CENTER VLADE REPUBLIKE SLOVENIJE
ZA INFORMATIKO

POLITIKA SIGOV-CA

za kvalificirana digitalna potrdila za institucije javne uprave*

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

veljavnost: od 28. oktobra 2003
verzija: 2.1

- **Politika za spletna kvalificirana digitalna potrdila za zaposlene in splošne nazive,** CP_{OID}: 1.3.6.1.4.1.6105.1.1.3
- **Politika za osebna kvalificirana digitalna potrdila za zaposlene in splošne nazive,** CP_{OID}: 1.3.6.1.4.1.6105.1.2.3
- **Politika za spletna kvalificirana digitalna potrdila za strežnike in podpis kode,** CP_{OID}: 1.3.6.1.4.1.6105.1.3.1
- **Politika za osebna kvalificirana digitalna potrdila za strežnike,** CP_{OID}: 1.3.6.1.4.1.6105.1.4.1
- **Politika za kvalificirana digitalna potrdila za izdajatelje varnih časovnih žigov,** CP_{OID}: 1.3.6.1.4.1.6105.1.5.1

* Institucije javne uprave, ki so ki so v informacijsko-telekomunikacijskem omrežju državnih organov.

Izdaje politik delovanja SIGOV-CA	
Verzija 2.1: pričetek veljavnosti: 28. oktober 2003	
• Politika SIGOV-CA za spletna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.1.1.3 • Politika SIGOV-CA za osebna kvalificirana digitalna potrdila za zaposlene in splošne nazive, CP_{OID}: 1.3.6.1.4.1.6105.1.2.3 • Politika SIGOV-CA za spletna kvalificirana digitalna potrdila za strežnike in podpis kode, CP_{OID}: 1.3.6.1.4.1.6105.1.3.1 • Politika SIGOV-CA za osebna kvalificirana digitalna potrdila za strežnike, CP_{OID}: 1.3.6.1.4.1.6105.1.4.1 • Politika SIGOV-CA za kvalificirana digitalna potrdila za izdajatelje varnih časovnih žigov, CP_{OID}: 1.3.6.1.4.1.6105.1.5.1 CP_{Name}: SIGOV-CA	*sprememba* • kvalificirana digitalna potrdila za izdajatelje varnih časovnih žigov • ločene politike za potrdila, za katere so obvezna sredstva za varno hrambo potrdil • struktura dokumenta v skladu z RFC 2527
Verzija 2: pričetek veljavnosti: 15. julij 2002	
• Politika SIGOV-CA za kvalificirana digitalna potrdila za institucije javne uprave, CP_{OID}: 1.3.6.1.4.1.6105.1.1.2 in 1.3.6.1.4.1.6105.1.2.2 CP_{Name}: SIGOV-CA	*sprememba:* kvalificirana digitalna potrdila za splošne nazive oz. organizacijske enote institucij in podpis kode
Verzija 1: pričetek veljavnosti: 17. januar 2001	
• Politika SIGOV-CA za službena spletna kvalificirana digitalna potrdila, CP_{OID}:1.3.6.1.4.1.6105.1.1.1, CP_{Name}: SIGOV-CA-1 • Politika SIGOV-CA za službena osebna kvalificirana digitalna potrdila, CP_{OID}: 1.3.6.1.4.1.6105.1.2.1, CP_{Name}: SIGOV-CA-2	*prva verzija politik*

VSEBINA

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 institucije javne uprave Republike Slovenije, ki so v informacijsko-telekomunikacijskem omrežju državnih organov (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.

Pričujoči dokument določa politike izdajatelja SIGOV-CA za posamezne vrste kvalificiranih digitalnih potrdil, ki izpolnjujejo najvišje varnostne zahteve. Na podlagi tega dokumenta SIGOV-CA izdaja osebna in spletna kvalificirana digitalna potrdila po različnih politikah (CP_{OID} = 1.3.6.1.4.1.6105.1.1.3, 1.3.6.1.4.1.6105.1.2.3, 1.3.6.1.4.1.6105.1.3.1, 1.3.6.1.4.1.6105.1.4.1, 1.3.6.1.4.1.6105.1.5.1). Pričujoči dokument nadomešča politike delovanja SIGOV-CA verzije 2 (CP_{OID} = 1.3.6.1.4.1.6105.1.1.2, 1.3.6.1.4.1.6105.1.2.2), ki ostanejo v veljavi za potrdila izdana pred veljavo pričujočih politik. Vsa kvalificirana digitalna potrdila, izdana oz. podaljšana po datumu veljavnosti nove politike, se obravnavajo po novi politiki. Spremembe pričujočega dokumenta so sledeče:

- digitalna potrdila, za katera se izda tudi sredstva za varno hranjenje potrdila (t.j. pametne kartice oz. druge varne kriptografske module), se izdajajo po svoji politiki (za zaposlene, splošne nazive oz. organizacijske enote, za spletna - CP_{OID} = 1.3.6.1.4.1.6105.1.1.3, za osebna - CP_{OID} = 1.3.6.1.4.1.6105.1.2.3),
- za informacijske sisteme in podpis kode, za katere SIGOV-CA priporoča uporabo sredstev za varno hranjenje potrdil, t.j. varne kriptografske module, pa po ločenih politikah (spletna - CP_{OID} = 1.3.6.1.4.1.6105.1.3.1, za osebna - CP_{OID} = 1.3.6.1.4.1.6105.1.4.1),
- uvedba nove vrste kvalificiranih digitalnih potrdil, in sicer za izdajatelje varnih časovnih žigov. Politika, pod katero se izdaja tovrstna potrdila, je CP_{OID} = 1..3.6.1.4.1.6105.1.5.1,
- struktura dokumenta sledi priporočilom RFC 2527 in ETSI TS 101 456.

Potrdila se pridobijo na podlagi zahtevka, ki ga mora podpisati predstojnik institucije in bodoči imetniki. V primeru potrdila za splošni naziv ali strežnik je bodoči imetnik zaposleni oz. oseba, ki jo predstojnik pooblasti za uporabo tega potrdila. Predstojnik s podpisom zahtevka jamči za istovetnost bodočih imetnikov. Izpolnjen zahtevek se osebno na prijavni službi (seznam je objavljen na spletni strani http://www.sigov-ca.gov.si/prijavne-slu.htm).

SIGOV-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 SIGOV-CA.

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

1. UVOD

1.1. Pregled

(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, ki so v informacijsko-telekomunikacijskem omrežju državnih organov,
- 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) 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.

(7) Po pričujoči politiki SIGOV-CA izdaja kvalificirana digitalna potrdila za institucije javne uprave, ki so v informacijsko-telekomunikacijskem omrežju državnih organov:
- 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,
- kvalificirana digitalna potrdila za izdajatelja varnih časovnih žigov[1],
- za druge overitelje digitalnih potrdil.

[1] Potrdilo za izdajatelja časovnih žigov se, kjer ni drugače navedeno, obravnava kot osebno kvalificirano digitalno potrdilo.

(8) Osebna kvalificirana digitalna potrdila SIGOV-CA 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.

(9) Spletna kvalificirana digitalna potrdila SIGOV-CA 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.

