CENTER VLADE REPUBLIKE SLOVENIJE
ZA INFORMATIKO

POLITIKA SIGEN-CA

za kvalificirana digitalna potrdila za pravne in fizične osebe, registrirane za opravljanje dejavnosti

Javni del notranjih pravil overitelja na Centru Vlade Republike Slovenije za informatiko

Politika je veljavna od 15. julija 2002

CP_{Name}: SIGEN-CA-1
CP_{OID}: 1.3.6.1.4.1.6105.2.1.2

Izdaje politik delovanja SIGEN-CA za prave in fizične osebe, registrirane za opravljanje dejavnosti
Verzija 2
Politika SIGEN-CA za kvalificirana digitalna potrdila za pravne in fizične osebe, registrirane za opravljanje dejavnosti CP_{OID}: 1.3.6.1.4.1.6105.2.1.2 CP_{Name}: SIGEN-CA-1 pričetek veljavnosti: 15. julij 2002
Verzija 1
Politika SIGEN-CA za kvalificirana digitalna potrdila za pravne in fizične osebe, registrirane za opravljanje dejavnosti CP_{OID}:1.3.6.1.4.1.6105.2.1.1 CP_{Name}: SIGEN-CA-1 pričetek veljavnosti: 15. oktober 2001

VSEBINA

1. UVOD 5

2. SPLOŠNE DOLOČBE 6

2.1. Zavarovanje odgovornosti overitelja na CVI 7

2.2. Zahteve za podrejene overitelje 8

2.3. Lastnosti medsebojnega priznavanja 8

3. RAZPOZNAVNI PODATKI SIGEN-CA 8

3.1. Identiteta overitelja na CVI 8

3.2. Identiteta izdajatelja SIGEN-CA 8

3.3. Identiteta potrdil oz. javnega imenik potrdil 9

3.4. Identiteta registra preklicanih potrdil 9

4. INFRASTRUKTURA OVERITELJA NA CVI 10

4.1. Osnovne lastnosti overitelja na CVI 10
4.1.1. Varnost in zanesljivost infrastrukture overitelja na CVI 10
4.1.2. Šifrirni algoritmi, formati podatkov in protokoli infrastrukture overitelja na CVI 10
4.1.3. Osebje overitelja na CVI 11
4.1.4. Vloga in pomen prijavnih služb SIGEN-CA 11
4.1.5. Javni imenik potrdil 12
4.1.6. Register preklicanih potrdil 12

4.2. Osnovne lastnosti potrdil 12
4.2.1. Lastnosti osebnega potrdila 14
4.2.2. Lastnosti spletnega potrdila 15
4.2.3. Lastnosti razločevalnega imena 15
4.2.4. Zahteve za elektronski naslov 17

5. UPRAVLJANJE POTRDIL 17

5.1. Pridobitev potrdila 17

5.2. Preklic potrdila 18

5.3. Podaljševanje veljavnosti potrdil - velja za osebna potrdila 19

5.4. Regeneriranje ključev - velja za osebna potrdila 19

5.5. Odkrivanje kopije ključev za dešifriranje - velja za osebna potrdila 19

5.6. Morebitno prenehanje delovanja overitelja na CVI oz. izdajatelja SIGEN-CA 19

6. OBVEZNOSTI IN ODGOVORNOST 20

6.1. Obveznosti in odgovornost imetnika potrdila oziroma organizacije 20

6.2. Obveznosti in odgovornost overitelja na CVI 21

6.3. Zahteve za tretje osebe 22

7. KONČNE DOLOČBE 22

8. TERMINOLOŠKI SLOVAR IN OZNAKE 23

POVZETEK

Overitelj na Centru Vlade RS za informatiko (CVI) 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), evropskimi direktivami ter drugimi veljavnimi predpisi. Politika delovanja overitelja na CVI določa namen, delovanje in metodologijo upravljanja s kvalificiranimi digitalnimi potrdili, odgovornost overitelja na CVI ter zahteve, ki jih morajo izpolnjevati imetniki, tretje osebe, ki se zanašajo na kvalificirana digitalna potrdila, in drugi overitelji.

Overitelja na CVI (http://www.gov.si/ca*)* predstavljata dva izdajatelja kvalificiranih digitalnih potrdil:

- SIGEN-CA (angl. *Slovenian General Certification Authority*) za državljane in pravne osebe (http://www.sigen-ca.si),
- SIGOV-CA (angl. *Slovenian Governmental Certification Authority*) za upravo Republike Slovenije (http://www.sigov-ca.gov.si).

Oba izdajatelja sta mednarodno registrirana, medsebojno priznana ter tehnološko in zakonsko enako veljavna.

Kvalificirana digitalna potrdila, ki jih izdaja overitelj na CVI, so namenjena:

- za upravljanje, dostop in izmenjavo podatkov, s katerimi upravlja javna uprava,
- za varno elektronsko komuniciranje med imetniki kvalificiranih digitalnih potrdil overitelja na CVI in
- za storitve oz. aplikacije, za katere se zahteva uporaba digitalnih potrdil overitelja na CVI.

Pričujoča politika določa pravila izdajatelja SIGEN-CA. Na podlagi te politike SIGEN-CA izdaja osebna in spletna kvalificirana digitalna potrdila za pravne in fizične osebe, registrirane za opravljanje dejavnosti (CP_{OID}= 1.3.6.1.4.1.6105.2.1.2), ki izpolnjujejo najvišje varnostne zahteve. Pričujoča politika nadomešča prvo verzijo politiko delovanja SIGEN-CA za pravne in fizične osebe, registrirane za opravljanje dejavnosti (CP_{OID}= 1.3.6.1.4.1.6105.2.1.1), ki ostaja v veljavi za potrdila izdana pred veljavo pričujoče politike. Vsa kvalificirana digitalna potrdila izdana oz. podaljšana po datumu veljavnosti te politiki se obravnavajo po novi politiki.

Na podlagi pričujoče politiki lahko pravne in fizične osebe, registrirane za opravljanje dejavnosti poleg kvalificiranih digitalnih potrdil za svoje zaposlene pridobijo tudi potrdila za splošne nazive oz. organizacijske enote in strežnike. Vsa potrdila se pridobijo na podlagi veljavne pogodbe med pravno in fizično osebo, registrirano za opravljanje dejavnosti, in overiteljem na CVI in zahtevka, ki ga mora podpisati odgovorna oseba pravne in fizične osebe, registrirane za opravljanje dejavnosti, in bodoči imetnik. Odgovorna oseba s podpisom zahtevka jamči za istovetnost bodočih imetnikov. Izpolnjen zahtevek se osebno odda na prijavni službi (naslovi, uradne ure in vse druge informacije so objavljene na spletnih straneh http://www.sigen-ca.si/prijavne-slu.htm).

SIGEN-CA na podlagi odobrenega zahtevka pripravi referenčno številko in avtorizacijsko kodo, ki sta unikatni za vsakega bodočega imetnika digitalnega potrdila posebej in ju bodoči imetnik potrebuje za prevzem svojega digitalnega potrdila. Bodoči imetnik prejme referenčno številko po elektronski pošti, avtorizacijsko kodo pa po priporočeni pošti na službeni naslov. S pomočjo obeh kod bodoči imetnik opravi prevzem svojega digitalnega potrdila na svoji delovni postaji v skladu z navodili SIGEN-CA.

Imetnik mora skrbno varovati zasebne ključe in potrdilo ter ravnati v skladu s politiko in obvestili izdajatelja SIGEN-CA.

