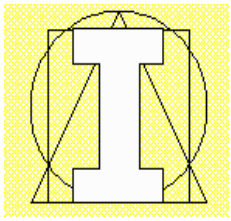

VLADA REPUBLIKE SLOVENIJE
CENTER ZA INFORMATIKO

POLITIKA SIGOV-CA

za službena spletna kvalificirana potrdila

Javni del notranjih pravil SIGOV-CA

Politika je veljavna od 17. januarja 2001

CP_{Name}: SIGOV-CA-1
CP_{OID}: 1.3.6.1.4.1.6105.1.1.1

VSEBINA

1. UVOD

(1) SIGOV-CA je overitelj kvalificiranih digitalnih potrdil na Centru Vlade za informatiko (CVI). Politike SIGOV-CA predstavljajo celoten javni del notranjih pravil SIGOV-CA glede posameznih vrst kvalificiranih digitalnih potrdil in določajo namen, delovanje in metodologijo upravljanja s kvalificiranimi digitalnimi potrdili, odgovornost SIGOV-CA ter varnostne zahteve, ki jih morajo izpolnjevati imetniki, tretje osebe, ki se zanašajo na kvalificirana digitalna potrdila, in drugi overitelji, ki želijo uporabljati storitve SIGOV-CA.

(2) SIGOV-CA izdaja kvalificirana digitalna potrdila, za katera velja najvišja stopnja varovanja in načela t.i. močne enkripcije ter deluje v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 57/2000) in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000 in 2/2001).

(3) Kvalificirana digitalna potrdila, ki jih izdaja SIGOV-CA, so namenjena izključno uporabi v javni upravi, za izmenjavo podatkov z institucijami javne uprave in za dostop do podatkov, s katerimi upravlja javna uprava. Za vsako drugo uporabo kvalificiranih digitalnih potrdil SIGOV-CA ni odgovorna. V primeru medsebojnega priznavanja z drugim overiteljem se dodatni namen kvalificiranih digitalnih potrdil določi na osnovi pisne dvostranske pogodbe obeh overiteljev in se javno objavi.

(4) SIGOV-CA izdaja štiri vrste kvalificiranih digitalnih potrdil:
- službena osebna kvalificirana digitalna potrdila,
- službena spletna kvalificirana digitalna potrdila,
- osebna kvalificirana digitalna potrdila za fizične in pravne osebe,
- spletna kvalificirana digitalna potrdila za fizične in pravne osebe.

(5) Osebna kvalificirana digitalna potrdila se lahko uporabljajo za:
- šifriranje in dešifriranje podatkov v elektronski obliki,
- digitalno podpisovanje podatkov v elektronski obliki ter izkazovanje identitete podpisnika,
- varno brisanje podatkov v elektronski obliki,
- uporabo v specifičnih aplikacijah, ki jih v soglasju z upraviteljem oziroma skrbnikom aplikacije ali z njo povezane podatkovne baze odobri SIGOV-CA in so navedene v seznamu odobrenih aplikacij, ki je javno objavljen na spletnih straneh SIGOV-CA.

(6) Spletna kvalificirana digitalna potrdila se lahko uporabljajo za:
- varno spletno komuniciranje po protokolih SSL (Secure Sockets Layer) in TLS (Transport Layer Security),
- varno pošiljanje elektronske pošte po protokolu S/MIME (Secure Multipurpose Internet Mail Extensions),
- uporabo v specifičnih aplikacijah, ki jih v soglasju z upraviteljem oziroma skrbnikom aplikacije ali z njo povezane podatkovne baze odobri SIGOV-CA in so navedene v seznamu odobrenih aplikacij, ki je javno objavljen na spletnih straneh SIGOV-CA.

(7) Službena kvalificirana digitalna potrdila so namenjena zaposlenim v javni upravi in drugim osebam, ki delajo za institucijo javne uprave in za katere želi ta institucija pridobiti službena kvalificirana digitalna potrdila, ki jih osebe potrebujejo za opravljanje dela za to institucijo.

Kvalificirana digitalna potrdila za fizične in pravne osebe pa so namenjena vsem fizičnim in pravnim osebam za izmenjavo podatkov z javno upravo.

(8) Politika delovanja SIGOV-CA je definirana z vrsto kvalificiranih digitalnih potrdil:

- Politika SIGOV-CA za službena spletna kvalificirana digitalna potrdila (CP_{OID} = 1.3.6.1.4.1.6105.1.1.1),
- Politika SIGOV-CA za službena osebna kvalificirana digitalna potrdila (CP_{OID} = 1.3.6.1.4.1.6105.1.2.1),
- Politika SIGOV-CA za spletna kvalificirana digitalna potrdila za fizične in pravne osebe (CP_{OID} = 1.3.6.1.4.1.6105.1.3.1),
- Politika SIGOV-CA za osebna kvalificirana digitalna potrdila za fizične in pravne osebe (CP_{OID} = 1.3.6.1.4.1.6105.1.4.1).

(9) Glede preklica službenih kvalificiranih digitalnih potrdil ima predstojnik institucije javne uprave oziroma poslovodni organ enake pravice kot imetnik kvalificiranega potrdila.