(10) Pričujoča politika določa delovanje overitelja na CVI za kvalificirana digitalna potrdila SIGOV-CA za institucije javne uprave, ki so v informacijsko-telekomunikacijskem omrežju državnih organov:
- CP_{OID} = 1.3.6.1.4.1.6105.1.1.3 za spletna potrdila za zaposlene in splošne nazive,
- CP_{OID} = 1.3.6.1.4.1.6105.1.2.3 za osebna potrdila za zaposlene in splošne nazive,
- CP_{OID} = 1.3.6.1.4.1.6105.1.3.1 za spletna potrdila za strežnike in podpis kode,
- CP_{OID} = 1.3.6.1.4.1.6105.1.4.1 za osebna kvalificirana potrdila za strežnike,
- CP_{OID} = 1.3.6.1.4.1.6105.1.5.1 za potrdila za izdajatelje varnih časovnih žigov,
- ter druge overitelje potrdil.

(11) Za osebna in spletna potrdila, izdana na podlagi politike po CP_{OID} = 1.3.6.1.4.1.6105.1.1.3 in CP_{OID} = 1.3.6.1.4.1.6105.1.2.3, se zahteva uporaba sredstev za varno digitalno podpisovanje oz. varno hranjenje zasebnih ključev in potrdil, za druga se priporoča upoštevanje navodil za zaščito zasebnih ključev oz. uporabo varnih kriptografskih modulov.

(12) Pričujoč dokument določa politiko upravljanja s kvalificiranimi digitalnimi potrdili in definira naslednje storitve: rezervacijo, izdajanje in overjanje, preklicevanje, regeneriranje ključev, odkrivanje kopije zasebnega ključa za dešifriranje, hranjenje in objavljanje kvalificiranih digitalnih potrdil.

(13) V primeru, da CVI nima zagotovljenih sredstev za institucijo, se medsebojna razmerja izvajajo tudi na podlagi pisnega dogovora med institucijo in overiteljem na CVI.

(14) 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.

(15) 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.

(16) Overitelj na CVI lahko overja in javno objavlja politike podrejenih overiteljev v primeru, da se namen uporabe kvalificiranih digitalnih potrdil razlikujejo od namena uporabe, definirane v tej politiki.

1.1.1 Pomen izrazov v politiki

Posamezni izrazi imajo v nadaljevanju te politike pomen, prikazan v spodnji tabeli:

SIGOV-CA	izdajatelj kvalificiranih digitalnih potrdil overitelja na CVI za institucije javne uprave, ki je v informacijsko-telekomunikacijskem omrežju državnih organov

institucija	institucija javne uprave, ki je v informacijsko-telekomunikacijskem omrežju državnih organov, in katere predstojnik je naročnik digitalnih potrdil (angl. *subscriber*)
potrdilo	osebno ali spletno kvalificirano digitalno potrdilo (angl. *qualified digital certificate*)
osebno potrdilo	osebno kvalificirano digitalno potrdilo v elektronski obliki (osebno potrdilo sestavlja potrdilo za podpis/overjanje podpisa in potrdilo za dešifriranje/šifriranje), ki povezuje podatke iz potrdila z imetnikovima zasebnima ključema ter potrjuje imetnikovo istovetnost (angl. *enterprise certificate*)
spletno potrdilo	spletno kvalificirano digitalno potrdilo v elektronski obliki, ki povezuje podatke iz potrdila z imetnikovim zasebnim ključem ter potrjuje imetnikovo istovetnost (angl. *web certificate*)
zaposleni	fizične osebe, ki so v delovnem razmerju z institucijo ali pa na drugačni pravni podlagi delajo za institucijo in za katere želi predstojnik le-te pridobiti potrdila, ki jih te osebe potrebujejo za opravljanje dela za to institucijo
izdajatelj TSA	izdajatelj varnih časovnih žigov (TSA, angl. Time Stamping Authority)
imetnik	zaposleni, ki so pooblaščeni za uporabo potrdila, za potrdila za splošne nazive, za strežnike, za podpis kode ali izdajatelj TSA (angl. *subject*)
zahtevki	obrazci SIGOV-CA za pridobivanje in preklic potrdil, regeneracijo ključev osebnega potrdila, odkrivanje kopije zasebnega ključa za dešifriranje osebnega potrdila, ki so dostopni preko spletnih strani SIGOV-CA oz. pri pooblaščenih osebah na prijavnih službah
prijavna služba	po pooblastilu prijavna služba overitelja na CVI sprejema zahtevke za pridobitev in preklic potrdil ter regeneracijo ključev osebnih potrdil in preverja istovetnosti bodočih imetnikov oz. podatkov o institucijah (angl. *registration authority*)
pridobitev potrdila	postopek, ki vključuje oddajo zahtevka za pridobitev na prijavno službo, preverjanje istovetnosti, odobritev zahtevka za pridobitev, rezervacijo potrdila z izdajo aktivacijskih kod za prevzem potrdila in postopek prevzema oz. izdaje potrdila
prevzem oz. izdaja potrdila	postopek generiranja ključev in izdaja potrdila, ki vključuje imetnikov javni ključ in ostale podatke
objava SIGOV-CA	javna objava na spletnih straneh SIGOV-CA
obvestila SIGOV-CA	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
Uredba	Uredba o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 77/2000 in 2/2001)
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 57/2000)

1.2. Razpoznavni podatki izdajatelja SIGOV-CA

1.2.1 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

1.2.2 Identiteta izdajatelja SIGOV-CA

(1) Izdajatelj SIGOV-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 SIGOV-CA.

Potrdilo SIGOV-CA vsebuje naslednje podatke.

Identifikacijska oznaka:	3A5C 701A
Overitelj potrdila:	ou=SIGOV-CA, o=state-institutions, c=si
Imetnik potrdila:	ou=SIGOV-CA, o=state-institutions, c=si
Veljavnost potrdila:	od 10. januarja 2001 do 10. januarja 2021
Dolžina ključa:	2048 bitov
Identiteta ključa (SHA1):	1EF8 D453 6BB3 8306 E904 0657 02F9 A5BF C658 3C72
Odtis potrdila (MD5):	739D D35F C63C 95FE C6ED 89E5 8208 DD89
Odtis potrdila (SHA-1):	7FB9 E2C9 95C9 7A93 9F9E 81A0 7AEA 9B4D 7046 3496

1.3. Subjekti in namen uporabe

1.3.1 Overitelj na CVI in izdajatelj SIGOV-CA

(1) Overitelj na CVI izdaja kvalificirana digitalna potrdila, za katera velja najvišja stopnja varovanja in načela t.i. močne enkripcije ter deluje v skladu z veljavnimi predpisi.

(2) Overitelja na CVI predstavljata dva izdajatelja kvalificiranih digitalnih potrdil:
- SIGOV-CA je izdajatelj kvalificiranih digitalnih potrdil overitelja na CVI za institucije javne uprave, ki delujejo v omrežju državnih organov.
- SIGEN-CA je izdajatelj kvalificiranih digitalnih potrdil overitelja na CVI za pravne in fizične osebe.