1. UVOD

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

(2) Overitelj na CVI 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), evropskimi direktivami ter drugimi veljavnimi predpisi.

(3) Kvalificirana digitalna potrdila, ki jih izdaja overitelj na CVI, so namenjena:
- za upravljanje s podatki javne uprave,
- za dostop in izmenjavo podatkov, s katerimi upravlja javna uprava,
- za varno elektronsko komuniciranje med imetniki kvalificiranih digitalnih potrdil overitelja na CVI in
- za storitve oz. aplikacije, za katere se zahteva uporaba digitalnih potrdil overitelja na CVI.

(4) Overitelja na CVI predstavljata dva izdajatelja kvalificiranih digitalnih potrdil:
- SIGOV-CA (angl. *Slovenian Governmental Certification Authority*) je izdajatelj kvalificiranih digitalnih potrdil overitelja na CVI za institucije javne uprave,
- SIGEN-CA (angl. *Slovenian General Certification Authority*) je izdajatelj kvalificiranih digitalnih potrdil overitelja na CVI za pravne in fizične osebe.

(5) Izdajatelja SIGOV-CA in SIGEN-CA sta mednarodno registrirana, medsebojno priznana, ter tehnološko in zakonsko enakovredna in enako veljavna.

(6) SIGOV-CA izdaja kvalificirana digitalna potrdila za institucije javne uprave:
- osebna kvalificirana digitalna potrdila za zaposlene v institucijah,
- osebna kvalificirana digitalna potrdila za splošne nazive oz. organizacijske enote institucij,
- spletna kvalificirana digitalna potrdila za zaposlene v institucijah,
- spletna kvalificirana digitalna potrdila za splošne nazive institucij oz. organizacijske enote institucij,
- osebna kvalificirana digitalna potrdila za strežnike, s katerimi upravljajo institucije,
- spletna kvalificirana digitalna potrdila za strežnike, s katerimi upravljajo institucije.

SIGEN-CA izdaja kvalificirana digitalna potrdila za pravne in fizične osebe:
- osebna kvalificirana digitalna potrdila za zaposlene pravnih in fizičnih oseb, registriranih za opravljanje dejavnosti,
- osebna kvalificirana digitalna potrdila za splošne nazive oz. organizacijske enote pravnih in fizičnih oseb, registriranih za opravljanje dejavnosti,
- spletna kvalificirana digitalna potrdila za zaposlene pravnih in fizičnih oseb, registriranih za opravljanje dejavnosti,
- spletna kvalificirana digitalna potrdila za splošne nazive oz. organizacijske enote pravnih in fizičnih oseb, registriranih za opravljanje dejavnosti,
- osebna kvalificirana digitalna potrdila za strežnike, s katerimi upravljajo pravne in fizične osebe, registrirane za opravljanje dejavnosti,
- spletna kvalificirana digitalna potrdila za strežnike, s katerimi upravljajo pravne in fizične osebe, registrirane za opravljanje dejavnosti,

- spletna kvalificirana digitalna potrdila za fizične osebe.

(7) Osebna kvalificirana digitalna potrdila se lahko uporabljajo za:
- šifriranje in dešifriranje podatkov v elektronski obliki,
- digitalno podpisovanje podatkov v elektronski obliki ter izkazovanje istovetnosti imetnika,
- varno brisanje podatkov v elektronski obliki,
- storitve oz. aplikacije, za katere se zahteva uporaba osebnih kvalificiranih digitalnih potrdil overitelja na CVI.

(8) Spletna kvalificirana digitalna potrdila se lahko uporabljajo za:
- šifriranje in dešifriranje podatkov v elektronski obliki,
- digitalno podpisovanje podatkov v elektronski obliki ter izkazovanje istovetnosti imetnika,
- storitve oz. aplikacije, za katere se zahteva uporaba spletnih kvalificiranih digitalnih potrdil overitelja na CVI.

(9) Javni del notranjih pravil overitelja na CVI je določen z naslednjimi politikami:
- Politika SIGOV-CA za kvalificirana digitalna potrdila za institucije javne uprave,
- Politika SIGEN-CA za kvalificirana digitalna potrdila za pravne in fizične osebe, registrirane za opravljanje dejavnosti,
- Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe.

(10) V primeru kvalificiranih digitalnih potrdil za institucije javne uprave ter za pravne in fizične osebe, registrirane za opravljanje dejavnosti, ima glede preklica kvalificiranih digitalnih potrdil predstojnik institucije javne uprave oz. odgovorna oseba pravne in fizične osebe, registrirane za opravljanje dejavnosti, enake pravice kot ostali imetniki kvalificiranih digitalnih potrdil iz iste institucije oz. pravne in fizične osebe, registrirane za opravljanje dejavnosti.

(11) Overitelj na CVI 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 oz. podaljšanju potrdil. Nova verzija oz. spremembe politike overitelja na CVI se sedem (7) dni pred veljavo predhodno objavi na spletnih straneh overitelja na CVI pod novo identifikacijsko številko (CP_{OID}) in označenim datumom začetka njene veljavnosti. Vsa kvalificirana digitalna potrdila izdana oz. podaljšana po tem datumu se obravnavajo po novi politiki.

(12) Overitelj na CVI se lahko povezuje v mrežo overiteljev na horizontalni ali vertikalni ravni, to je ustanavlja oz. overja podrejene ali priznava enakovredne overitelje ter se povezuje v hierarhično globalno strukturo overiteljev.

(13) Overitelj na CVI 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 definira delovanje overitelja na CVI za kvalificirana digitalna potrdila SIGEN-CA (CP_{OID} = 1.3.6.1.4.1.6105.2.1.2) za:
- pravne in fizične osebe, registrirane za opravljanje dejavnosti pri pristojnem organu Republike Slovenije oziroma tuje osebe, ki opravljajo dejavnost in lahko svojo istovetnost dokažejo v skladu z veljavnimi predpisi in
- druge overitelje potrdil.

(2) Posamezni izrazi imajo v nadaljevanju te politike naslednji pomen:
- **SIGEN-CA** je izdajatelj kvalificiranih digitalnih potrdil overitelja na CVI za pravne in fizične osebe,