(10) SIGOV-CA si pridržuje pravico do spremembe te politike in nadgradnje infrastrukture brez predhodnega obveščanja imetnikov kvalificiranih digitalnih potrdil. Veljavna kvalificirana digitalna potrdila pri tem ostanejo v veljavi do konca preteka veljavnosti po veljavni politiki ob njihovi izdaji. Nova politika SIGOV-CA se predhodno objavi na spletnih straneh SIGOV-CA pod novo identifikacijsko številko (CP_{OID}) in označenim datumom začetka njene veljavnosti. Vsa kvalificirana digitalna potrdila izdana po tem datumu se obravnavajo po novi politiki.

(11) SIGOV-CA se lahko povezuje v mrežo overiteljev na horizontalni (bilateralni) ali vertikalni ravni, to je ustanavlja in overja podrejene ali priznava enakovredne overitelje ter se povezuje v hierarhično globalno strukturo overiteljev.

(12) SIGOV-CA lahko overja in javno objavlja politike podrejenih overiteljev v primeru, da se nameni uporabe kvalificiranih digitalnih potrdil razlikujejo od namena uporabe, definirane v tej politiki.

2. SPLOŠNE DOLOČBE

(1) Pričujoča politika (CP_{OID} = 1.3.6.1.4.1.6105.1.1.1) definira delovanje SIGOV-CA za službena spletna kvalificirana digitalna potrdila.

(2) Posamezni izrazi imajo v nadaljevanju te politike naslednji pomen:

- **potrdilo** je službeno spletno kvalificirano digitalno potrdilo v elektronski obliki, ki povezuje podatke iz potrdila z imetnikovim zasebnim ključem ter potrjuje imetnikovo identiteto (*angl.: Digital certificate*),
- **povezana oseba** je oseba, ki dela za institucijo javne uprave in za katero želi ta institucija pridobiti potrdilo, ki ga oseba potrebuje za opravljanje dela za to institucijo,
- **objava SIGOV-CA** je javna objava na spletnih straneh SIGOV-CA,
- **obvestila SIGOV-CA** so vsa navodila, pojasnila, seznami, pogoji, posamezna obvestila, priporočila, standardi in drugi dokumenti, ki jih določi ali priporoči SIGOV-CA in jih objavi ali kako drugače posreduje imetnikom potrdil, njihovim institucijam ali tretjim osebam.

(3) SIGOV-CA upravlja (izdaja in overja, preklicuje, hrani in objavlja) s potrdili za:

- zaposlene v javni upravi in povezane osebe,
- strežnike (aplikacije ali podatkovne baze) v javni upravi, za katere institucija javne uprave želi pridobiti potrdilo in
- druge overitelje potrdil.

(4) Institucija javne uprave za svoje zaposlene in z njo povezane osebe opravlja naloge prijavne službe SIGOV-CA.

(5) Vsak prosilec za potrdilo ali imetnik potrdila ima pravico pritožbe glede kateregakoli postopka overitelja. Pritožbo v roku 15 dni v pisni obliki poda Komisiji za pritožbe SIGOV-CA osebno ali pošlje na elektronski naslov *komisija.sigov-ca@gov.si* oziroma poštni naslov:

Komisija za pritožbe SIGOV-CA
Center Vlade za informatiko
Langusova 4
1000 Ljubljana

(6) Komisijo za pritožbe SIGOV-CA sestavljajo predsednik in štirje člani. Vsaj dva člana ne smeta biti zaposlena na CVI, en član pa mora biti predstavnik imetnikov. Nihče od članov Komisije za pritožbe ne sme biti iz osebja SIGOV-CA.

(7) Komisijo za pritožbe SIGOV-CA imenuje direktor CVI. Komisija je pri svojem delu neodvisna in samostojna. Strokovno, tehnično in administrativno podporo Komisiji za pritožbe nudi CVI.

(8) Komisija za pritožbe SIGOV-CA odloči o vsaki prejeti pritožbi z večino glasov opredeljenih članov v roku 30 dni. O postopkovnih vprašanjih odloča z večino glasov vseh članov. Odločitev Komisije za pritožbe SIGOV-CA je dokončna in jo je SIGOV-CA dolžna izvršiti.

Komisija za pritožbe SIGOV-CA deluje v skladu s poslovnikom, ki ga odobri direktor CVI.

(9) Stroški upravljanja s potrdili se obračunavajo instituciji javne uprave enkrat letno po ceniku, ki ga objavi SIGOV-CA.

3. RAZPOZNAVNI PODATKI SIGOV-CA

3.1. Identiteta SIGOV-CA

Enolično ime: **C=SI, O=state-institutions, OU=SIGOV-CA**

Naslov: **SIGOV-CA**
Center Vlade za informatiko
Langusova 4
1000 LJUBLJANA
Slovenija
Tel.: (+386) 01 4788 600
Fax: (+386) 01 4788 649
E-pošta: SIGOV-CA@GOV.SI

Dežurna številka za preklice: **Tel.: (+386) 01 4788 777**

Osnovne informacije o SIGOV-CA so na voljo na spletnem strežniku CVI z naslovom:

http://www.sigov-ca.gov.si

SIGOV-CA je ob začetku svojega produkcijskega delovanja generirala svoje lastno potrdilo (potrdilo SIGOV-CA, serijska številka 3A5C 701A), ki je namenjeno podpisovanju potrdil za druge uporabnike ter preverjanju podpisa SIGOV-CA oz. veljavnosti podatkov v potrdilih uporabnikov.