1.3.2 Prijavna služba SIGOV-CA

(1) Naloge prijavnih služb so:
- preverjanje istovetnost imetnikov oz. bodočih imetnikov, podatkov o instituciji in drugih potrebnih podatkov,
- sprejemanje zahtevkov za pridobitev potrdil,
- sprejemanje zahtevkov za preklic potrdil,
- sprejemanje zahtevkov za regeneracijo ključev osebnih potrdil,
- preverjanje zahtevkov,
- izdajanje potrebne dokumentacije imetnikom oz. bodočim imetnikom in institucijam,
- posredovanje zahtevkov in ostalih podatkov na varen način na SIGOV-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) Naloge prijavne službe SIGOV-CA vrši:
- institucija za svoje zaposlene osebe opravlja del nalog prijavnih služb po določilih SIGOV-CA, in sicer predstojnik institucije, kjer je bodoči imetnik potrdila zaposlen, jamči za istovetnost bodočega imetnika potrdila, ki jo je preveril v skladu z 31. členom in drugimi določili ZEPEP,
- preverjanje istovetnost imetnikov oz. bodočih imetnikov, podatkov o instituciji in drugih potrebnih podatkov in izdajanje potrebne dokumentacije vršijo pooblaščene osebe prijavne službe na sedežu overitelja na CVI.

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

1.3.3 Institucije in imetniki potrdil

(1) Institucija oz. predstojnik je naročnik digitalnih potrdil (angl. subscriber) za imetnike - zaposlene v instituciji.

(2) Predstojnik s podpisom zahtevka za pridobitev potrdila jamči za podatke o instituciji in istovetnosti bodočih imetnikov in jih pooblašča za uporabo potrdil v imenu opravljanja nalog za institucijo.

(3) Imetniki potrdil so vedno fizične osebe. V primeru potrdila za informacijske sisteme, splošne nazive in podpis kode, je imetnik takega potrdila pooblaščen s strani predstojnika, v primeru potrdila za izdajatelja varnih časovnih žigov in druge overitelje pa predstojnik institucije izdajatelje varnih časovnih žigov. Imetniki so tako lahko:
- zaposleni,
- zaposleni, pooblaščeni za uporabo splošnih nazivov oz. organizacijske enote institucij,
- zaposleni, pooblaščeni za uporabo strežnikov (storitev oz. aplikacij), s katerim upravljajo institucije,
- zaposleni, pooblaščeni za uporabo programske opreme za podpis kode,
- predstojniki institucij izdajateljev varnih časovnih žigov in
- predstojniki institucij drugih overiteljev potrdil.

(4) Glede preklica kvalificiranih digitalnih potrdil ima predstojnik institucije enake pravice kot ostali imetniki potrdil iz iste institucije.

1.3.4 Tretje osebe

Tretje osebe so subjekti, ki se zanašajo na izdana potrdila izdajatelja SIGOV-CA.

1.3.5 Namen uporabe

(1) Osebna kvalificirana digitalna potrdila SIGOV-CA, izdana po pričujoči politiki, se lahko uporabljajo za[2]:
- 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.

(2) Spletna kvalificirana digitalna potrdila SIGOV-CA izdana po pričujoči politiki 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.

(3) Za potrdila, izdana na podlagi te politike, se zahteva uporaba sredstev za varno digitalno podpisovanje oz. varno hranjenje zasebnih ključev in potrdil, kot je to določeno v razd. 1.1.

(4) Potrdila, ki jih izdaja SIGOV-CA, se morajo uporabljati v skladu s to politiko in veljavno zakonodajo.

[2] Namen uporabe osebnih potrdil za izdajatelje TSA je omejen na digitalno podpisovanje.

1.4. Kontaktni podatki

Naslov:	SIGOV-CA Center Vlade Republike Slovenije za informatiko Langusova 4 1000 Ljubljana Slovenija
E-pošta:	sigov-ca@gov.si
Telefon:	01 4788 600
Fax:	01 4788 649
URL:	http://www.sigov-ca.gov.si
Dežurna tel. številka za preklice (24 ur vse dni v letu):	(**+386) 01 4788 777**

2. SPLOŠNE DOLOČBE

2.1. Obveznosti

2.1.1 Obveznosti 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 institucijah,
- zagotoviti delovanje prijavnih služb v skladu z določili SIGOV-CA in ostalimi veljavnimi predpisi,
- objavljati na svojih spletnih straneh vse informacije o tistih spremembah glede dejavnosti overitelja, ki kakorkoli vplivajo na imetnike potrdil, institucije in tretje osebe.

(2) 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. Vzdrževalna dela ali nadgradnje infrastrukture overitelja na CVI SIGOV-CA najavi vsaj tri (3) dni pred pričetkom del.

2.1.2 Obveznost prijavne službe

Prijavna služba je dolžna:
- preverjati istovetnost imetnikov oz. bodočih imetnikov in podatkov o instituciji,
- sprejemati zahtevke za storitve SIGOV-CA,
- preverjati zahtevke,
- izdajati potrebno dokumentacijo imetnikom oz. bodočim imetnikom in institucijam,
- posredovati zahtevke in ostale podatke na varen način na SIGOV-CA.

2.1.3 Obveznosti imetnika potrdila oziroma institucije

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

(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 SIGOV-CA,
- zasebne ključe 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 zasebnih ključev,
- po preteku oz. preklicu veljavnosti potrdila ravnati v skladu z obvestili SIGOV-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 SIGOV-CA oziroma zahtevati preklic,
- uporabljati potrdilo za namen in na način, ki je določen s politiko SIGOV-CA,
- uporabljati tako programsko in opremo, ki je v skladu z obvestili SIGOV-CA (z dovolj močnimi kriptografskimi moduli),
- skrbeti za originalno podpisane dokumente in arhiv teh dokumentov.

(4) Institucija je dolžna:
- skrbno prebrati to politiko in določila iz dogovora med institucijo in overiteljem na CVI pred podpisom zahtevka za pridobitev potrdila,
- zagotoviti, da imetniki potrdil za njegovo institucijo izpolnjujejo vse zahteve iz te politike in veljavnih predpisov,
- redno spremljati vsa obvestila SIGOV-CA,
- ravnati v skladu z obvestili, to politiko in dogovorom med institucijo 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 institucije, 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.

2.1.4 Obveznosti 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 SIGOV-CA, če izve, da so bili 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 preveriti, če potrdilo ni v registru preklicanih potrdil,
- v času uporabe potrdila preveriti, če je bil digitalni podpis kreiran v času veljavnosti in z ustreznim namenom potrdila,
- v času uporabe potrdila preveriti podpis izdajatelja potrdila SIGOV-CA, ki je objavljen v tej politiki in tudi na spletnih straneh SIGOV-CA oz. drugih izdajateljev potrdil overitelja na CVI,
- upoštevati druge določbe, v kolikor je z overiteljem sklenil dogovor o uporabi potrdil.

2.2. Odgovornosti

2.2.1 Odgovornost overitelja na CVI

(1) 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 pripadajoč v potrdilu navedenemu javnemu ključu,
- za enoličnost razločevalnih imen.