- **organizacija** je pravna ali fizična oseba, ki je registrirana za opravljanje dejavnosti v skladu z veljavnimi predpisi v Republiki Sloveniji ali tuja oseba, ki opravlja dejavnost in lahko svojo istovetnost dokaže v skladu z veljavnimi predpisi,
- **odgovorna oseba** je fizična oseba, ki je pooblaščena za zastopanje organizacije v pravnem prometu,
- **potrdilo** je osebno ali spletno kvalificirano digitalno potrdilo (angl. *qualified digital certificate*),
- **osebno potrdilo** je osebno kvalificirano digitalno potrdilo v elektronski obliki (osebno potrdilo sestavlja potrdilo za overjanje podpisa in potrdilo za šifriranje), ki povezuje podatke iz potrdila z imetnikovima zasebnima ključema ter potrjuje imetnikovo identiteto (angl. *enterprise certificate*),
- **spletno potrdilo** je spletno kvalificirano digitalno potrdilo v elektronski obliki, ki povezuje podatke iz potrdila z imetnikovim zasebnim ključem ter potrjuje imetnikovo identiteto (angl. *web certificate*),
- **zaposleni** so fizične osebe, ki so v delovnem razmerju z organizacijo ali pa na drugačni pravni podlagi delajo za organizacijo in za katere želi odgovorna oseba le-te pridobiti potrdila, ki jih te osebe potrebujejo za opravljanje dela za to organizacijo,
- **zahtevki** so obrazci SIGEN-CA za pridobivanje in preklic potrdil, regeneracijo ključev osebnega potrdila, odkrivanje kopije zasebnega ključa za dešifriranje osebnega potrdila, ki so dostopni preko spletnih strani SIGEN-CA oz. pri pooblaščenih osebah na prijavnih službah,
- **prijavna služba** po pooblastilu overitelja na CVI sprejema zahtevke za pridobitev in preklic potrdil ter regeneracijo ključev osebnih potrdil in preverja istovetnosti bodočih imetnikov oz. podatkov o organizacijah,
- **pridobitev potrdila** je postopek, ki vključuje oddajo zahtevka za pridobitev na prijavno službo, preverjanje istovetnosti, odobritev zahtevka za pridobitev, rezervacijo potrdila z izdajo kod za prevzem potrdila in postopek prevzema oz. izdaje potrdila,
- **prevzem oz. izdaja potrdila** je postopek generiranja ključev in izdaja potrdila, ki vključuje imetnikov javni ključ in ostale podatke,
- **objava SIGEN-CA** je javna objava na spletnih straneh SIGEN-CA,
- **obvestila SIGEN-CA** so vsa navodila, pojasnila, seznami, pogoji, posamezna obvestila, priporočila, standardi in drugi dokumenti, ki jih določi ali priporoči SIGEN-CA in jih objavi ali kako drugače posreduje imetnikom potrdil, njihovim organizacijam ali tretjim osebam.

(3) Ta politika določa upravljanje (rezervacijo, izdajanje in overjanje, preklicevanje, regeneriranje ključev, odkrivanje kopije zasebnega ključa za dešifriranje, hranjenje in objavljanje) potrdil za imetnike potrdil, ki so lahko:
- zaposleni,
- zaposleni, pooblaščeni za uporabo splošnih nazivov oz. organizacijskih enot organizacij,
- zaposleni, pooblaščeni za uporabo strežnikov (storitev oz. aplikacij), s katerim upravljajo organizacije,
- drugi overitelji potrdil.

(4) Odgovorna oseba s podpisom zahtevka za pridobitev potrdila jamči za podatke o organizaciji in istovetnosti bodočih imetnikov in jih pooblašča za uporabo potrdila v imenu opravljanja nalog za organizacijo.

(5) Medsebojna razmerja med organizacijo in overiteljem na CVI se izvaja tudi na podlagi pisne pogodbe.

(6) Za potrdila, izdana na podlagi te politike, SIGEN-CA priporoča uporabo sredstev za varno shranjevanje in uporabo potrdil.

(7) Stroške potrebne strojne ali programske opreme, ki jo zahteva oz. priporoča SIGEN-CA za varno shranjevanje in uporabo potrdil, krije imetnik potrdila oz. njegova organizacija.

(8) Stroški upravljanja s potrdili se obračunavajo organizaciji po objavljenem ceniku.

2.1. Zavarovanje odgovornosti overitelja na CVI

CVI ima glede delovanja overitelja na CVI ustrezno zavarovano svojo odgovornost po ZEPEP ter Uredbi o pogojih za elektronsko poslovanje in elektronsko podpisovanje.

2.2. Zahteve za podrejene overitelje

(1) Medsebojna razmerja med overiteljem na CVI in podrejenim overiteljem se izvaja na podlagi pisne pogodbe.

(2) Overitelj na CVI zagotavlja, da podrejeni overitelji izpolnjujejo ustrezno raven varnostnih zahtev. Overitelj na CVI redno pregleduje izpolnjevanje varnostnih zahtev in postopkov pri upravljanju s potrdili podrejenih overiteljev.

2.3. Lastnosti medsebojnega priznavanja

(1) Overitelj na CVI se lahko povezuje in priznava z domačimi in tujimi overitelji, vendar ni dolžan priznati drugih overiteljev tudi, če ima drugi overitelj status akreditiranega overitelja ali overitelja kvalificiranih digitalnih potrdil. Medsebojno priznavanje se izvaja na podlagi pisne pogodbe.

(2) Overitelj na CVI zagotavlja, da bo izvajal medsebojno priznavanje izključno po podpisu pisne pogodbe z drugimi overitelji, ki pa morajo izpolnjevati raven varnostnih zahtev, ki jih predpiše overitelj CVI. Pooblaščene osebe overitelja na CVI pregledujejo notranja pravila drugega overitelja ter njegovo izpolnjevanje varnostnih zahtev.

(3) Stroške potrebne infrastrukture, ki jo zahteva overitelj na CVI za medsebojno priznavanje, krije drugi overitelj.

3. RAZPOZNAVNI PODATKI SIGEN-CA

3.1. Identiteta overitelja na CVI

Naslov:	Center Vlade Republike Slovenije za informatiko Langusova 4 1000 Ljubljana Slovenija
Telefon:	(+386) 01 4788 600
Fax:	(+386) 01 4788 649
URL:	http://www.gov.si/ca

3.2. Identiteta izdajatelja SIGEN-CA

Enolično ime:	ou=SIGEN-CA, o=state-institutions, c=si
Naslov:	SIGEN-CA Center Vlade Republike Slovenije za informatiko Langusova 4 1000 Ljubljana Slovenija
E-pošta:	sigen-ca@gov.si
Telefon:	(+386) 01 4788 600
Fax:	(+386) 01 4788 649
URL:	http://www.sigen-ca.si

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

SIGEN-CA je ob začetku svojega produkcijskega delovanja generiral svoje lastno potrdilo, ki je namenjeno podpisovanju potrdil za druge imetnike oz. overitelje, podpisovanju registra preklicanih potrdil oz. preverjanju podpisa SIGEN-CA.

Potrdilo SIGEN-CA vsebuje naslednje podatke:

Identifikacijska oznaka:	3B3C F9C9
Overitelj potrdila:	SIGEN-CA
Imetnik potrdila:	SIGEN-CA
Veljavnost potrdila:	od 29. junija 2001 do 29. junija 2021
Dolžina ključa:	2048 bitov
Identiteta ključa (SHA1):	717B 8A06 1F31 0555 AB60 1277 4720 1E03 8818 EC89
Odtis potrdila (MD5):	49EF A6A1 F0DE 8EA7 6AEE 5B7D 1E5F C446
Odtis potrdila (SHA-1):	3E42 A187 06BD 0C9C CF59 4750 D2E4 D6AB 0048 FDC4

3.3. Identiteta potrdil oz. javnega imenik potrdil

(1) Potrdila so shranjena v strukturi javnega imenika na strežniku x500.gov.si (dostopna po protokolu LDAP).

c=si, o=state-institutions, ou= sigen-ca (v polju "userCertificate").

(2) Potrdila so dostopna tudi preko spletne strani SIGEN-CA po protokolu HTTPS:

https://www.sigen-ca.si/cda-cgi/clientcgi?action=directorySearch.

Opis javnega imenika in potrdil je tudi v pogl. 4.1.5 oz. 4.2.

3.4. Identiteta registra preklicanih potrdil

(1) Register preklicanih potrdil se nahaja v strukturi javnega imenika na strežniku x500.gov.si v veji (dostopen po protokolu LDAP):

c=si, o=state-institutions, ou=sigen-ca, cn=CRL*n*[1].

(2) Celotni register preklicanih potrdil (angl. *Combined RevocationList*) se nahaja v veji:

ou= sigen-ca, o=state-institutions, c=si (v polju "CertificationRevocationList").