Potrdilo SIGOV-CA vsebuje naslednje podatke:

Serijska številka	3A5C 701A
Overitelj potrdila	SIGOV-CA
Imetnik potrdila	SIGOV-CA
Veljavnost potrdila	od 10.1.2001 do 10.1.2021
Dolžina ključa	2048 bitov
MD5	739D D35F C63C 95FE C6ED 89E5 8208 DD89
SHA-1	7FB9 E2C9 95C9 7A93 9F9E 81A0 7AEA 9B4D 7046 3496

3.2. Identiteta imetnikov potrdil

Potrdila so shranjena v hierarhični podstrukturi imenika javne uprave na strežniku z imenom *x500.gov.si*, ki je dostopen znotraj podatkovno-komunikacijskega omrežja državnih organov.

Potrdila se nahajajo v veji:

OU=government, OU=web-certificates, O=state-institutions, C=si

Potrdila za strežnike se nahajajo v veji:

OU=servers, OU=web-certificates, O=state-institutions, C=si

3.3. Identiteta registra preklicanih potrdil

Register preklicanih potrdil se nahaja v veji:

CN=CRL*n*[1], OU=SIGOV-CA, O=state-institutions, C=si

[1] V registru preklicanih potrdil v imeniku javne uprave je lahko več takšnih seznamov oz. registrov, ki so označeni z zaporednimi številkami CRL1, CRL2, ...

4. INFRASTRUKTURA SIGOV-CA

4.1. Osnovne lastnosti SIGOV-CA

4.1.1. Varnost in zanesljivost infrastrukture SIGOV-CA

(1) Oprema SIGOV-CA je postavljena v posebnih, ločenih prostorih v okviru infrastrukture CVI, deloma pa tudi izven le-te. Zavarovana je z večnivojskim sistemom fizičnega in elektronskega varovanja. Stopnja varovanja infrastrukture SIGOV-CA ustreza nivoju varovanja po standardu *FIPS 140-1 level 3*.

(2) Varnostne kopije programske opreme in šifriranih baz SIGOV-CA se redno obnavljajo in shranjujejo v dveh ločenih in fizično varovanih prostorih. Redno se preverjajo računalniški dnevniki na vseh računalniško-komunikacijskih napravah s strani SIGOV-CA, izvajanje postopkov pa s strani nadzorne skupine SIGOV-CA.

(3) Opis infrastrukture SIGOV-CA, operativno delovanje in postopki upravljanja z infrastrukturo ter naloge nadzorne skupine SIGOV-CA so določeni z Interno politiko SIGOV-CA, ki predstavlja zaupni del notranjih pravil SIGOV-CA.

4.1.2. Šifrirni algoritmi, formati podatkov in protokoli infrastrukture SIGOV-CA

(1) SIGOV-CA uporablja:

- za podpisovanje potrdil algoritem SHA-1 z RSA s parom ključev dolžine 2048 bitov,
- za šifriranje podatkov algoritme Triple DES, CAST-128 in RC2, (standardi FIPS PUB 81, ANSI X3.106 in ISO/IEC 10116),
- zgostitveni algoritem SHA-1 (FIPS PUB 180-1 in ANSI X9.30(2)) in MD5 (RFC 1321),
- način uporabe algoritma RSA za upravljanje s ključi RSA (RFC 1421 in RFC 1423(PEM)) in PKCS#1,
- format potrdil ustreza priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:1997 ter X.509 ver. 3 (v3),
- registri preklicanih potrdil ustrezajo priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:1997, vključno z verzijo 2 (v2),
- oblika RSA enoličnih razločevalnih imen ter format javnega ključa ustrezajo priporočilu RFC 1422 in 1423 in PKCS#1,
- protokol LDAP ustreza priporočilu RFC 1777,
- hranjenje zasebnega ključa ustreza priporočiloma PKCS#5 in PKCS#8,
- komunikacija med programsko opremo na strani imetnika in infrastrukturo SIGOV-CA poteka po protokolu SEP (Secure Exchange Protocol), ki temelji na standardu GULS (Generic Upper Layers Security), ki ustreza priporočilom ITU-T za X.830, X.831, X.832 in ISO/IEC 11586-1, 11586-2 in 11586-3.

(2) Celoten nabor algoritmov, formatov podatkov in protokolov je na razpolago pri SIGOV-CA.

4.1.3. Osebje SIGOV-CA

(1) Operativno, organizacijsko in strokovno pravilno delovanje SIGOV-CA vodi vodja Službe za upravljanje digitalnih potrdil na CVI in je organizacijsko direktno podrejen direktorju CVI.