(2) Overitelj na CVI ni odgovoren za:
- uporabo potrdil za namen in na način, ki ni izrecno predviden v tej politiki oz. dogovoru med institucijo in SIGOV-CA,
- nepravilno ali pomanjkljivo varovanje gesel ali zasebnih ključev imetnikov, izdajanje zaupnih podatkov ali ključev tretjim osebam in neodgovorno ravnanje imetnika,
- kakršnokoli zlorabo oziroma vdor v informacijski sistem imetnika potrdila in s tem do podatkov o potrdilih s strani nepooblaščenih oseb,
- nedelovanje ali slabo delovanje informacijske infrastrukture imetnika potrdila ali tretjih oseb,
- nepreverjanje podatkov in veljavnosti potrdil v registru preklicanih potrdil,
- nepreverjanje časa veljavnosti potrdila,
- ravnanje imetnika potrdila, njegove institucije ali tretje osebe v nasprotju z obvestili SIGOV-CA, to politiko in drugimi predpisi,
- škodo, ki je bodisi posredno ali neposredno povzročena zato, ker je bila omogočena uporaba oz. zloraba imetnikovega potrdila nepooblaščenim osebam,
- škodo, ki izhaja iz potrdila, izdanega z napačnimi podatki in neverodostojnosti podatkov ali drugih dejanj imetnika ali institucije ali overitelja,
- uporabo potrdil ter veljavnost potrdil ob spremembah podatkov iz potrdila, elektronskih naslovov ali spremembah imen institucij ali imetnikov,
- izpad infrastrukture, ki ni v domeni upravljanja overitelja na CVI,
- podatke, ki se šifrirajo ali podpisujejo z uporabo potrdil,
- ravnanje imetnikov pri uporabi potrdil, in sicer tudi v primeru, če je imetnik ali tretja oseba spoštoval vsa določila te politike, obvestila SIGOV-CA ali druge veljavne predpise,
- uporabo in zanesljivost delovanja strojne in programske opreme imetnikov potrdil.

2.2.2 Odgovornost imetnika potrdila oziroma institucije

Institucija odgovarja za:

- nastalo škodo v primeru zlorabe potrdila od prijave preklica do preklica,
- vsako škodo, ki je bodisi posredno ali neposredno povzročena zato, ker je bila omogočena uporaba oz. zloraba imetnikovega potrdila s strani nepooblaščenih oseb,
- vsako drugo škodo, ki izvira iz nespoštovanja določil te politike in drugih obvestil SIGOV-CA.

2.3. Finančna odgovornost

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

2.4. Skladnost z veljavno zakonodajo

(1) Overitelj na CVI deluje v skladu z:
- Zakonom o elektronskem poslovanju in elektronskem podpisu (Ur.l. RS, št. 57/2000 in 30/2001),
- Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Ur.l. RS, št. 77/2000, 2/2001),
- in drugimi veljavnimi predpisi.

(2) Oblika in vsebina javnega dela notranjih pravil overitelja je usklajena z:
- RFC 2527 »Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework«,
- ETSI TS 101 456 »Policy requirements for certification authorities issuing qualified«.

2.5. Cenik

(1) Stroški upravljanja s potrdili se obračunavajo instituciji javne uprave po objavljenem ceniku na spletni strani http://www.sigov-ca.gov.si/cenik.htm.

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

2.6. Objave

Vse v zvezi z delovanjem SIGOV-CA, obvestila imetnikom in tretjim osebam SIGOV-CA objavlja javno na spletnih straneh SIGOV-CA.

2.6.1 Objava javnega imenik potrdil

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

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

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

(3) Struktura javnega imenika je objavljena v razd. 3.1.1.

(4) Potrdila se objavijo v javnem imeniku takoj po njihovem prevzemu, evidenčni podatki o potrdilu (imetnikov naziv, naslov e-pošte, serijska številka ...) pa že ob sami rezervaciji potrdila.

2.6.2 Objava 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=sigov-ca, cn=CRL*n*[3].

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

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

(3) Dostop do registra po protokolu http je:

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

(4) Preklicano potrdilo se v register uvrsti takoj po opravljenem preklicu.

(5) Opis registra preklicanih potrdil je v razd. 7.2.

2.7. Nadzor

(1) Izvajanje določb ZEPEP overitelja na CVI skladno z ZEPEP opravlja pristojna inšpekcijska služba.

(2) Overitelj na CVI javno objavi sklepe inšpekcijskega nadzorstva.

2.8. Varovanje podatkov

(1) Z vsemi osebnimi in zaupnimi podatki o imetnikih potrdil ali podatkov o institucijah, ki so nujno potrebni za storitve upravljanja s potrdili, overitelj ravna v skladu z veljavno zakonodajo.

(2) Overitelj na CVI ne posreduje drugih podatkov o imetnikih potrdil oz. institucijah, 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. predstojnik institucije, 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.

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

(3) Javno dostopni podatki so:
- potrdila, objavljena v javnem imeniku potrdil,
- register preklicanih potrdil,
- politike delovanje overitelje,
- izjave o delovanju overitelja,
- način varovanja osebnih podatkov,
- podatki o opravljenem inšpekcijskem nadzoru,
- in druga obvestila SIGOV-CA.

2.9. Določbe glede avtorskih, sorodnih in drugih pravic intelektualne lastnine

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. instituciji.

3. UGOTAVLJANJE ISTOVETNOSTI IMETNIKOV

3.1. Dodelitev imen

3.1.1 Vrste imen

(1) Razločevalno ime vsebuje enolične osnovne podatke o imetniku oz. nazivu, lahko tudi o instituciji in overitelju.

(2) Razločevalna imena potrdil SIGOV-CA so oblikovana v skladu s standardom X.501.

(3) V polju »Issuer« vseh potrdil SIGOV-CA je razločevalno ime izdajatelja SIGOV-CA, in sicer:
c=si,
o=state-institutions,
ou=SIGOV-CA

(4) Razločevalno ime vsebuje osnovne podatke o imetniku oz. nazivu, tudi o instituciji in overitelju. Razločevalno ime se glede na vrsto potrdila tvori po naslednjih pravilih[4]:

Vrsta potrdila	Razločevalno ime (polje »Subject«)
potrdilo izdajatelja SIGOV-CA	c=si, o=state-institutions, ou=SIGOV-CA
osebna potrdila za zaposlene in splošne nazive institucij oz. organizacijske enote institucij	c=si, o=state-institutions ou=certificates, ou=<kratko ime institucije>,

[4] Pomen posameznih podatkov je razložen v nadaljevanju. Pravila za tvorbo razločevalnega imena za osebna potrdila za strežnike in izdajatelja TSA objavi SIGOV-CA.

	cn=<naziv>, sn=<serijska številka>
spletna potrdila za zaposlene in splošne nazive institucij oz. organizacijske enote institucij	c=si, o=state-institutions, ou=web-certificates, cn=<naziv>, sn=<serijska številka>
spletna potrdila za strežnike	c=si, o=state-institutions, ou=web-certificates, ou=servers, cn=<ime DNS>, sn=<serijska številka>
spletna potrdila za podpis kode	c=si, o=state-institutions, ou=web-certificates, ou=codesign, cn=<naziv>, sn=<serijska številka>

3.1.2 Zahteve pri tvorbi razločevalnega imena

(1) Kratko ime institucije, ki je v skladu z določili razd. 3.1.1 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. institucijo,
- največja dolžina je lahko 63 znakov.

(2) Pod nazivom, ki je v skladu z določili razd. 3.1.1 vključeno v razločevalno ime, je v primeru potrdila:
- za zaposlene navedeno imetnikovo ime in priimek,
- za splošni naziv oz. organizacijske enote institucije naveden splošni naziv oz. organizacijska enota institucije.

(3) Največja dolžina naziva je 63 znakov.

(4) V primeru potrdila za strežnik mora biti navedeno ime strežnika ustrezno registrirano v registru DNS (angl. *Domain Name Syste*m).

3.1.3 Pravila za interpretacijo razločevalnih imen

(1) Interpretacija imen je navedena v razd. 3.1.1 in 3.1.2.

(2) Podatki o imetniku oz. nazivu in instituciji 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

3.1.4 Enoličnost razločevalnih imen

(1) Vsako potrdilo ima enolično razločevalno ime.