Celotni register preklicanih potrdil je dostopen tudi po protokolu HTTP:

http://www.sigen-ca.si/crl/sigen-ca.crl.

Opis registra preklicanih potrdil je v pogl. 4.1.6.

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

4. INFRASTRUKTURA OVERITELJA NA CVI

4.1. Osnovne lastnosti overitelja na CVI

4.1.1. Varnost in zanesljivost infrastrukture overitelja na CVI

(1) Oprema overitelja na CVI 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 overitelja na CVI ustreza nivoju varovanja po standardu *FIPS 140-1 level 3*.

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

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

4.1.2. Šifrirni algoritmi, formati podatkov in protokoli infrastrukture overitelja na CVI

(1) Overitelj na CVI uporablja:
- za podpisovanje potrdil in registra preklicanih 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,
- registri preklicanih potrdil ustrezajo priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:1997, vključno z ver. 2,
- 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 SIGEN-CA poteka po protokolu SEP (angl. Secure Exchange Protocol), ki temelji na standardu GULS (angl. 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 overitelju na CVI.

4.1.3. Osebje overitelja na CVI

(1) Operativno, organizacijsko in strokovno pravilno delovanje overitelja na CVI vodi vodja Sektorja za upravljanje digitalnih potrdil na CVI in je organizacijsko direktno podrejen direktorju CVI.

(2) Med pooblaščene osebe overitelja na CVI spadajo člani overitelja na CVI, prijavne službe in nadzorne skupine, ki jo vodi vodja Službe za varovanje in zaščito na CVI.

(3) Člani overitelja na CVI so razporejeni v 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 delovanja overitelja na CVI - Določevanje prvega varnostnega inženirja - Operativno vodenje overitelja na CVI	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

(4) Navedeno število oseb predstavlja minimalno število. Vloge posameznih organizacijskih skupin so določene z Interno politiko overitelja na CVI.

4.1.4. Vloga in pomen prijavnih služb SIGEN-CA

(1) Naloge prijavnih služb so:
- preverjanje istovetnost imetnikov oz. bodočih imetnikov, podatkov o organizaciji in drugih potrebnih podatkov,
- sprejemanje zahtevkov za pridobitev potrdil,
- sprejemanje zahtevkov za preklic potrdil,
- sprejemanje zahtevkov za regeneracijo ključev osebnih potrdil,
- izdajanje potrebne dokumentacije imetnikom oz. bodočim imetnikom in organizacijam,
- posredovanje zahtevkov in ostalih podatkov na varen način na SIGEN-CA.

(2) Institucije, ki opravljajo naloge prijavnih služb, pooblasti overitelj na CVI. Izpolnjevati morajo pogoje za opravljanje nalog prijavnih služb overitelja na CVI in delovati v skladu z veljavnimi zakoni in predpisi.

(3) Organizacija oz. odgovorna oseba za svoje zaposlene osebe opravlja del nalog prijavnih služb po določilih SIGEN-CA, in sicer odgovorna oseba organizacije, kjer je bodoči imetnik potrdila zaposlen, jamči za istovetnost bodočega imetnika potrdila, ki jo je preverila v skladu z 31. členom in drugimi določili ZEPEP.

(4) Seznam prijavnih služb je objavljen na spletnih straneh SIGEN-CA.

4.1.5. Javni imenik potrdil

(1) Vsa potrdila so objavljena v javnem imeniku, ki je v skrbništvu overitelja na CVI (glej pogl. 3.3).

(2) Javni imenik je stalno dostopen:
- po protokolu LDAP in
- po protokolu HTTPS.

(3) V javnem imeniku je tudi register preklicanih potrdil.

4.1.6. Register preklicanih potrdil

(1) Register preklicanih potrdil je stalno dostopen v javnem imeniku potrdil (glej pogl. 3.4):
- po protokolu LDAP in
- po protokolu HTTP.

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

(3) Register preklicanih potrdil poleg ostalih podatkov v skladu s priporočili, navedenimi v pogl. 4.1.2, vsebuje:
- identifikacijske oznake preklicanih potrdil in
- čas in datum preklicev.

4.2. Osnovne lastnosti potrdil

(1) Na podlagi pričujoče politike SIGEN-CA izdaja naslednje vrste potrdil:
- osebna potrdila za zaposlene,
- spletna potrdila za zaposlene,
- osebna potrdila za splošne nazive organizacij oz. organizacijske enote,
- spletna potrdila za splošne nazive organizacij oz. organizacijske enote,
- osebna potrdila za strežnike,
- spletna potrdila za strežnike,
- spletna potrdila za podpis kode,
- potrdila za druge overitelje potrdil.

(2) Potrdilo se izda na osnovi odobrenega zahtevka za pridobitev in veljavne pogodbe (glej pogl. 5.1, podrobnejši potek izdaje glede na vrsto potrdila je podan v pogl. 4.2.1 in 4.2.2).

(3) SIGEN-CA poleg podatkov, ki so vključeni v potrdilo, hrani ostale potrebne podatke o imetniku in organizaciji za namen elektronskega poslovanja v skladu z veljavnimi predpisi.

(4) V potrdilu so navedeni podatki o imetniku in izdajatelju skladno s standardi iz pogl. 4.1.2. Osnovni podatki v potrdilu so navedeni spodaj, ostali podatki pa so vsebovani glede na vrsto potrdilo (glej pogl. od 4.2.1 do 4.2.3):

Podatek	Vrednost oz. pomen
Verzija X.509, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Numb*er	<enolična interna številka potrdila>
Algoritem za podpis potrdila, angl. *Signature Algorithm*	sha1WithRSAEncryption
Ime izdajatelja, angl. *Issuer*	c=si, o=state-institutions, ou=sigen-ca
Pričetek in konec veljavnosti potrdila, angl. *Validity*	Not Before: <pričetek veljavnosti po GMT> Not After: <konec veljavnosti po GMT>
Imetnik, angl. *Subject*	<razločevalno ime imetnika, ki vključuje naziv imetnika, serijsko številko potrdila in organizacijo, glej pogl. 4.2.3>
Alternativno ime, angl. *Subject Alternative Name*	<elektronski naslov imetnika oz. splošnega naziva oz. strežnika>
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, angl. *RSA Public Key (1024 bit)*	<javni ključ, šifriran z algoritmom RSA, dolžine 1024 bitov>
Identiteta imetnikovega ključa, angl. *Subject Key Identifier*	<odtis imetnikovega javnega ključa>
Politike, pod katero je bilo izdano potrdilo (OID), in iz katere je razvidno tudi, da gre za kvalificirano potrdilo, angl. *Certificate Policies*	Policy: 1.3.6.1.4.1.6105. 2.1.2 CPS: http://www.gov.si/ca/cps
Identiteta registra preklicanih potrdil, angl. *CRL Distribution Points*	c=si, o=state-institutions, ou=sigen-ca, cn=CRL<zaporedna številka registra (glej pogl. 3.4)> Url: ldap://x500.gov.si/ou=sigen-ca,o=state-institutions,c=si?certificateRevocationList?base Url: http://www.sigen-ca.si/crl/sigen-ca.crl
Podpis izdajatelja SIGEN-CA	<podpis potrdila s strani izdajatelja SIGEN-CA>
Identiteta ključa izdajtelja SIGEN-CA, angl. *Authority Key Identifier* (SHA1)	717B 8A06 1F31 0555 AB60 1277 4720 1E03 8818 EC89

(5) Pod istimi podatki o nazivu, podatki o organizaciji, elektronskim naslovom ima imetnik lahko eno samo veljavno istovrstno potrdilo.