Med stalno pooblaščene osebe SIGOV-CA spadajo člani skupine SIGOV-CA in nadzorne skupine, ki jo vodi vodja Službe za varovanje in zaščito na CVI. Zunanje sodelavce, ki opravljajo dela za SIGOV-CA po potrebi, predlaga vodja SIGOV-CA in odobri direktor CVI.

(2) Skupina SIGOV-CA predstavlja operativno skupino SIGOV-CA. Razdeljena je na štiri organizacijske skupine, ki pokrivajo naslednja vsebinska področja:

- upravljanje z informacijskim sistemom,
- upravljanje s kvalificiranimi potrdili,
- varovanje in kontrola,
- pravno-administrativno.

Organizacijska skupina	Vloga	Osnovne naloge	Število oseb
Upravljanje z informacijskim sistemom	Upravljalec sistema	Strategija razvoja SIGOV-CA Določevanje prvega varnostnega inženirja Operativno vodenje SIGOV-CA	2
Upravljanje s kvalificiranimi potrdili	Prvi varnostni inženir	Določevanje in izvajanje pravil varnega delovanja sistema za podeljevanje potrdil Določevanje drugih varnostnih inženirjev	1
	Drugi varnostni inženirji	Določevanje in izvajanje pravil varnega delovanja sistema za podeljevanje potrdil	2
	Administratorji potrdil	Upravljanje s potrdili	2
Varovanje in kontrola	Varnostni administrator	Upravljanje s telekomunikacijami (sistem za preprečevanje in odkrivanje vdorov, požarna pregrada, ...) Vzdrževanje varnostnih kopij	1
Pravno-administrativno	Pravnik		1

(3) Vse organizacijske skupine skupine SIGOV-CA so med seboj nezdružljive. Navedeno število oseb predstavlja minimalno število, ki pa se lahko povečuje. Ob pomanjkanju ustrezno usposobljenega kadra pa se lahko zaradi podobne vrste opravil združi osebje določenih skupin z enakimi oz. podobnimi privilegiji delovanja. Vloge posameznih organizacijskih skupin so določene z Interno politiko SIGOV-CA.

4.1.4. Zavarovanje odgovornosti SIGOV-CA

CVI ima glede delovanja SIGOV-CA ustrezno zavarovano svojo odgovornost. Podrobnejše informacije so objavljene na spletnih straneh.

4.1.5. Zahteve za podrejene overitelje

SIGOV-CA zagotavlja, da podrejeni overitelji izpolnjujejo raven varnostnih zahtev, ki so določene v Pogojih za podrejene overitelje, ki jih izda in objavi SIGOV-CA. SIGOV-CA redno pregleduje izpolnjevanje varnostnih zahtev in postopkov pri upravljanju s potrdili podrejenih overiteljev.

4.1.6. Zahteve pri medsebojnem priznavanju

(1) SIGOV-CA se lahko povezuje in priznava z domačimi in tujimi overitelji, vendar ni dolžna priznati drugih overiteljev tudi, če ima drugi overitelj status akreditiranega overitelja. Medsebojno priznavanje se izvaja v skladu z na spletnih straneh objavljenimi Pogoji za medsebojno priznavanje overiteljev s SIGOV-CA in na podlagi podpisane pisne pogodbe.

(2) SIGOV-CA zagotavlja, da bo izvajala medsebojno priznavanje izključno po podpisu pisne pogodbe z drugimi overitelji, ki pa morajo izpolnjevati vsaj najmanjšo raven varnostnih zahtev, ki veljajo za podrejene overitelje SIGOV-CA. Pooblaščene osebe SIGOV-CA pregledujejo javni in zaupni del notranjih pravil drugega overitelja.

(3) Stroške potrebne infrastrukture, ki jo zahteva SIGOV-CA za medsebojno priznavanje, krije drugi overitelj.

(4) Bistvene dele pogodb o medsebojnem priznavanju, ki se nanašajo na lastnosti potrdil enega ali obeh overiteljev ali na pravice in obveznosti imetnikov teh potrdil ali tretjih oseb, ki se zanašajo na ta potrdila, objavi SIGOV-CA.

4.1.7. Namen prijavnih služb

(1) Institucija javne uprave za svoje zaposlene in z njo povezane osebe opravlja naloge prijavne službe SIGOV-CA. Institucija, kjer je bodoči imetnik potrdila zaposlen ali za katero opravlja delo, jamči za identiteto bodočega imetnika potrdila, ki jo je preverila v skladu z 31. členom in drugimi določili ZEPEP. Institucija je dolžna sporočiti vsako spremembo podatkov, ki bi vplivala na veljavnost potrdil, ki jih uporabljajo zaposleni oziroma povezane osebe.

(2) Institucija javne uprave in bodoči imetnik izpolnita vlogo za izdajo potrdila (obr. SSDP, VSSDP, STSDP, VSTSDP).

4.1.8. Namen imenika javne uprave

(1) Vsa potrdila so za uporabnike podatkovno-komunikacijskega omrežja državnih organov objavljena v imeniku javne uprave, ki je v skrbništvu SIGOV-CA.

V tem imeniku je tudi register preklicanih potrdil.

(2) Dostop do imenika javne uprave je možen po protokolu LDAP. Potrdila so shranjena v polju "userCertificate" v vejah, ki so označene v poglavju »3. Razpoznavni podatki SIGOV-CA«.