(2) Vsa potrdila imetnikov vključujejo še serijsko številko.

(3) Serijsko številko, ki je vključena v razločevalno ime, dodeli SIGOV-CA.

(4) 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 SIGOV-CA	1	
2.- 8. mesto	enolično število imetnika	/	
9. - 10. mesto	osebna potrdila	zaposleni	20
		splošni naziv	22
		strežnik	24
		izdajatelj TSA	26
	spletna potrdila	zaposleni	14
		splošni naziv	18
		strežnik	10
		podpis kode	19
11. – 12. mesto	zaporedna številka istovrstnega potrdila	/	
13. mesto	kontrolna številka	/	

3.1.5 Postopek v primeru sporov

(1) Določila glede imen so določena v razd. 3.1.1 in 3.1.2.

(2) SIGOV-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.

(3) V primeru potrdila za splošni naziv oz. organizacijske enote institucije si SIGOV-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.

3.1.6 Imena in zaščitene znamke

Določeno v razd. 3.1.2 in 3.1.5.

3.1.7 Metoda za dokazovanje posedovanja zasebnega ključa

Dokazovanje o posedovanju zasebnega ključa je zagotovljeno z varnimi protokoli ob prevzemu potrdil.

3.1.8 Preverjanje istovetnosti pravnih oseb

Pri ustreznih službah se preveri pravilnost podatkov o instituciji v javni upravi, za pravilnost podatkov pa jamči predstojnik institucije.

3.1.9 Preverjanje istovetnosti imetnikov

Institucija za svoje zaposlene osebe opravlja del nalog prijavnih služb po določilih SIGOV-CA, in sicer predstojnik institucije, kjer je bodoči imetnik potrdila zaposlen, jamči za istovetnost bodočega imetnika potrdila, ki ga je preveril v skladu z 31. členom in drugimi določili ZEPEP.

3.2. Preverjanje imetnikov ob menjavi ključev

Skladno z določili razd. 4.7.

3.3. Preverjanje imetnikov za ponovno pridobitev potrdila po preklicu

Skladno z določili razd. 3.1.9.

3.4. Preverjanje imetnikov ob zahtevi za preklic

Skladno z določili razd. 4.4.3.

4. UPRAVLJANJE S POTRDILI

4.1. Zahtevek za pridobitev potrdil

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

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

4.2. Pridobitev potrdil

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

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

(3) SIGOV-CA na podlagi odobrenega zahtevka (v primeru, da CVI nima zagotovljenih sredstev za institucijo tudi dogovora med institucijo in overiteljem na CVI) opravi rezervacijo potrdila najkasneje v desetih (10) dneh od odobritve zahtevka.

(4) SIGOV-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.

(5) Bodoči imetnik potrdila mora po prejemu referenčne številke in avtorizacijske kode potrdilo prevzeti v šestdesetih (60) dneh od rezervacije potrdila. Na zahtevo bodočega imetnika je možno čas za prevzem podaljšati za novih šestdesetih (60), sicer SIGOV-CA rezervacijo potrdila prekliče.

4.3. Prevzem potrdila

(1) Za prevzem potrdila bodoči imetnik potrebuje referenčno številko in avtorizacijsko kodo, ki mu ju izda SIGOV-CA, glej razd. 4.2.

(2) Način in podrobna navodila za prevzem vseh vrst potrdil, navedenih v razd. 1.1, je opisan na spletni strani http://www.sigov-ca.gov.si. Prav tako so na spletni strani objavljene tudi vse novosti v zvezi z načinom prevzema potrdil.

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

4.4. Preklic in suspenz potrdila

4.4.1 Razlogi za preklic

(1) Preklic potrdila morata imetnik ali predstojnik institucije 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 instituciji ali je prenehal z delom za institucijo ali ni več pooblaščen za opravljanje storitev z uporabo potrdila.

(2) Overitelj na CVI prekliče potrdilo tudi brez zahteve imetnika ali predstojnika institucije, takoj ko izve:
- da je imetnik potrdila prenehal delati v ali za institucijo,
- 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,
- da so se spremenile druge okoliščine, ki vplivajo na veljavnost potrdila,
- za neizpolnjevanje obveznosti imetnika oz. institucije iz te politike in dogovora med institucijo 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 SIGOV-CA prenehal 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.

4.4.2 Kdo zahteva preklic

Preklic potrdila lahko zahteva:
- pooblaščena oseba overitelja na CVI,
- predstojnik,
- imetnik,
- pristojno sodišče,
- sodnik za prekrške ali
- upravni organ.

4.4.3 Postopki za preklic

(1) Preklic lahko imetnik zahteva:
- osebno v rednem delovnem času,
- elektronsko 24 ur na dan vse dni v letu,
- telefonsko 24 ur na dan vse dni v letu.

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

(3) Če se preklic opravi:
- osebno: potrebno je izpolniti ustrezen zahtevek za preklic potrdila ter ga oddati na prijavno službo;
- elektronsko: imetnik ali predstojnik institucije morata na SIGOV-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 SIGOV-CA na dežurno telefonsko številko za preklice (glej razd. 1.4);
- telefonsko: imetnik mora poklicati na dežurno telefonsko številko za preklice (glej razd. 1.4), ob tem mora navesti geslo, ki ga je v ustreznem zahtevku za pridobitev potrdila imetnik podal kot geslo za preklic potrdila oz. ga je drugače varno posredoval SIGOV-CA. Brez gesla za preklic imetnik ne more telefonsko preklicati potrdila.

(4) O datumu ter času preklica, izdajatelju zahtevka za preklic ter vzrokih za preklic morata biti vedno obveščena imetnik in predstojnik.

4.4.4 Čas od prejetega zahtevka za preklic do izvedbe preklica

(1) Overitelj na CVI po prejemu veljavne zahteve za preklic najkasneje v štirih (4) urah prekliče potrdilo.

(2) V tem času je preklicano potrdilo dodano v register preklicanih potrdil in brisano iz javnega imenika potrdil[5].

4.4.5 Razlogi za suspenz

Ni podprto.

4.4.6 Kdo zahteva suspenz

Ni podprto.

4.4.7 Postopki za suspenz

Ni podprto.

4.4.8 Omejitve v zvezi s suspenzom

Ni podprto.

4.4.9 Čas veljavnosti registra preklicanih potrdil

Register preklicanih potrdil se osvežuje (za dostop do registra glej razd. 2.6.2):
- po vsakem preklicu potrdila,
- enkrat dnevno, če ni novih zapisov oz. sprememb v registru preklicanih potrdil, in sicer 24 ur po zadnjem osveževanju.

[5] V javnem imeniku ostanejo evidenčni podatki o potrdilu.

4.4.10 Zahteve po preverjanju registra preklicanih potrdil

Tretje osebe, ki se zanašajo na potrdilo, morajo pred uporabo preveriti najnovejši objavljeni register preklicanih potrdil. Zaradi verodostojnosti in celovitosti je vedno potrebno preveriti tudi verodostojnost registra, ki je digitalno podpisan s strani SIGOV-CA.

4.4.11 Sprotno preverjanje statusa potrdila[6]

Ni podprto.

4.4.12 Zahteve za sprotno preverjanje statusa potrdila

Ni podprto.

4.4.13 Drugi načini za objavo preklicanih potrdil

Ni podprto.

4.4.14 Zahteve za druge načine objave preklicanih potrdil

Ni podprto.

