IZJAVA O POLITIKI SIGOV-CA

za kvalificirana digitalna potrdila za državne organe

Povzetek javnega dela notranjih pravil Državnega centra za storitve zaupanja

veljavnost: od 31. decembra 2025
verzija: 8.7

CP_{Name}: SIGOV-CA

- Politika za spletna kvalificirana digitalna potrdila za zaposlene
  CP_{OID}: 1.3.6.1.4.1.6105.1.1.10
- Politika za spletna kvalificirana digitalna potrdila za zaposlene z obvezno uporabo pametnih kartic
  CP_{OID}: 1.3.6.1.4.1.6105.1.2.10
- Politika za posebna kvalificirana digitalna potrdila za zaposlene
  CP_{OID}: 1.3.6.1.4.1.6105.1.3.10
- Politika za posebna kvalificirana digitalna potrdila za zaposlene z obvezno uporabo pametnih kartic
  CP_{OID}: 1.3.6.1.4.1.6105.1.4.10
- Politika za spletna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom
  CP_{OID}: 1.3.6.1.4.1.6105.1.5.10
- Politika za spletna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom z obvezno uporabo pametnih kartic
  CP_{OID}: 1.3.6.1.4.1.6105.1.6.10
- Politika za posebna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom
  CP_{OID}: 1.3.6.1.4.1.6105.1.7.10
- Politika za posebna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom z obvezno uporabo pametnih kartic
  CP_{OID}: 1.3.6.1.4.1.6105.1.8.10
- Politika za spletna normalizirana digitalna potrdila za informacijske sisteme
  CP_{OID}: 1.3.6.1.4.1.6105.1.9.10
- Politika za spletna normalizirana digitalna potrdila za podpis kode
  CP_{OID}: 1.3.6.1.4.1.6105.1.10.10
- Politika za normalizirana digitalna potrdila za izdajatelje kvalificiranih **časovnih žigov**
  CP_{OID}: 1.3.6.1.4.1.6105.1.11.10
- Politika za normalizirana digitalna potrdila za sisteme za preverjanje veljavnosti digitalnih potrdil
  CP_{OID}: 1.3.6.1.4.1.6105.1.12.10
- **Politika za spletna kvalificirana digitalna potrdila za avtentikacijo spletišč**
  CP_{OID}: 1.3.6.1.4.1.6105.1.13.10
- Politika za spletna kvalificirana digitalna potrdila za elektronski žig
  CP_{OID}: 1.3.6.1.4.1.6105.1.14.10
- Politika za spletna kvalificirana digitalna potrdila za elektronski žig z obvezno uporabo pametnih kartic
  CP_{OID}: 1.3.6.1.4.1.6105.1.15.10

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 ... 4
2.3. **Uporaba potrdil in ključev** ... 5
3. OMEJITVE PRI UPORABI ... 5
4. DOLŽNOSTI IN ODGOVORNOSTI IMETNIKA OZIROMA ORGANIZACIJE ... 6
5. ZAHTEVE PO PREVERJANJU REGISTRA PREKLICANIH POTRDIL ZA TRETJE OSEBE ... 7
6. ZANIKANJE IN OMEJITEV ODGOVORNOSTI ... 7
7. POLITIKA IN VELJAVNA ZAKONODAJA ... 8
*8. **VAROVANJE OSEBNIH PODATKOV IN ČAS HRAMBE** ... 9*
8.1. Varovanje osebnih podatkov ... 9
8.2. **Čas hrambe** ... 9
9. POVRNITEV STROŠKOV ... 9
10. POSTOPEK V PRIMERU SPOROV ... 9
11. SKLADNOST Z VELJAVNO ZAKONODAJO ... 10

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:	https://www.si-trust.gov.si
Oznaka:	State-institutions

Kontaktni podatki izdajatelja SIGOV-CA:

Naslov:	SIGOV-CA Državni center za storitve zaupanja Ministrstvo za digitalno preobrazbo Tržaška cesta 21 1000 Ljubljana
E-pošta:	sigov-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 SIGOV-CA izdaja naslednja digitalna potrdila:

- posebna kvalificirana digitalna potrdila za zaposlene v organizacijah,
- posebna kvalificirana digitalna potrdila za zaposlene v organizacijah z obvezno uporabo pametnih kartic,
- posebna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom organizacije oz. organizacijske enote,
- posebna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom organizacije oz. organizacijske enote z obvezno uporabo pametnih kartic,
- spletna kvalificirana digitalna potrdila za zaposlene v organizacijah,
- spletna kvalificirana digitalna potrdila za zaposlene v organizacijah z obvezno uporabo pametnih kartic,
- spletna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom organizacije oz. organizacijske enote,
- spletna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom organizacije oz. organizacijske enote z obvezno uporabo pametnih kartic,