4.2. Varnostne zahteve za imetnika potrdila oziroma njegovo institucijo

(1) Imetnik oziroma bodoči imetnik potrdila je dolžan:

- skrbno prebrati to politiko pred podpisom vloge za potrdilo ter spremljati vsa obvestila SIGOV-CA in ravnati v skladu z njimi in to politiko,
- spremljati razvoj tehnologije oziroma obvestila SIGOV-CA in ustrezno posodabljati potrebno strojno in programsko opremo za varno delo s potrdili,
- uporabljati tako programsko opremo, ki je v skladu z obvestili SIGOV-CA (z dovolj močnimi kriptografskimi moduli),
- zasebni ključ in vse druge zaupne podatke ščititi s primernim geslom ali na drug način tako, da ima dostop do njih samo imetnik,
- na začetku narediti varnostno kopijo svojega ključa, če programska oprema to omogoča, in jo shraniti na varnem mestu,
- vse spremembe, ki so povezane s potrdilom, nemudoma sporočiti SIGOV-CA,
- zahtevati preklic potrdila, če je bil zasebni ključ ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

(2) Institucija javne uprave, v kateri je zaposlen ali je z njo povezan imetnik potrdila, je dolžna zagotoviti, da imetnik izpolnjuje vse zahteve iz te politike in veljavnih predpisov. Institucija je tudi dolžna:

- redno spremljati to politiko ter vsa obvestila SIGOV-CA,
- spremljati razvoj tehnologije oziroma obvestila SIGOV-CA in ustrezno posodabljati potrebno strojno in programsko opremo za varno delo s potrdili,
- uporabljati tako programsko opremo, ki je v skladu z obvestili SIGOV-CA (z dovolj močnimi kriptografskimi moduli),
- vse spremembe, ki so povezane s potrdilom imetnika, nemudoma sporočiti SIGOV-CA,
- zahtevati preklic potrdila, če je bil zasebni ključ imetnika potrdila ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

(3) Stroške potrebne strojne ali programske opreme, ki jo predlaga SIGOV-CA za varno shranjevanje in uporabo potrebnih podatkov za potrdilo na strani imetnika potrdila, krije imetnik potrdila ali njegova institucija.

4.3. Varnostne zahteve za tretje osebe

(1) Ob prvi uporabi potrdil SIGOV-CA po tej politiki mora tretja oseba skrbno prebrati to politiko in vsa obvestila SIGOV-CA.

(2) Tretja oseba mora vedno v času uporabe potrdila natančno preveriti, če potrdilo ni v registru preklicanih potrdil.

(3) Če potrdilo vsebuje podatke o tretji osebi, je ta dolžna zahtevati preklic potrdila, če izve, da je bil zasebni ključ ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

4.4. Osnovne lastnosti potrdila

(1) SIGOV-CA izdaja dve vrsti potrdil:

- potrdilo za uslužbence v javni upravi in povezane osebe, ki se izdaja na osnovi pravilno izpolnjene in podpisane vloge na ustreznem obrazcu (obr. SSDP, VSSDP),
- potrdilo za strežnik je namenjeno institucijam javne uprave za strežnike, ki se izdaja na osnovi pravilno izpolnjene in podpisane vloge na ustreznem obrazcu (obr. STSDP, VSTSDP).

(2) Vsak imetnik potrdila ima en par ključev, ki ga sestavlja zasebni in javni ključ. Par ključev se tvori z imetnikovo programsko opremo. Zasebni ključ ima samo imetnik. Javni ključ imetnika pa se pošlje overitelju v postopku izdaje potrdila. Javni ključ je objavljen kot sestavni del potrdila.

(3) SIGOV-CA hrani podatke o imetnikih potrdil. SIGOV-CA nikoli ne hrani in tudi nima dostopa do zasebnega ključa imetnika.

(4) Veljavnost potrdil je največ pet (5) let od prevzema. Po preteku veljavnosti potrdila lahko imetnik zaprosi za novo potrdilo.

(5) Imetnik potrdila se zavezuje, da bo uporabljal svoj par ključev le v obdobju veljavnosti svojega potrdila.

(6) Podatki v potrdilu so:

a) za potrdilo za zaposlene v javni upravi in povezane osebe:

- identifikacijska oznaka,
- nedvoumno razločevalno ime potrdila (DN), ki vsebuje tudi ime in priimek imetnika potrdila in dodatno serijsko številko,
- elektronski naslov imetnika potrdila,
- številka politike, pod katero je bilo izdano potrdilo (CP_{OID}), in iz katere je razvidno tudi, da gre za kvalificirano potrdilo,
- začetek in konec veljavnosti potrdila,
- naziv in sedež SIGOV-CA,
- javni ključ, ki pripada paru ključev imetnika potrdila,
- identiteta registra preklicanih potrdil,
- podatki o uporabi potrdila,
- podatki o šifrirnih algoritmih.

b) za potrdilo za strežnike:

- identifikacijska oznaka,
- nedvoumno razločevalno ime potrdila (DN), ki vsebuje tudi ime strežnika, vpisano v DNS, in dodatno serijsko številko,
- elektronski naslov skrbnika strežnika,
- številka politike, pod katero je bilo izdano potrdilo (CP_{OID}), in iz katere je razvidno tudi, da gre za kvalificirano potrdilo,
- začetek in konec veljavnosti potrdila,
- naziv in sedež SIGOV-CA,
- javni ključ, ki pripada paru ključev strežnika,
- identiteta registra preklicanih potrdil,
- podatki o uporabi potrdila,

- podatki o šifrirnih algoritmih.