4.4.15 Posebne zahteve pri zlorabi zasebnega ključa

Ni določeno.

4.5. Postopki varnostnih pregledov

V skladu z Uredbo je to določeno v Interni politiki overitelja na CVI.

4.6. Arhiviranje podatkov

(1) SIGOV-CA skladno z Uredbo hrani naslednje podatke:

[6] OCSP, angl. Online Certificate Status Protocol

- dnevnike,
- zapisnike
- vsa dokazila o opravljenem preverjanju istovetnosti imetnikov in institucij,
- vse zahtevke;
- potrdila,
- politike delovanja,
- objave in obvestila SIGOV-CA,
- zasebne ključe za dešifriranje v skladu z razd. 6.1.1.

(2) Čas hrambe in način je v skladu z Uredbo in je določen v Interni politiki overitelja na CVI.

4.7. Podaljšanje veljavnosti potrdil

4.7.1 Podaljševanje veljavnosti osebnih potrdil

(1) Podaljševanje veljavnosti potrdil za osebna potrdila: generiranje novih parov ključev in podaljševanje veljavnosti osebnega potrdila se izvaja avtomatsko po varnem protokolu PKIX-CMP ob prvi uporabi potrdila imetnika z neposrednim dostop do infrastrukture SIGOV-CA v obdobju stotih (100) dni pred zadnjim dnem veljavnosti potrdila.

(2) Za podaljšana potrdila velja Politika SIGOV-CA, veljavna ob datumu generiranja novih parov ključev.

4.7.2 Podaljševanje veljavnosti spletnih potrdil

Spletna potrdila se ne podaljšujejo avtomatsko. Potrebno je ponoviti postopek za pridobitev novega potrdila.

4.8. Okrevalni načrt

V skladu z Uredbo je to določeno v Interni politiki delovanja overitelja na CVI.

4.9. Prenehanje delovanja SIGOV-CA

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

4.10. Regeneriranje ključev - velja za osebna potrdila[7]

4.10.1 Razlogi za regeneracijo

[7] Dodatna storitev overitelja, ki je RFC 2527 ne predvideva.

(1) Regeneriranje ključev za osebno potrdilo se izvede, če imetnik potrdila:
- pozabi geslo za dostop do zasebnih ključev,
- izgubi ali poškoduje nosilce za hrambo 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
- ali preklicem.

4.10.2 Kdo zahteva regeneracijo

Regeneracijo lahko zahteva imetnik potrdila.

4.10.3 Postopek za izdajo zahtevka za regeneracijo

(1) Regeneriranje ključev za potrdila se izvede na osnovi izpolnjenega zahtevka za regeneriranje ključev s strani imetnika potrdila, ki ga odda na prijavni službi SIGOV-CA.

(2) 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.

4.11. Odkrivanje kopije ključev za dešifriranje - velja za osebna potrdila[8]

4.11.1 Razlogi za odkrivanje kopije ključev za dešifriranje

(1) Overitelj na CVI odkrije kopijo ključev za dešifriranje le v izjemnih primerih, ko le-ti iz kakršnegakoli razloga niso dostopni, za dostop do podatkov, ki so zašifrirani in dostopni le z imetnikovim ključem za dešifriranje,

(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.

4.11.2 Kdo zahteva odkrivanje kopije ključev za dešifriranje

Kopijo ključev za dešifriranje lahko zahteva:
- predstojnik na podlagi zahtevka za odkrivanje kopije ključev za dešifriranje 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.

[8] Dodatna storitev overitelja, ki jo RFC 2527 ne predvideva.

4.11.3 Postopek ob zahtevku za odkrivanje kopije ključev za dešifriranje

(1) Predstojnik mora izpolniti zahtevka za odkrivanje kopije ključev za dešifriranje in ga na varen način posredovati na SIGOV-CA.

(2) 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.

4.12. Zahteve za podrejene overitelje

(1) Medsebojno razmerje 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.

4.13. 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.

5. VARNOSTNI NADZOR INFRASTRUKTURE

5.1. Fizični nadzor

(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) Podrobnejše določbe fizičnega varovanja so skladno z Uredbo določene v zaupnem delu notranjih pravil SIGOV-CA.

(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.

5.1.1 Šifrirni algoritmi, formati podatkov in protokoli infrastrukture overitelja na CVI[9]

(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 SIGOV-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.

5.2. Organizacija overitelja

(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	Vloga	Osnovne naloge	Število

9 Ta razdelek ni predviden v RFC 2527.

skupina			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 skladno z Uredbo določene z Interno politiko overitelja na CVI.

5.3. Nadzor nad osebjem

(1) Osebje overitelja ima skladno z zahtevami ZEPEP in Uredbo ustrezne kvalifikacije in redna izobraževanja.

(2) V skladu z Uredbo so podrobnejša določila glede nadzora osebja določena v Interni politiki overitelja na CVI.

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev ključev

6.1.1 Generiranje ključev

(1) Par ključev izdajatelja SIGOV-CA za podpisovanje je bil ustvarjen ob namestitvi programske opreme SIGOV-CA.

(2) Ključi imetnikov se generirajo v skladu s spodnjo tabelo.

tip potrdila	potrdilo	ključi se generirajo
osebno	par za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	pri imetniku[10]
	par za dešifriranje/šifriranje (potrdilo za šifriranje)	pri izdajatelju SIGOV-CA
spletno	par digitalno podpisovanje/overjanje in dešifriranje/šifriranje	pri imetniku[10]

[10] Za potrdila po politikah CP_{OID}: 1.3.6.1.4.1.6105.1.1.3 in CP_{OID}: 1.3.6.1.4.1.6105.1.2.3 na pametnih karticah oz. drugih varnih kriptografskih modulih

potrdilo za izdajatelja TSA	par za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	pri izdajatelju TSA

6.1.2 Dostava zasebnega ključa

Način varnega prenosa zasebnega ključa je podan v spodnji tabeli.

tip potrdila	potrdilo	ključ	dostava
osebno	par za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	zasebni ključ za podpisovanje	ni prenosa[11]
	par za dešifriranje/šifriranje (potrdilo za šifriranje)	zasebni ključ za dešifriranje	PKIX-CMP[12]
spletno	par digitalno podpisovanje/overjanje in dešifriranje/šifriranje	zasebni ključ	ni prenosa

6.1.3 Dostava javnega ključa izdajatelju potrdil

Imetniki v postopku prevzem dostavijo svoj javni ključ v podpis izdajatelju SIGOV-CA po protokolu PKIX-CMP za osebna potrdila in protokolu PKCS#10 za spletna potrdila.

6.1.4 Dostava izdajateljevega javnega ključa in dostava potrdil imetnikom[13]

(1) Potrdilo z javnim ključem izdajatelja SIGOV-CA je imetniku dostavljeno oz. tretjim osebam dostopno:
- v javnem imeniku x500.gov.si po protokolu LDAP (glej razd. 2.6.1),
- preko spletne strani https://www.sigov-ca.gov.si/cda-cgi/clientcgi?action=caCert,
- v obliki PEM na naslovu https://www.sigov-ca.gov.si/SIGOV-CA.pem,
- preko protokola PKIX-CMP za osebna potrdila in PKCS#7 za spletna potrdila.

(2) Potrdilo z imetnikovim javnim ključem je imetniku dostavljeno oz. tretjim osebam dostopno:
- preko protokola PKIX-CMP za osebna potrdila in PKCS#7 za spletna potrdila,
- v javnem imeniku x500.gov.si po protokolu LDAP,
- preko spletne strani https://www.sigov-ca.gov.si/cda-cgi/clientcgi?action=directorySearch.