(6) Imetnik potrdila je nedvoumno določen z razločevalnim imenom.

4.2.1. Lastnosti osebnega potrdila

(1) Vsak imetnik osebnega potrdila ima dva ločena para ključev - za digitalno podpisovanje/overjanje in za šifriranje/dešifriranje podatkov. Oba para imata en zasebni in en javni ključ.

Par ključev za digitalno podpisovanje/overjanje sestavlja:
- zasebni ključ za podpisovanje (v nadaljevanju *ključ za podpisovanje*) ter
- javni ključ za overjanje podpisa (v nadaljevanju *ključ za overjanje podpisa*).

Par ključev za šifriranje/dešifriranje sestavlja:
- zasebni ključ za dešifriranje (v nadaljevanju *ključ za dešifriranje*) ter
- javni ključ za šifriranje (v nadaljevanju *ključ za šifriranje*).

(2) Par ključev za podpisovanje/overjanje se tvori z imetnikovo programsko opremo. SIGEN-CA nikoli ne hrani in tudi nima dostopa do ključa za podpisovanje. Ključ za overjanje podpisa se pošlje SIGEN-CA, ki izda osebno potrdilo za verifikacijo podpisa, katerega sestavni del je ključ za overjanje podpisa. Osebno potrdilo za verifikacijo podpisa se shrani pri imetniku.

Par ključev za šifriranje/dešifriranje se tvori na strani overitelja. Ključ za dešifriranje hrani imetnik. Zaradi možnega dostopa (dešifriranja) do pomembnih zašifriranih podatkov, če ključ za dešifriranje iz kakršnihkoli vzrokov ni več dostopen, se ta ključ po posebnem režimu, ki je določen z Interno politiko overitelja na CVI, varno hrani tudi v arhivu SIGEN-CA. SIGEN-CA izda osebno potrdilo za šifriranje, katerega sestavni del je ključ za šifriranje. Osebno potrdilo za šifriranje se objavi v javnem imeniku potrdil.

(3) Veljavnost osebnega potrdila je največ tri (3) leta od prevzema. Podaljšanje veljavnih potrdil in generiranje novih parov ključev se izvaja avtomatsko pred iztekom roka, določenem za veljavnost potrdila.

Veljavnost ključa za overjanje digitalnega podpisa je največ pet (5) let od prevzema. Nov ključ za overjanje podpisa se generira avtomatsko pred iztekom roka, določenem za veljavnost potrdila.

(4) Poleg osnovnih podatkov iz pogl. 4.2 osebno potrdilo za šifriranje, objavljeno v javnem imeniku, vključuje še podatke, navedene v spodnji tabeli.

Podatek	Vrednost (osebno-za šifriranje)
Namen uporabe, angl. *Key Usage*	Key Encipherment
Pričetek in konec veljavnosti ključa za dešifriranje, angl. *Private Key Usage Period*	Not Before: <pričetek veljavnosti po GMT> Not After: <konec veljavnosti po GMT>

(5) Poleg podatkov iz pogl. 4.2 osebno potrdilo za verifikacijo podpisa, ki ga hrani imetnik, vključuje še podatke, navedene v spodnji tabeli.

Podatek	Vrednost (osebno – za verifikacijo podpisa)
Namen uporabe, angl. *Key Usage*	Digital Signature
Pričetek in konec veljavnosti ključa za podpisovanje, angl. *Private Key Usage Period*	Not Before: <pričetek veljavnosti po GMT> Not After: <konec veljavnosti po GMT>

(6) SIGEN-CA lahko izda tudi osebno potrdilo za strežnik. Tako potrdilo lahko vključuje tudi druge, tehnično

pogojene podatke.

4.2.2. Lastnosti spletnega potrdila

(1) Vsak imetnik spletnega 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. SIGEN-CA nikoli ne hrani in tudi nima dostopa do imetnikovega zasebnega ključa. Javni ključ se pošlje SIGEN-CA, ki izda in objavi spletno potrdilo z javnim ključem, kot sestavnim delom potrdila.

(2) Veljavnost spletnih potrdil je največ pet (5) let od prevzema.

(3) Poleg podatkov iz pogl. 4.2 vključuje spletno potrdilo še podatke, navedene v spodnji tabeli.

Podatek	Vrednost (spletno)	Vrednost (spletno-strežnik)
Namen uporabe, angl. *Key Usage*	Digital Signature, Key Encipherment	
Pričetek in konec veljavnosti zasebnega ključa, angl. *Private Key Usage Period*	Not Before: <pričetek veljavnosti po GMT> Not After: <konec veljavnosti po GMT>	
Vrsta potrdila, angl. *Netscape Cert Type*	SSLClient, S/MIME	SSL Server

(4) SIGEN-CA lahko izda tudi spletno potrdilo za podpis kode. Tako potrdilo vključuje tudi druge, tehnično pogojene podatke.

4.2.3. Lastnosti razločevalnega imena

(1) Razločevalno ime vsebuje osnovne podatke o imetniku oz. nazivu in organizaciji. Razločevalno ime se glede na vrste potrdil tvori po naslednjih pravilih[2]:

Vrsta potrdila	Razločevalno ime
osebna potrdila organizacij	c=si, o=state-institutions, ou=sigen-ca, ou=companies (*ali* ou=org) ou=<kratko ime organizacije>-<davčna št. organizacije>, cn=<naziv>, sn=<serijska številka>
spletna potrdila organizacij	c=si, o=state-institutions, ou=sigen-ca, ou=companies-web (*ali* ou=org-web) ou=<kratko ime organizacije>-<davčna št. organizacije>, cn=<naziv>, sn=<serijska številka>

[2] Pomen posameznih podatkov je razložen v nadaljevanju.

(2) Kratko ime organizacije, ki je po spodaj navedenih pravilih vključeno v razločevalno ime, mora izpolnjevati naslednje zahteve:
- mora biti enolično, registrirano v poslovnem ali drugem uradnem registru ali drugače določeno,
- mora biti pomensko povezano z imetnikom oz. organizacije,
- maksimalna dolžina je lahko 70 znakov.

(3) SIGEN-CA si pridržuje pravico za zavrnitev kratkega imena, če ugotovi:
- da je le-to neprimerno oz. žaljivo,
- da je zavajajoče za tretje stranke oz. že pripada neki drugi pravni ali fizični osebi,
- da je v nasprotju z veljavnimi predpisi.

(4) Pod nazivom, ki je po spodaj navedenih pravilih vključeno v razločevalno ime, je v primeru potrdila:
- za zaposlene navedeno imetnikovo ime in priimek,
- za splošni naziv oz. organizacijske enote organizacije naveden splošni naziv oz. organizacijska enota organizacije,
- za strežnike navedeno ime strežnika DNS, ki je ustrezno registrirano.

(5) V primeru potrdila za splošni naziv oz. organizacijske enote organizacije si SIGEN-CA pridržuje pravico za zavrnitev naziva, če ugotovi:
- da je le-to neprimerno oz. žaljivo,
- da je zavajajoče za tretje stranke oz. že pripada neki drugi pravni ali fizični osebi,
- da je v nasprotju z veljavnimi predpisi.

(6) Podatki o imetniku oz. nazivu in organizaciji v razločevalnem imenu vsebujejo črke angleške abecede. Drugi znaki se pretvorijo po pravilih iz spodnje tabele.