(7) Vsak imetnik potrdila ima lahko pod istimi naštetimi podatki le eno samo potrdilo. Imetnik potrdila je nedvoumno določen z razločevalnim imenom (DN) ter enoličnim naslovom elektronske pošte.

(8) SIGOV-CA ne posreduje drugih osebnih podatkov o imetnikih potrdil, ki niso navedeni v potrdilu, razen če se določeni podatki posebej zahtevajo za izvajanje specifičnih funkcij oz. aplikacij, povezanih s potrdili, ter je to na vlogi za izdajo potrdila ali kasneje v pisni obliki odobril imetnik potrdila, ali na zahtevo pristojnega sodišča, sodnika za prekrške ali upravnega organa.

5. UPRAVLJANJE POTRDIL

5.1. Vloga za potrdilo

(1) Potrdilo se izda na osnovi pravilno izpolnjene in podpisane vloge na ustreznem obrazcu:
- obrazec SSDP za vlogo za potrdilo izpolnita zaposleni v javni upravi ali z njo povezana oseba in predstojnik institucije,
- obrazec STSDP za vlogo za potrdilo za strežnik izpolnita zaposleni v javni upravi ali z njo povezana oseba, ki je skrbnik strežnika in predstojnik institucije,
- obrazec VSSDP za vlogo za potrdilo izpolnita zaposleni v javni upravi ali z njo povezana oseba in predstojnik institucije, če bodoči imetnik že ima istovrstno potrdilo SIGOV-CA,
- obrazec VSTSDP za vlogo za potrdilo za strežnik izpolnita zaposleni v javni upravi ali z njo povezana oseba, ki je skrbnik strežnika in predstojnik institucije, če institucija za strežnik že ima istovrstno potrdilo SIGOV-CA.

(2) Izdajo potrdila odobri direktor CVI. Vloge za potrdila so dostopne preko pooblaščenih oseb SIGOV-CA ali preko spletnih strani SIGOV-CA.

(3) Potrdila se izdajajo izključno na infrastrukturi in s strani SIGOV-CA. Institucije vse vloge na varen in zanesljiv način posredujejo na SIGOV-CA.

5.2. Izdaja potrdila

(1) Ob odobritvi vloge za potrdilo SIGOV-CA po elektronski pošti obvesti bodočega imetnika o odobritvi ali zavrnitvi vloge. Če je vloga odobrena, SIGOV-CA opravi rezervacijo potrdila. Bodoči imetnik potrdila prejme:
- referenčno številko in avtorizacijsko kodo za prevzem potrdila,
- navodila za tvorjenje zahtevka za potrdilo in prevzem potrdila,
- dokumentacijo, ki vključuje to politiko ter navodila in pojasnila v skladu z veljavnimi predpisi in s katerimi je bil bodoči imetnik seznanjen že pred podpisom vloge za izdajo potrdila.

(2) SIGOV-CA preda bodočemu imetniku potrdila referenčno številko in avtorizacijsko kodo osebno v zaprti kuverti ali pa jo posreduje po dveh ločenih poteh: referenčno številko po elektronski pošti, avtorizacijsko kodo pa po priporočeni pošti v zaprti kuverti. Po prevzemu potrdila postaneta referenčna številka in avtorizacijska koda neuporabni za prevzem drugega potrdila.

(3) Bodoči imetnik potrdila mora po prejemu obvestila o izdanem potrdilu, referenčne številke in avtorizacijske kode potrdilo prevzeti v tridesetih (30) dneh od izdaje, sicer SIGOV-CA rezervacijo za potrdilo prekliče.

(4) Imetnik potrdila mora ob prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti SIGOV-CA oziroma zahtevati preklic.

5.3. Preklic potrdila

(1) SIGOV-CA prekliče potrdilo na zahtevo imetnika ali predstojnika institucije, v določenih primerih pa tudi na zahtevo tretje osebe.

(2) Preklic potrdila morata imetnik ali predstojnik institucije 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,
- nadomestitve potrdila z drugim potrdilom, (npr. ob izgubi datoteke z imetnikovim zasebnim ključem, izgubi gesla za dostop do zasebnega ključa in podobno),
- če so se spremenili podatki, ki so navedeni v potrdilu, ali če imetnik ni več zaposlen v instituciji ali je prenehal z delom za institucijo.