6.1.5 Dolžina ključev

vrsta ključev	dolžina ključa po RSA[14] [bit]
potrdilo izdajatelja SIGOV-CA	2048

[11] Ključ se generira pri imetniku in se nikoli ne hrani pri izdajatelju SIGOV-CA.
[12] Prenos od izdajatelja SIGOV-CA do imetnika.
[13] RFC 2527 ne predvideva opisa načina dostave potrdil imetnikom.
[14] Vrednost pomeni min. predpisano dolžino. Overitelj si pridržuje pravico podaljšati dolžino ključa, v kolikor za to obstaja utemeljen razlog.

potrdilo za: • zaposlene • splošne nazive • strežnike • podpis kode	1024
potrdilo izdajatelja TSA	2048

6.1.6 Določanje parametrov javnih ključev

Parametri izdajateljevega ključa SIGOV-CA se določijo v programski in strojni opremi SIGOV-CA, parametri za ključe imetnikov pa v okolju v pristojnosti imetnikov.

6.1.7 Preverjanje parametrov

Kvaliteta parametrov ključa izdajatelja SIGOV-CA je zagotovljena s strani proizvajalca programske opreme z uporabo kvalitetnih generatorjev naključnih števil (angl. *random number generator*).

6.1.8 Programsko/strojno generiranje ključev

(1) Ključi izdajatelja SIGOV-CA so ustvarjeni v okolju infrastrukture, varovanem v skladu z FIPS 140-1 level 3. Podrobna določila so v skladu z Uredbo določena v Interni politiki overitelja na CVI.

(2) Programsko in strojno okolje, kjer se generirajo ključi, je v pristojnosti imetnika.

6.1.9 Nameni ključev in potrdil

(1) Namen uporabe ključev oz. potrdil je v skladu z X.509 v.3 določen v potrdilu v polju »keyUsage« in »extended keyUsage«.

(2) Za podpis potrdil in registra je namenjeno potrdilo izdajatelja SIGOV-CA.

(3) Uporaba različnih vrst potrdil imetnikov je določena v razd. 7.1.

6.2. Zaščita zasebnega ključa

6.2.1 Standardi za kriptografski modul

Zasebni ključ izdajatelja SIGOV-CA je zaščiten v programski opremi, ki je certificirana v skladu z FIPS 140-1 level 2 oz. Common Criteria EAL3.

6.2.2 Nadzor zasebnega ključa s strani pooblaščenih oseb

Določila glede dostopa do zasebnega ključa izdajatelja SIGOV-CA so v skladu z Uredbo določeni v Interni politiki overitelja na CVI.

6.2.3 Odkrivanje kopije zasebnega ključa (angl. Key Escrow)

(1) SIGOV-CA odkriva kopije zasebnega ključa za dešifriranje za osebna potrdila, za katere se skladno z določili iz razd. 6.1.1 generira ključ na strani izdajatelja SIGOV-CA.

(2) Postopek za odkrivanje kopije zasebnega ključa za dešifriranje za osebna potrdila je določen v razd. 4.11.

6.2.4 Varnostna kopija zasebnega ključa

Varnostne kopije zasebnih ključev za dešifriranje osebnih potrdil (skladno z določili iz razd. 6.1.1) se hranijo v šifriranih bazah SIGOV-CA, se redno obnavljajo in shranjujejo v dveh ločenih in fizično varovanih prostorih.

6.2.5 Arhiviranje zasebnega ključa

SIGOV-CA arhivira kopije zasebnih ključev za dešifriranje osebnih potrdil (skladno z določili iz razd. 6.1.1), kot je to določeno v razd. 4.6.

6.2.6 Zapis zasebnega ključa v kriptografski modul

(1) Zasebni ključi za dešifriranje osebnih potrdil imetnikov se iz mesta, kjer se ustvarijo, t.j. pri izdajatelju SIGOV-CA, prenesejo na imetnikovo stran po protokolu PKIX-CMP.

(2) Ostali zasebni ključi imetnikov se generirajo pri imetniku.

6.2.7 Postopek za aktiviranje zasebnega ključa

(1) Aktiviranje zasebnega ključa izdajatelja SIGOV-CA poteka v skladu z določili Interne politike overitelja na CVI.

(2) Imetniki dostopajo do svojega zasebnega ključa z geslom z ustreznimi aplikacijami.

6.2.8 Postopek za deaktiviranje zasebnega ključa

(1) Deaktivacija zasebnega ključa izdajatelja SIGOV-CA je zagotavljena z programsko opremo SIGOV-CA ob zaustavitvi le-te.

(2) Imetniki morajo uporabljati tako programsko okolje, ki ob odjavi ali po določenem pretečenem času deaktivira

dostop do njihovega zasebnega ključa.

6.2.9 Postopek za uničenje zasebnega ključa

(1) Postopek za uničenje zasebnega ključa izdajatelja SIGOV-CA poteka na varen način skladno z določili Interne politike overitelja na CVI. Zasebni ključ se uniči tako, da ga ni mogoče restavrirati.

(2) Uničenje zasebnih ključev na strani imetnikov je v pristojnosti imetnikov. Uporabiti morajo ustrezne aplikacije za varno brisanje potrdil.

6.3. Ostali aspekti upravljana ključev

Ni določeno.

6.3.1 Arhiviranje javnega ključa

Izdajatelj SIGOV-CA arhivira svoj javni ključ in javne ključe imetnikov, kot je podano v razd. 4.6.

6.3.2 Obdobje veljavnosti za javne in zasebne ključe

tip potrdila	št. ključev in potrdil	ključi	maks. veljavnost
osebno potrdilo	par za digitalno podpisovanje/overjanje (osebno potrdilo – za overjanje podpisa)	zasebni ključ za podpisovanje	3 leta
		javni ključ za overjanje podpisa	5 let
	par za dešifriranje/šifriranje (osebno potrdilo – za šifriranje)	zasebni ključ za dešifriranje	3 leta
		javni ključ za šifriranje	3 leta
spletno potrdilo	par digitalno podpisovanje/overjanje in dešifriranje/šifriranje	zasebni ključ	5 let
		javni ključ	5 let

6.4. Aktivacijski podatki

6.4.1 Generacija in inštalacija aktivacijskih podatkov

6.4.1.1 Aktivacijski podatki za prevzem potrdila

Aktivacijska podatka za prevzem potrdila, t.j. referenčna številka (angl. reference number) in avtorizacijska koda (angl. authorization code), ki jih imetniki potrebujejo za prevzem potrdil, se ustvarijo na strani SIGOV-CA. Številke in kode so unikatne.

6.4.1.2 Geslo za dostop do zasebnih ključev

Imetniki sami določijo geslo, s katerim zaščitijo dostop do svojih zasebnih ključev. SIGOV-CA priporoča uporabo varnih gesel:

- mešano uporaba velikih in malih črk, števil in posebnih znakov,
- geslo, dolžine vsaj 8 znakov,
- odsvetuje se uporabo besed, ki so zapisane v slovarjih.

6.4.2 Zaščita aktivacijskih podatkov

6.4.2.1 Kode za prevzem potrdila

(1) Kode za prevzem potrdila se generirajo varno pri izdajatelju SIGOV-CA.

(2) SIGOV-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 po priporočeni pošti.