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

- spletna kvalificirana digitalna potrdila za avtentikacijo spletišč, s katerimi upravljajo organizacije,
- spletna kvalificirana digitalna potrdila za elektronske žige organizacij,
- spletna kvalificirana digitalna potrdila za elektronske žige organizacij z obvezno uporabo pametnih kartic,
- spletna normalizirana digitalna potrdila za informacijske sisteme, s katerimi upravljajo organizacije,
- spletna normalizirana digitalna potrdila za podpis kode za potrebe organizacije,
- normalizirana digitalna potrdila za izdajatelje kvalificiranih časovnih žigov,
- normalizirana digitalna potrdila za sisteme za sprotno preverjanje veljavnosti digitalnih potrdil.

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

- CP_{OID}: 1.3.6.1.4.1.6105.1.1.10 za spletna kvalificirana digitalna potrdila za zaposlene,
- CP_{OID}: 1.3.6.1.4.1.6105.1.2.10 za spletna kvalificirana digitalna potrdila za zaposlene z obvezno uporabo pametnih kartic,
- CP_{OID}: 1.3.6.1.4.1.6105.1.3.10 za posebna kvalificirana digitalna potrdila za zaposlene,
- CP_{OID}: 1.3.6.1.4.1.6105.1.4.10 za posebna kvalificirana digitalna potrdila za zaposlene z obvezno uporabo pametnih kartic,
- CP_{OID}: 1.3.6.1.4.1.6105.1.5.10 za spletna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom,
- CP_{OID}: 1.3.6.1.4.1.6105.1.6.10 za spletna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom z obvezno uporabo pametnih kartic,
- CP_{OID}: 1.3.6.1.4.1.6105.1.7.10 za posebna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom,
- CP_{OID}: 1.3.6.1.4.1.6105.1.8.10 za posebna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom z obvezno uporabo pametnih kartic,
- CP_{OID}: 1.3.6.1.4.1.6105.1.9.10 za spletna normalizirana digitalna potrdila za strežnike,
- CP_{OID}: 1.3.6.1.4.1.6105.1.10.10 za spletna normalizirana digitalna potrdila za podpis kode,
- CP_{OID}: 1.3.6.1.4.1.6105.1.11.10 za normalizirana digitalna potrdila za izdajatelje kvalificiranih časovnih žigov (v nadaljevanju *TSA*, angl. *Time Stamp Authority*),
- CP_{OID}: 1.3.6.1.4.1.6105.1.12.10 za normalizirana digitalna potrdila za sisteme za preverjanje veljavnosti digitalnih potrdil (v nadaljevanju *OCSP*, angl. *Online Certificate Status Protocol*),
- CP_{OID}: 1.3.6.1.4.1.6105.1.13.10 za spletna kvalificirana digitalna potrdila za avtentikacijo spletišč,
- CP_{OID}: 1.3.6.1.4.1.6105.1.14.10 za spletna kvalificirana digitalna potrdila za elektronski žig,
- CP_{OID}: 1.3.6.1.4.1.6105.1.15.10 za spletna kvalificirana digitalna potrdila za elektronski žig z obvezno uporabo pametnih kartic.

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

2.2. Pridobitev potrdil[3]

Bodoči imetniki potrdil so vedno fizične osebe, zaposlene v organizaciji, za katere le-ta želi pridobiti potrdilo. V primeru potrdila za informacijske sisteme, podpis kode, avtentikacijo spletišč in elektronske žige je imetnik takega potrdila pooblaščen s strani predstojnika, v primeru potrdila za izdajatelja kvalificiranih časovnih žigov in sistem za sprotno preverjanje veljavnosti digitalnih potrdil pa predstojnik organizacije oz. od predstojnika pooblaščena oseba.

Za pridobitev potrdila morata bodoči imetnik in predstojnik pravilno izpolniti in podpisati zahtevek za pridobitev potrdila.

Predstojnik organizacije, kjer je bodoči imetnik potrdila zaposlen, jamči za istovetnost bodočega imetnika potrdila, ki ga je preveril v skladu z veljavno zakonodajo.

[3] Politika SIGOV-CA, pogl. 4.1, 4.2, 4.3

Zahtevek za pridobitev potrdila odobrijo oz. v primeru nepravilnih ali pomanjkljivih podatkov ali neizpolnjevanja obveznosti iz dogovora s strani organizacije zavrnejo pooblaščene osebe SI-TRUST.