(3) Če potrdilo vsebuje podatke o tretji osebi, je ta dolžna zahtevati preklic potrdila, če izve, da je bil zasebni ključ imetnika potrdila ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

(4) SIGOV-CA prekliče potrdilo tudi brez zahteve imetnika ali predstojnika institucije, takoj ko izve:
- da je imetnik potrdila prenehal delati v ali za institucijo javne uprave ali da so se spremenile okoliščine, ki vplivajo na veljavnost potrdila,
- da je podatek v potrdilu napačen ali je bilo potrdilo izdano na podlagi napačnih podatkov,
- da je bila infrastruktura SIGOV-CA 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 SIGOV-CA prenehala z delovanjem ali ji je delovanje prepovedano in njene dejavnosti ni prevzel drug overitelj,
- da je preklic odredilo pristojno sodišče, sodnik za prekrške ali upravni organ.

(5) SIGOV-CA v primerih iz prejšnjega odstavka prekliče potrdilo brez predhodnega obvestila imetniku potrdila. Imetnika potrdila in predstojnika njegove institucije naknadno obvesti o datumu ter času preklica, izdajatelju zahtevka za preklic ter vzrokih za preklic.

(6) Preklic lahko imetnik zahteva osebno v rednem delovnem času, elektronsko in telefonsko pa 24 ur na dan vse dni v letu.

(7) Preklic lahko predstojnik zahteva osebno v rednem delovnem času, elektronsko pa 24 ur na dan vse dni v letu.

(8) Če se preklic opravi osebno, je potrebno izpolniti vlogo za preklic potrdila (obr. P-SSDP, P-STSDP) ter jo v rednem delovnem času osebno predati na SIGOV-CA.

(9) Če se preklic opravi elektronsko, morata imetnik ali predstojnik na SIGOV-CA poslati vlogo za preklic (obr. P-SSDP, P-STSDP), ki mora biti elektronsko podpisana z veljavnim potrdilom. Ob poslanem zahtevku za preklic mora izdajatelj zahtevka za preklic hkrati tudi telefonsko obvestiti SIGOV-CA na dežurno telefonsko številko za preklice.

(10) Če se preklic zahteva s strani imetnika digitalnega potrdila samo telefonsko na dežurno telefonsko številko za preklice, mora imetnik ob tem navesti geslo, ki ga je v ustrezni vlogi za izdajo potrdila imetnik podal kot geslo za preklic potrdila.

(11) SIGOV-CA bo po prejemu veljavne zahteve za preklic najkasneje v štirih (4) urah preklicala potrdilo. V tem času bo preklicano potrdilo v imeniku javne uprave dodano v register preklicanih potrdil.

(12) Register preklicanih potrdil se osvežuje:
- po vsakem preklicu potrdila,
- enkrat dnevno, če ni novih zapisov oz. sprememb v registru preklicanih potrdil (24 ur po zadnjem osveževanju).

(13) Register preklicanih potrdil vsebuje:
- identifikacijsko oznako preklicanega potrdila in
- čas in datum preklica.

5.4. Morebitno prenehanje delovanja SIGOV-CA

Če bo SIGOV-CA prenehala z opravljanjem svoje dejavnosti, bo ukrepala v skladu z ZEPEP.

6. ODGOVORNOST SIGOV-CA

(1) SIGOV-CA je odgovorna:
- za izdajanje potrdil in upravljanje z njimi v skladu s svojimi notranjimi pravili in veljavnimi predpisi,
- za varno hranjenje vseh osebnih in zaupnih podatkov o SIGOV-CA, imetnikih potrdil in njihovih institucijah,
- za točnost podatkov v potrdilu od trenutka izdaje do preklica ali prenehanja veljavnosti potrdila,

- da potrdilo vsebuje vse predpisane podatke za potrdilo po tej politiki in veljavnih predpisih,
- da je imel imetnik potrdila v času izdaje le-tega zasebni ključ ustrezen v potrdilu navedenemu javnemu ključu,
- za takojšen preklic potrdila in objavo preklica v registru preklicanih potrdil, če za preklic obstajajo razlogi po tej politiki ali veljavnih predpisih,
- za izpolnjevanje drugih zahtev te politike, svoje interne politike in veljavnih predpisov.

(2) SIGOV-CA je dolžna:
- upoštevati odločitve Komisije za pritožbe SIGOV-CA,
- objavljati na svojih spletnih straneh vse informacije o tistih spremembah glede dejavnosti SIGOV-CA, ki kakorkoli vplivajo na imetnike potrdil in tretje osebe.

(3) SIGOV-CA ni odgovorna za posledice, do katerih bi prišlo zaradi:
- uporabe potrdil za namene, ki niso izrecno predvideni v tej politiki,
- nepravilnega ali pomanjkljivega varovanja gesel ali zasebnega ključa, izdajanje zaupnih podatkov ali ključa tretjim osebam in podobnega ravnanja imetnika,
- kakršnekoli zlorabe oziroma vdora v informacijski sistem imetnika potrdila in s tem do podatkov s strani nepooblaščene osebe,
- nedelovanja ali slabega delovanja informacijske infrastrukture imetnika potrdila ali tretjih oseb,
- nepreverjanja podatkov in veljavnosti potrdil v registru preklicanih potrdil,
- uporabe potrdil na nestandardni način ali na opremi z okrnjenimi kriptografskimi moduli,
- drugega ravnanja imetnika potrdila, njegove institucije ali tretje osebe v nasprotju z obvestili SIGOV-CA, to politiko in veljavnimi predpisi.

