIGEN-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 (glej prejšnje podpoglavje), 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 hrambe¹¹

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

¹⁰ Politika SIGEN-CA za fizične osebe, pogl. 9.4

¹¹ Politika SIGEN-CA za fizične osebe, pogl. 5.5.2

zakonodajo.

9. Povrnitev stroškov¹²

Stroški upravljanja s potrdili se obračunavajo po objavljenem ceniku na spletni strani <https://www.si-trust.gov.si/sl/digitalna-potrdila/fizicne-osebe/>.

10. Postopek v primeru sporov¹³

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 zakonodajo¹⁴

Nadzor nad skladnostjo delovanja SI-TRUST 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.

Notranje preverjanje skladnosti delovanja izvaja notranji revizor in ostale pooblaščen 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 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.

¹² Politika SIGEN-CA za fizične osebe, pogl. 9.1

¹³ Politika SIGEN-CA za fizične osebe, pogl. 9.13

¹⁴ Politika SIGEN-CA za fizične osebe, pogl. 9.15, 8