Znak	Pretvorba
č	c
š	s
ž	z
ü	ue
ö	oe
Ø	oe
ß	ss
ñ	n
ŕ	rz

(7) Serijsko številko, ki je vključeno v razločevalno ime, dodeli SIGEN-CA.

(8) Serijska številka je 13-mestno število in enolično določa potrdilo. Spodnja tabela natančneje določa pomen in vrednosti posameznih mest serijskega števila:

Serijska številka	Pomen	Vrednost	
1. mesto	oznaka za potrdilo SIGEN-CA	2	
2.- 8. mesto	enolično število imetnika	/	
9. - 10. mesto	osebna potrdila	zaposleni	20
		splošni naziv	22
		strežnik	24
	spletna potrdila	zaposleni	16
		splošni naziv	18
		strežnik	10

		podpis kode	19
11. – 12. mesto	zaporedna številka istovrstnega potrdila	/	
13. mesto	kontrolna številka	/	

4.2.4. Zahteve za elektronski naslov

(1) Elektronski naslov mora izpolnjevati naslednje zahteve:
- mora biti veljaven in
- mora biti pomensko povezan z imetnikom oz. organizacijo.

(2) SIGEN-CA si pridržuje pravico za zavrnitev zahtevka za pridobitev potrdila, če ugotovi, da je elektronski naslov:
- neprimeren oz. žaljiv,
- da je zavajajoč za tretje stranke,
- predstavlja neko drugo pravno ali fizično osebo,
- je v nasprotju z veljavnimi predpisi in standardi.

5. UPRAVLJANJE POTRDIL

5.1. Pridobitev potrdila

(1) Za pridobitev potrdila morata bodoči imetnik in odgovorna oseba pravilno izpolniti in podpisati zahtevek za pridobitev potrdila.

(2) Zahtevki za pridobitev so dostopni na prijavnih službah in na spletnih straneh SIGEN-CA.

(3) Zahtevek za pridobitev potrdila odobrijo oz. v primeru nepravilnih ali pomanjkljivih podatkov ali neizpolnjevanja obveznosti iz pogodbe s strani organizacije zavrnejo pooblaščene osebe overitelja na CVI. O odobritvi oz. zavrnitvi je bodoči imetnik obveščen. Ob odobritvi odgovorna oseba in bodoči imetnik prejmeta vso potrebno dokumentacijo v skladu z ZEPEP, s katero sta bila seznanjena že pred podpisom zahtevka za pridobitev potrdila.

(4) Potrdila se izdajajo izključno na infrastrukturi overitelja na CVI.

(5) SIGEN-CA na podlagi odobrenega zahtevka in veljavne pogodbe med organizacijo in overiteljem na CVI opravi rezervacijo potrdila najkasneje v desetih (10) dneh od odobritve zahtevka.

(6) SIGEN-CA preda bodočemu imetniku potrdila referenčno številko in avtorizacijsko kodo osebno ali pa ju posreduje po dveh ločenih poteh: referenčno številko po elektronski pošti, avtorizacijsko kodo pa po priporočeni pošti. Po prevzemu potrdila postaneta referenčna številka in avtorizacijska koda neuporabni.

(7) Bodoči imetnik potrdila mora po prejemu referenčne številke in avtorizacijske kode potrdilo prevzeti v šestdesetih (60) dneh od rezervacije potrdila, sicer SIGEN-CA rezervacijo potrdila prekliče.

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

5.2. Preklic potrdila

(1) Overitelj na CVI prekliče potrdilo na zahtevo odgovorne osebe, imetnika, na zahtevo pristojnega sodišča, sodnika za prekrške ali upravnega organa.

(2) O datumu ter času preklica, izdajatelju zahtevka za preklic ter vzrokih za preklic mora biti vedno obveščen imetnik in odgovorna oseba.

(3) Preklic potrdila morata imetnik ali odgovorna oseba organizacije zahtevati v primeru:
- če so bili zasebni ključi imetnika potrdila ogroženi na način, ki vpliva na zanesljivost uporabe,
- če obstaja nevarnost zlorabe zasebnih ključev ali potrdila imetnika,
- če so se spremenili oz. so napačni ključni podatki, navedeni v potrdilu,
- če imetnik ni več zaposlen v organizaciji ali je prenehal z delom za organizacijo ali ni več pooblaščen za opravljanje storitev z uporabo potrdila.

(4) Overitelj na CVI prekliče potrdilo tudi brez zahteve imetnika ali odgovorne osebe organizacije, takoj ko izve:
- da je imetnik potrdila prenehal delati v ali za organizacijo,
- da so se spremenile druge okoliščine, ki vplivajo na veljavnost potrdila,
- da je podatek v potrdilu napačen ali je bilo potrdilo izdano na podlagi napačnih podatkov,
- da je prišlo do napake pri preverjanju istovetnosti podatkov na prijavni službi,
- za neizpolnjevanje obveznosti imetnika oz. organizacije iz te politike in iz pogodbe med organizacijo in overiteljem na CVI,
- če niso poravnani stroški za upravljanje digitalnih potrdil,
- da je bila infrastruktura overitelja na CVI ogrožena na način, ki vpliva na zanesljivost potrdila,
- da so bili zasebni ključi imetnika potrdila ogroženi na način, ki vpliva na zanesljivost uporabe,
- da bo SIGEN-CA prenehala z izdajanjem potrdil ali da je bilo overitelju na CVI prepovedano upravljanje s potrdili in njegove dejavnosti ni prevzel drug overitelj,
- da je preklic odredilo pristojno sodišče, sodnik za prekrške ali upravni organ.

(5) Overitelj na CVI v primerih iz prejšnjega odstavka prekliče potrdilo brez predhodnega obvestila imetniku potrdila ali odgovorni osebi organizacije.

(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 odgovorna oseba organizacije 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 ustrezen zahtevek za preklic potrdila ter ga izročiti na prijavno službo.

(9) Če se preklic opravi elektronsko, morata imetnik ali odgovorna oseba na SIGEN-CA poslati zahtevek za preklic, ki mora biti digitalno podpisan z zaupanja vrednim potrdilom. Ob poslanem zahtevku za preklic mora izdajatelj zahtevka za preklic hkrati o tem telefonsko obvestiti SIGEN-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 ustreznem zahtevku za pridobitev potrdila imetnik podal kot geslo za preklic potrdila oz. ga je drugače varno posredoval SIGEN-CA. Brez gesla za preklic imetnik ne more telefonsko preklicati potrdila.

(11) Overitelj na CVI po prejemu veljavne zahteve za preklic najkasneje v štirih (4) urah prekliče potrdilo. V tem času je preklicano potrdilo dodano v register preklicanih potrdil in brisano iz javnega imenika potrdil.

5.3. Podaljševanje veljavnosti potrdil - velja za osebna potrdila

Generiranje novih parov ključev in podaljševanje veljavnosti osebnega potrdila se izvaja avtomatsko ob prvi uporabi potrdila imetnika z neposrednim dostop do infrastrukture SIGEN-CA v obdobju stotih (100) dni pred zadnjim dnem veljavnosti potrdila. Za podaljšana potrdila velja Politika SIGEN-CA, veljavna ob datumu generiranja novih parov ključev.

5.4. Regeneriranje ključev - velja za osebna potrdila

(1) Regeneriranje ključev za osebno potrdilo se izvede, če imetnik potrdila:
- pozabi geslo za dostop do zasebnih ključev,
- izgubi ali poškoduje nosilcev ključnih podatkov za uporabo potrdila,
- nima omogočenega avtomatičnega podaljševanja veljavnosti potrdila,
- ni izvedel dostopa do svojega potrdila tako dolgo, da mu je potekla veljavnost ključa za digitalno podpisovanje in s tem dostop do potrdila.