SIGOV-CA bodočemu imetniku digitalnega potrdila z obvezno uporabo pametne kartice pametno kartico skupaj z digitalnim potrdilom in navodili za ravnanje na varen način posreduje najkasneje v desetih (10) dneh od odobritve zahtevka.

SIGOV-CA bodočemu imetniku digitalnega potrdila brez obvezne uporabe pametne kartice avtorizacijsko kodo in referenčno številko posreduje najkasneje v desetih (10) dneh od odobritve zahtevka.

Potrdila se izdajajo izključno na infrastrukturi SI-TRUST.

V primeru odobrenega zahtevka za potrdilo z obvezno uporabo pametne kartice SIGOV-CA bodočemu imetniku potrdila preko kontaktne osebe organizacije, ki je zaprosila za imetnikovo potrdilo, posreduje pametno kartico z digitalnim potrdilom, prednastavljeno geslo za dostop do digitalnega potrdila pa s poštno pošiljko z oznako »Osebno« na naslov njegove organizacije.

V primeru odobrenega zahtevka za potrdilo brez obvezne uporabe pametne kartice SIGOV-CA posreduje bodočemu imetniku potrdila referenčno številko in avtorizacijsko kodo po dveh ločenih poteh: referenčno številko po elektronski pošti, avtorizacijsko kodo pa s poštno pošiljko, izjemoma pa ju lahko pooblaščena oseba SIGOV-CA preda tudi osebno. Oba podatka bodoči imetnik potrebuje za prevzem digitalnega potrdila.

*2.3. Uporaba potrdil **in ključev**[4]*

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 SIGOV-CA,
- zasebni ključ in vse druge zaupne podatke ščititi s primernim geslom v skladu s priporočili SIGOV-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 SIGOV-CA.

Imetnik mora varovati zasebni ključ za podpisovanje podatkov pred nepooblaščeno uporabo.

3. Omejitve pri uporabi[5]

Digitalna potrdila SIGOV-CA (v nadaljevanju *potrdila*) 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.

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] Politika SIGOV-CA, pogl. 4.5
[5] Politika SIGOV-CA, pogl. 1.1, 4.5, 5.4.3

4. Dolžnosti in odgovornosti imetnika oziroma organizacije[6]

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 SIGOV-CA,
- zasebni ključ in vse druge zaupne podatke ščititi s primernim geslom v skladu s priporočili SIGOV-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 SIGOV-CA.

Imetnik mora varovati zasebni ključ za podpisovanje podatkov pred nepooblaščeno uporabo.

Imetnik oziroma bodoči imetnik potrdila je dolžan:
- seznaniti se s to politiko in morebitnim dogovorom med organizacijo in SI-TRUST pred izdajo potrdila,
- ravnati v skladu s politiko in določili iz morebitnega dogovora med organizacijo in SI-TRUST in ostalimi veljavnimi predpisi,
- če po oddaji zahtevka za pridobitev potrdila oz. drugo storitev od izdajatelja SIGOV-CA ne prejme obvestila po e-pošti, ki jo je navedel v zahtevku, se mora obrniti na pooblaščene osebe izdajatelja SIGOV-CA,
- po prejemu oz. po prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti SIGOV-CA oziroma zahtevati preklic potrdila,
- spremljati vsa obvestila SIGOV-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 SIGOV-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 SIGOV-CA,
- skrbeti za originalno podpisane dokumente in arhiv teh dokumentov.

Predstojnik oz. organizacija je dolžna:
- skrbno prebrati politiko in določila iz dogovora med organizacijo in SI-TRUST pred podpisom zahtevka za pridobitev potrdila,
- zagotoviti, da imetniki potrdil za njegovo organizacijo izpolnjujejo vse zahteve iz te politike in veljavnih predpisov,
- redno spremljati vsa obvestila SIGOV-CA,
- ravnati v skladu z obvestili, politiko in dogovorom med organizacijo in SI-TRUST in ostalimi veljavnimi predpisi,
- zagotoviti, da imetniki potrdil ustrezno posodabljajo potrebno strojno in programsko opremo za varno delo s potrdili,
- skrbeti za arhiv elektronskih dokumentov ter potrebnih podatkov za uporabo potrdil,
- vse spremembe glede imetnika in organizacije, ki so povezane s potrdilom imetnika, nemudoma sporočiti SIGOV-CA,
- zahtevati preklic potrdila, če so bili zasebni ključi imetnika potrdila ogroženi na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

Organizacija 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,

[6] Politika SIGOV-CA, pogl. 4.5.1, 9.6.3

- vsako drugo škodo, ki izvira iz neupoštevanja določil te politike in drugih obvestil SIGOV-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 register preklicanih potrdil.