(4) SIGOV-CA ni v nobenem primeru odgovo
rna za vsebino podatkov, ki se šifrirajo ali podpisujejo z uporabo njenih potrdil, ali za ravnanje imetnikov pri uporabi potrdil in sicer tudi v primeru, če je imetnik ali tretja oseba spoštoval vsa določila te politike, obvestil SIGOV-CA ter veljavnih predpisov.

(5) Infrastruktura SIGOV-CA ustreza najvišjim stopnjam varovanja in zaščite potrdil in ključev, vendar je varnost potrdil zagotovljena samo, če imetniki in tretje osebe, ki se zanašajo na potrdila, upoštevajo in ravnajo v skladu z obvestili SIGOV-CA.

7. KONČNE DOLOČBE

(1) Ob morebitnem sporu med SIGOV-CA na eni strani in imetnikom potrdila, njegovo institucijo ali tretjo osebo na drugi strani, se bo druga stran najprej pritožila Komisiji za pritožbe SIGOV-CA.

(2) Če postopek pred Komisijo za pritožbe SIGOV-CA ne reši spora, je zanj pristojno sodišče v Ljubljani po pravu Republike Slovenije.

(3) Določbe glede avtorske, sorodnih in drugih pravic intelektualne lastnine:
- na zasebnem in javnem ključu pripadajo vse pravice imetniku potrdila,

- na vseh ostalih podatkih v potrdilu vse pravice pripadajo SIGOV-CA.

8. TERMINOLOŠKI SLOVAR IN OZNAKE

CP_{Name}	Ime politike delovanja overitelja (*Angl.:Certification Policy Name*), enolično povezano z mednarodno številko politike delovanja CP_{OID} (*Angl.:Certification Policy Object Identifier*).
CP_{OID}	Mednarodna številka, ki enolično določa politiko delovanja (*Angl.:Certification Policy Object IDentifier*).
CRL	Seznam preklicanih potrdil (prim. definicijo Register preklicanih potrdil). *Angl.: CRL, Certification Revocation List*.
CVI	Center Vlade za informatiko.
DN	Enolično razločevalno ime (prim. definicijo Razločevalno ime). *Angl.: Distinguished Name.*
DNS	Baza imen računalnikov, ki so vključeni v internet. Omogoča povezave imen računalnikov z njihovimi številkami IP. *Angl.: Domain Name System*.
Dodatna serijska številka	Enolično 13-mestno število, ki ga potrdilu podeli SIGOV-CA. Prvih 8 mest številke je enolično število uporabnika, 9. in 10. mesto določata vrsto potrdila, naslednji dve mesti predstavljata zaporedno številko potrdila, zadnje mesto je kontrola zapisa po mod. 11.
Imenik javne uprave	Imenik javne uprave na CVI po standardu X.500, kjer so shranjena potrdila po standardu X.509 ver. 3, do katerih je znotraj podatkovno- komunikacijskega omrežja državnih organov možen dostop po protokolu LDAP.
Imetnik potrdila	Imetnik potrdila je oseba, ki je navedena v potrdilu overitelja in ki razpolaga s svojim zasebnim ključem.
Institucija	Institucije javne uprave, kjer je imetnik potrdila zaposlen ali za katerega opravlja delo.
Infrastruktura SIGOV-CA	Infrastruktura SIGOV-CA so vsi prostori overitelja, njegova strojna in programska oprema ter varnostni mehanizmi, ki so potrebni za varno delovanje SIGOV-CA.
LDAP	Leightweight Directory Access Protocol je protokol, ki določa dostop do imenika in je specificiran po IETF (Internet Engineering Task Force) priporočilu RFC 1777.
OID	Mednarodna številka, ki enolično določa politiko delovanja. *Angl.:Certification Policy Object IDentifier*.

Overitelj	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi. *Angl.:Certification Authority (CA*).
Potrdilo	Potrdilo v elektronski obliki, ki povezuje podatke iz potrdila z zasebnim ključem določene osebe ter potrjuje njeno identiteto. *Angl.: Digital certificate*. Za potrebe te politike je potrdilo službeno spletno kvalificirano potrdilo.
Prijavna služba	Služba ali oseba za sprejem vlog za potrdila in preverjanje istovetnosti bodočih imetnikov. *Angl.: Registration Authority (RA)*.
Razločevalno ime	Enolično ime (prim. definicijo DN) v potrdilu, ki nedvoumno in enolično definira uporabnika v strukturi imenika javne uprave. *Primer* *cn*=ime priimek%serijska številka, *OU=government, OU=web-certificates, O=state-institutions, C=si*
Register preklicanih potrdil	Seznam preklicanih potrdil. *Angl.: CRL, Certification Revocation List*. Osvežuje se enkrat dnevno oz. z vsakim preklicem potrdila.
SIGOV-CA	Overitelj potrdil na Centru Vlade za informatiko (CVI). SI - *Angl.: Slovenian*, GOV - *Angl.:* Governmental, CA - Overitelj (prim. definicijo Overitelj).
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 57/2000)