(2) Overitelj na CVI si glede na varnostne okoliščine dovoljuje samostojno odločitev med:
- regeneriranjem ključev imetnikovega potrdila
- ali preklicem.

(3) Regeneriranje ključev za potrdila se izvede na osnovi izpolnjenega zahtevka za regeneriranje ključev s strani imetnika potrdila, ki ga odda na prijavni službi SIGEN-CA. Podobno kot pri izdaji novega potrdila dobi imetnik referenčno številko in avtorizacijsko kodo za dostop do para ključev za šifriranje in generiranje novega para ključev za podpisovanje. Regeneracijo mora opraviti v šestdesetih (60) dneh.

5.5. Odkrivanje kopije ključev za dešifriranje - velja za osebna potrdila

(1) Overitelj na CVI odkrije kopijo ključev za dešifriranje le v izjemnih primerih, ko le-ti iz kakršnegakoli razloga niso dostopni:
- odgovorni osebi na podlagi zahtevka za odkrivanje kopije ključev za dešifriranje, ki ga odgovorna oseba podpiše in na varen način posreduje na SIGEN-CA za dostop do podatkov, ki so zašifrirani in dostopni z imetnikovim ključem za dešifriranje,
- če to odredi pristojno sodišče, sodnik za prekrške ali upravni organ.

(2) Overitelj na CVI si pridružuje pravico, da ne odobri odkritja kopije ključev za dešifriranje, če gre za potrdilo, ki je bilo preklicano zaradi napačnih podatkov v potrdilu.

(3) Overitelj na CVI pred odkrivanjem kopije ključev za dešifriranje:
- po elektronski pošti obvesti imetnika potrdila o datumu ter izdajatelju zahtevka za odkrivanje kopije njegovih ključev za dešifriranje podatkov, in
- prekliče veljavnost potrdila in po elektronski pošti o preklicu obvesti imetnika.

5.6. Morebitno prenehanje delovanja overitelja na CVI oz. izdajatelja SIGEN-CA

Če bo overitelj na CVI prenehal z opravljanjem svoje dejavnosti ali izdajatelj SIGEN-CA prenehal z izdajanjem potrdil, bo overitelj na CVI ukrepal v skladu z ZEPEP.

6. OBVEZNOSTI IN ODGOVORNOST

6.1. Obveznosti in odgovornost imetnika potrdila oziroma organizacije

(1) Imetnik oziroma bodoči imetnik potrdila je dolžan:
- seznaniti se in ravnati v skladu s to politiko in pogodbo med organizacijo in overiteljem na CVI pred podpisom zahtevka za potrdilo,
- ravnati v skladu s to politiko in določili iz pogodbe med organizacijo in overiteljem na CVI in ostalimi veljavnimi predpisi,
- 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.

(2) Imetnik oziroma bodoči imetnik potrdila je glede varovanja zasebnih ključev dolžan tudi:
- podatke za prevzem potrdila skrbno varovati pred nepooblaščenimi osebami,
- hraniti zasebne ključe in potrdilo na način in na sredstvih za varno hranjenje zasebnih ključev v skladu z obvestili SIGEN-CA,
- zasebne ključe 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 zasebnih ključev,
- po preteku oz. preklicu veljavnosti potrdila ravnati v skladu z obvestili SIGEN-CA.

(3) Imetnik oziroma bodoči imetnik potrdila je glede uporabe potrdila dolžan tudi:
- ob prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti SIGEN-CA oziroma zahtevati preklic,
- uporabljati potrdilo za namen in na način, ki je določen s politiko SIGEN-CA,
- uporabljati tako programsko in opremo, ki je v skladu z obvestili SIGEN-CA (z dovolj močnimi kriptografskimi moduli),
- skrbeti za arhiv elektronskih dokumentov ter potrebnih podatkov za uporabo potrdila.

(4) Odgovorna oseba oz. organizacija je dolžna:
- skrbno prebrati to politiko in določila iz pogodbe med organizacijo in overiteljem na CVI 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 SIGEN-CA,
- ravnati v skladu z obvestili, to politiko in pogodbo med organizacijo in overiteljem na CVI 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 SIGEN-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.

(5) Organizacija odgovarja:
- za nastalo škodo v primeru zlorabe potrdila od prijave preklica do preklica,
- za vsako škodo, ki je bodisi posredno ali neposredno povzročena zato, ker je bila omogočena uporaba oz. zloraba imetnikovega potrdila s strani nepooblaščenih oseb.

6.2. Obveznosti in odgovornost overitelja na CVI

(1) Overitelj na CVI je dolžan:
- izdajati potrdila, upravljati z njimi ter delovati v skladu s svojimi notranjimi pravili in ostalimi veljavnimi predpisi,
- preklicati potrdilo in objaviti preklicano potrdilo v registru preklicanih potrdil, ko ugotovi, da so podani razlogi po tej politiki ali drugih veljavnih predpisih,
- varno ravnati z osebnimi in zaupnimi podatki o overitelju, imetnikih potrdil ali podatkov o organizacijah,
- zagotoviti delovanje prijavnih služb v skladu z določili SIGEN-CA in ostalimi veljavnimi predpisi,
- objavljati na svojih spletnih straneh vse informacije o tistih spremembah glede dejavnosti overitelja, ki kakorkoli vplivajo na imetnike potrdil, organizacije in tretje osebe.

(2) Overitelj na CVI ni dolžan preverjati obstoja pravic firmskega prava ali pravic industrijske lastnine, ampak je za to pooblaščena izključno organizacija.

(3) Overitelj na CVI je odgovoren:
- da potrdilo vsebuje vse predpisane podatke za potrdilo po tej politiki in drugih predpisih,
- da je imel imetnik potrdila v času izdaje le-tega zasebni ključ ustrezen v potrdilu navedenemu javnemu ključu.

(4) Overitelj na CVI ni odgovoren za:
- uporabo potrdil za namen in na način, ki ni izrecno predviden v tej politiki oz. pogodbi med organizacijo in SIGEN-CA,
- nepravilnega ali pomanjkljivega varovanja gesel ali zasebnih ključev imetnikov, izdajanje zaupnih podatkov ali ključev tretjim osebam in neodgovornega ravnanja imetnika,
- kakršnekoli zlorabe oziroma 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 v registru preklicanih potrdil,
- drugega ravnanja imetnika potrdila, njegove organizacije ali tretje osebe v nasprotju z obvestili SIGEN-CA, to politiko in drugimi predpisi.
- škode, ki je bodisi posredno ali neposredno povzročena zato, ker je bila omogočena uporaba oz. zloraba imetnikovega potrdila nepooblaščenim osebam,
- za uporabo potrdil ter veljavnost potrdil ob spremembah podatkov iz potrdila elektronskih naslovov ali spremembah imen organizacij ali imetnikov,
- odgovornost v primeru izpada infrastrukture, ki ni v domeni upravljanja overitelja na CVI,
- za podatke, ki se šifrirajo ali podpisujejo z uporabo potrdil,
- za ravnanje imetnikov pri uporabi potrdil, in sicer tudi v primeru, če je imetnik ali tretja oseba spoštoval vsa določila te politike, obvestila SIGEN-CA ali druge veljavne predpise,
- za uporabo in zanesljivost delovanja strojne in programske opreme imetnikov potrdil.