Zaradi verodostojnosti in celovitosti je vedno potrebno preveriti veljavnost in verodostojnost tega registra, ki je digitalno podpisan s strani SIGOV-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[8]

SI-TRUST ni odgovoren za škodo, ki bi nastala zaradi:
- uporabe potrdil za namen in na način, ki ni izrecno predviden v politiki izdajatelja SIGOV-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 SIGOV-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 SIGOV-CA ali druge veljavne predpise,
- uporabe in zanesljivosti delovanja strojne in programske opreme imetnikov potrdil.

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

Izdajatelj SIGOV-CA oz. SI-TRUST jamči za vrednost posameznega pravnega posla glede na vrsto potrdila do vrednosti:

- za digitalna potrdila z obvezno uporabo pametnih kartic do višine 5.000 EUR ter
- za potrdila brez obvezne uporabe pametnih kartic do višine 1.000 EUR.

7. Politika in veljavna zakonodaja[9]

Izhodiščni dokument je Politika SIGOV-CA kvalificirana digitalna potrdila za državne organe.

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

- CP_{OID}: 1.3.6.1.4.1.6105.1.1.10 za spletna kvalificirana digitalna potrdila za zaposlene,
- CP_{OID}: 1.3.6.1.4.1.6105.1.2.10 za spletna kvalificirana digitalna potrdila za zaposlene z obvezno uporabo pametnih kartic,
- CP_{OID}: 1.3.6.1.4.1.6105.1.3.10 za posebna kvalificirana digitalna potrdila za zaposlene,
- CP_{OID}: 1.3.6.1.4.1.6105.1.4.10 za posebna kvalificirana digitalna potrdila za zaposlene z obvezno uporabo pametnih kartic,
- CP_{OID}: 1.3.6.1.4.1.6105.1.5.10 za spletna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom,
- CP_{OID}: 1.3.6.1.4.1.6105.1.6.10 za spletna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom z obvezno uporabo pametnih kartic,
- CP_{OID}: 1.3.6.1.4.1.6105.1.7.10 za posebna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom,
- CP_{OID}: 1.3.6.1.4.1.6105.1.8.10 za posebna kvalificirana digitalna potrdila za zaposlene s splošnim nazivom z obvezno uporabo pametnih kartic,
- CP_{OID}: 1.3.6.1.4.1.6105.1.9.10 za spletna normalizirana digitalna potrdila za strežnike,
- CP_{OID}: 1.3.6.1.4.1.6105.1.10.10 za spletna normalizirana digitalna potrdila za podpis kode,
- CP_{OID}: 1.3.6.1.4.1.6105.1.11.10 za normalizirana digitalna potrdila za izdajatelje kvalificiranih časovnih žigov (v nadaljevanju *TSA*, angl. *Time Stamp Authority*),
- CP_{OID}: 1.3.6.1.4.1.6105.1.12.10 za normalizirana digitalna potrdila za sisteme za preverjanje veljavnosti digitalnih potrdil (v nadaljevanju *OCSP*, angl. *Online Certificate Status Protocol*),
- CP_{OID}: 1.3.6.1.4.1.6105.1.13.10 za spletna kvalificirana digitalna potrdila za avtentikacijo spletišč,
- CP_{OID}: 1.3.6.1.4.1.6105.1.14.10 za spletna kvalificirana digitalna potrdila za elektronski žig,
- CP_{OID}: 1.3.6.1.4.1.6105.1.15.10 za spletna kvalificirana digitalna potrdila za elektronski žig z obvezno uporabo pametnih kartic.

SI-TRUST in SIGOV-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,

[9] Politika SIGOV-CA, pogl. 1.2, 9.14

- 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[10]

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 SIGOV-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 oz. odgovorna oseba organizacije pooblasti SI-TRUST oz. izdajatelja SIGOV-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 oz. predstojnik organizacije 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[11]

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[12]

Stroški upravljanja s potrdili se imetnikom ne obračunavajo.

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

[10] Politika SIGOV-CA, pogl. 9.4
[11] Politika SIGOV-CA, pogl. 5.5.2
[12] Politika SIGOV-CA, pogl. 9.1
[13] Politika SIGOV-CA, pogl. 9.13

Republike Slovenije.

11. Skladnost z veljavno zakonodajo[14]

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 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 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.

[14] Politika SIGOV-CA, pogl. 9.15, 8