(5) Infrastruktura overitelja na CVI deluje 24 ur na dan vse dni v letu, vendar si overitelj na CVI pridržuje

pravico za ustavitev delovanja v primeru nepravilnega delovanja, možnosti zlorabe, tehničnih vzrokov. V primeru vzdrževanja ali nadgradnje overitelja na CVI se vzdrževalna dela tri (3) dni predhodno objavi.

(6) Overitelj na CVI ne posreduje drugih podatkov o imetnikih potrdil oz. organizacijah, ki niso navedeni v potrdilu, razen če se določeni podatki posebej zahtevajo za izvajanje specifičnih storitev oz. aplikacij, povezanih s potrdili, ter je to na zahtevku za pridobitev potrdila ali kasneje v pisni obliki odobril imetnik potrdila oz. odgovorna oseba organizacije, ali na zahtevo pristojnega sodišča, sodnika za prekrške ali upravnega organa. Podatki se posredujejo tudi brez pisne privolitve, če to določa zakonodaja oz. veljavni predpisi.

6.3. Zahteve za tretje osebe

Tretja oseba, ki se zanaša na potrdilo, mora:
- ravnati in uporabljati potrdila v skladu in namenom s to politiko in ostalimi veljavnimi predpisi,
- skrbno proučiti vse možnosti tveganja in odgovornosti pri uporabi potrdil in določiti politiko za način uporabe,
- obvestiti SIGEN-CA, če izve, da so bil zasebni ključi ogroženi na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, navedeni v potrdilu,
- skrbeti za originalno podpisane dokumente,
- v času uporabe potrdila natančno preveriti, če potrdilo ni v registru preklicanih potrdil,
- v času uporabe potrdila natančno preveriti, če je bil digitalni podpis kreiran v času veljavnosti in z ustreznim namenom potrdila,
- v času uporabe potrdila preveriti podpis izdajatelja potrdila SIGEN-CA, ki je objavljen v tej politiki in tudi na spletnih straneh SIGEN-CA oz. drugih izdajateljev potrdil overitelja na CVI.

7. KONČNE DOLOČBE

(1) Ob morebitnem sporu med overiteljem na CVI na eni strani in imetnikom potrdila, njegovo organizacijo ali tretjo osebo na drugi strani, je pristojno sodišče v Ljubljani po pravu Republike Slovenije.

(2) Določbe glede avtorskih, sorodnih in drugih pravic intelektualne lastnine:
- na pričujoči politiki pripadajo vse pravice overitelju na CVI,
- na javnem imeniku potrdil in registru preklicanih potrdil pripadajo vse pravice overitelju na CVI,
- na vseh podatkih v potrdilih pripadajo vse pravice overitelju na CVI,
- na zasebnem ključu za podpisovanje pripadajo vse pravice imetniku potrdila oz. organizaciji.

8. TERMINOLOŠKI SLOVAR IN OZNAKE

CP_{Name}	Ime politike delovanja overitelja (angl. *Certification Policy Name*), povezano z mednarodno številko politike delovanja CP_{OID} (CP_{Name}, angl. *Certification Policy Object Identifier*).
CP_{OID}	Mednarodna številka, ki enolično določa politiko delovanja (CP_{OID}, angl. *Certification Policy Object IDentifier*).
CRL	Seznam preklicanih potrdil (prim. definicijo Register preklicanih potrdil). (CRL, angl. *Certification Revocation List*).
CVI	Center Vlade Republike Slovenije za Informatiko, Langusova 4, 1000 Ljubljana, slovenija (http://www.gov.si/cvi).
DNS	Baza imen računalnikov, ki so vključeni v internet. Omogoča povezave imen računalnikov z njihovimi številkami IP. (DNS, angl. *Domain Name System*)
Identifikacijska oznaka	Interna enolična številka potrdila.
Imetnik potrdila	Imetnik potrdila je oseba, ki je navedena v potrdilu in ki razpolaga s svojimi zasebnimi ključi oz. pooblaščena oseba za uporabo potrdila za splošne nazive organizacij oz. organizacijske enote organizacij ali za uporabo strežnike (storitve oz. aplikacije).
Infrastruktura overitelja na CVI	Infrastruktura overitelja na CVI so vsi prostori overitelja, njegova strojna in programska oprema ter varnostni mehanizmi, ki so potrebni za varno delovanje SIGEN-CA.
Javni imenik potrdil	Javni imenik na CVI po standardu X.500, kjer so shranjena potrdila po standardu X.509 ver. 3.
LDAP	Protokol, ki določa dostop do imenika in je specificiran po IETF (angl. *Internet Engineering Task Force*) priporočilu RFC 1777. (LDAP, angl. *Leightweight Directory Access Protocol*)
Odgovorna oseba	Fizična oseba, ki je pooblaščena za zastopanje pravne ali fizične osebe, registrirane za opravljanje dejavnosti, v pravnem prometu.
Overitelj	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi. (CA, angl. *Certification Authority*).
Politika SIGEN-CA	Javni del notranjih pravil Overitelja na CVI za izdajatelja kvalificiranih digitalnih potrdil SIGEN-CA za pravne in fizične osebe, registrirane za opravljanje dejavnosti.

Potrdilo	Kvalificirano digitalno potrdilo v elektronski obliki, ki povezuje podatke iz potrdila določene osebe z zasebnim ključem določene osebe ter potrjuje njeno istovetnost. (angl. *qualified digital certificate)*.
Prevzem oz. izdaja potrdila	Postopek generiranja ključev in izdaja potrdila na osnovi odobrenega zahtevka za pridobitev za določeno osebo. Potrdilo vključuje javni ključ določene osebe in ostale podatke. Potrdilo je izdano po trenutno veljavni politiki (prim. definicijo Pridobitev potrdila).
Pridobitev potrdila	Postopek pridobitve vključuje oddajo zahtevka za pridobitev na prijavni službi, preverjanje istovetnosti, odobritev zahtevka za pridobitev, rezervacijo potrdila z izdajo kod za prevzem potrdila in postopek prevzema oz. izdaje potrdila (prim. definicijo Potrdilo in Prevzem oz. izdaja potrdila).
Prijavna služba	Služba za sprejem zahtevkov za potrdila in preverjanje istovetnosti bodočih imetnikov, imetnikov in organizacij (*RA,* angl. *Registration Authority)*.
Razločevalno ime	Enolično ime v potrdilu, ki nedvoumno in enolično definira imetnika v strukturi javnega imenika. (DN, angl. *Distinguished Name).*
Register preklicanih potrdil	Seznam preklicanih potrdil (CRL, angl. *Certification Revocation List)*. Osvežuje se enkrat dnevno oz. z vsakim preklicem potrdila.
Serijska številka	Enolično 13-mestno število, ki ga potrdilu podeli SIGEN-CA. Prvo mesto določa potrdilo izdajatelja SIGEN-CA, 7 mest številke je enolično število imetnika oz. uporabnika, 9. in 10. mesto določata vrsto potrdila, naslednji dve mesti predstavljata zaporedno številko potrdila, zadnje mesto je kontrola zapisa.
SIGEN-CA	Izdajatelj potrdil za pravne in fizične osebe overitelja potrdil na Centru Vlade RS za informatiko (CVI). (SIGEN-CA, angl. *Slovenian General Certification Authority*) (prim. definicijo Overitelj).
SIGOV-CA	Izdajatelj potrdil za institucije javne uprave overitelja potrdil na Centru Vlade RS za informatiko (CVI). (SIGOV-CA, angl. *Slovenian Governmental Certification Authority*) (prim. definicijo Overitelj).
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 57/2000).