(3) Do prevzema potrdila mora bodoči imetnik skrbno varovati kode za prevzem, po prevzemu potrdila postaneta kodi neuporabni in ju lahko zavrže.

6.4.2.2 Geslo za dostop do zasebnih ključev

(1) SIGOV-CA priporoča, da se geslo za dostop do zasebnega ključa shrani na varno mesto in da ima do njega dostop le imetnik.

(2) SIGOV-CA priporoča, da se geslo zamenja vsaj vsake 6 mesecev.

6.4.3 Drugi aspekti aktivacijskih podatkov

Ni določeno.

6.5. Varnostne zahteve za računalnike

6.5.1 Specifične tehnične varnostne zahteve za računalnike

V skladu z Uredbo je to določeno v Interni politiki overitelja na CVI.

6.5.2 Nivo varnostne zaščite računalnikov

V skladu z Uredbo je to določeno v Interni politiki overitelja na CVI.

6.6. Tehnični nadzor življenjskega cikla izdajatelja

6.6.1 Nadzor razvoja sistema

SIGOV-CA uporablja programsko opremo proizvajalca Entrust, ki je certificirana po Common Criteria EAL3 in FIPS 140-1 level 2.

6.6.2 Upravljanje varnosti

V skladu z Uredbo je to določeno v Interni politiki overitelja na CVI.

6.7. Varnostne kontrole računalniške mreže

V skladu z Uredbo je to določeno v Interni politiki overitelja na CVI.

6.8. Tehnične kontrole kriptografskih modulov

V skladu z Uredbo je to določeno v Interni politiki overitelja na CVI.

7. PROFIL POTRDIL IN REGISTRA PREKLICANIH POTRDIL

7.1. Profil potrdil

7.1.1 Splošno

(1) Na podlagi pričujoče politike SIGOV-CA izdaja in v tem razd. obravnava naslednje vrste potrdil za potrebe javne uprave[15]:

- osebna potrdila za zaposlene,
- spletna potrdila za zaposlene,
- osebna potrdila za splošne nazive institucij oz. organizacijske enote,
- spletna potrdila za splošne nazive institucij oz. organizacijske enote,
- osebna potrdila za strežnike,
- spletna potrdila za strežnike,
- spletna potrdila za podpis kode,
- osebna potrdila za izdajatelje varnih časovnih žigov.

(2) Potrdilo se izda na osnovi odobrenega zahtevka za pridobitev (glej razd. 5.1), v primeru, da CVI nima zagotovljenih sredstev za institucijo, pa tudi pisnega dogovora med institucijo in overiteljem na CVI (podrobnejši potek izdaje glede na vrsto potrdila je podan v razd. 4.2).

[15] Potrdilo izdajatelja SIGOV-CA je podrobno podano že v razd. 1.2.2.

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

(4) V potrdilu so navedeni podatki o imetniku in izdajatelju skladno s standardi iz razd. 5.1.1. Osnovni podatki v potrdilu so navedeni spodaj, ostali podatki pa so vsebovani glede na vrsto potrdila (glej razd. od 7.1.2 do 7.1.3):

Nazivi polj	*Nazivi polj - angleško*	*Vrednost oz. pomen*
Osnovna polja v potrdilu	Standard fields in cert.	
različica X.509	Version	2 (kar pomeni verzijo 3)
identifikacijska oznaka potrdila	Serial Number	<enolična interna številka potrdila> (celo število)
algoritem za podpis	Signature algorithm	sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5)
izdajatelj	Issuer	c=si, o=state-institutions, ou=sigov-ca
velja od - do	Validity	Not Before: <pričetek veljavnosti po GMT> Not After: <konec veljavnosti po GMT> V formatu *UTCTime*– oblika LLMMDDuummssZ
imetnik	Subject	<razločevalno ime imetnika, ki vključuje naziv imetnika (in institucijo in serijsko številko (*glej razd. 3.1.1)*> Zapisano kot PrintableString
algoritem za javni ključ	Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
javni ključ	Public Key (... bits)	< modul, eksponent,...>
Razširitve X.509v3	X509v3 extensions	
OID 2.5.29.17 alternativno ime	Subject Alternative Name	<elektronski naslov imetnika oz. splošnega naziva oz. strežnika>
OID 2.16.840.1.113730.1.1 netscapeCertType	NetscapeCertType	*odvisno od vrste potrdila, glej razd. 7.1.2 in 7.1.3*
OID 2.16.840.1.113730.1.2 izhodiščni URL	NetscapeBase URL	http://www.sigov-ca.gov.si/cda-cgi/
OID 2.16.840.1.113730.1.3 URL za preverjanje potrdila	NetscapeRevocation URL	clientcgi?action=checkRevocation&&CRL=cn=CRL1&serial=
OID 2.16.840.1.113730.1.13 opis potrdila	Netscape certificate comment	*odvisno od vrste potrdila, glej razd. 7.1.2 in 7.1.3*
OID 2.5.29.31 objava registra preklicanih potrdil	CRL Distribution Points	c=si, o=state-institutions, ou=sigov-ca, cn=CRL<zaporedna številka registra (glej razd. 2.6.2 in 7.2)> Url: ldap://x500.gov.si/ou=sigov-ca,o=state-institutions,c=si?certificateRevocationList?base Url: http://www.sigov-ca.gov.si/crl/sigov-ca.crl.
OID 2.5.29.16 zasebni ključ za podpisovanje velja do	Private Key Usage Period	*odvisno od vrste potrdila, glej razd. 7.1.2 in 7.1.3*
OID 2.5.29.15 uporaba ključa	Key Usage	*odvisno od vrste potrdila, glej razd. 7.1.2 in 7.1.3*
OID 2.5.29.37 razširjena uporaba	Extended Key Usage	*odvisno od vrste potrdila, glej razd. 7.1.2 in 7.1.3*
OID 2.5.29.35 identifikator izdajateljevega ključa	Authority Key Identifier	1EF8 D453 6BB3 8306 E904 0657 02F9 A5BF C658 3C72
OID 2.5.29.14 identifikator imetnikovega ključa	Subject Key Identifier	<identifikator imetnikovega ključa>

OID 2.5.29.32 politika, pod katero je bilo izdano potrdilo	certificatePolicies	Certificate Policy: PolicyIdentifier= *odvisno od vrste potrdila, glej razd. 7.1.2 in 7.1.3* [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.gov.si/ca/cps/
OID 2.5.29.19 osnovne omejitve	Basic Constraints	/
OID 1.2.840.113533.7.65.0 verzija Entrust	Entrust version extension	V5.0
Dodatna identifikacija (ni del digitalnega potrdila)		
razpoznavni odtis potrdila- MD5	Certificate Fingerprint – MD5	<razpoznavni odtis potrdila - MD5>
razpoznavni odtis potrdila – SHA1	Certificate Fingerprint – SHA1	<razpoznavni odtis potrdila - SHA1>

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

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

7.1.2 Lastnosti osebnega potrdila

(1) Vsak imetnik osebnega potrdila ima dva ločena para ključev - za digitalno podpisovanje/overjanje in za dešifriranje/šifriranje 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 dešifriranje/šifriranje sestavlja:
- zasebni ključ za dešifriranje (v nadaljevanju *ključ za dešifriranje*) ter
- javni ključ za šifriranje (v nadaljevanju *ključ za šifriranje*).

(2) Izdajatelju varnih časovnih žigov se podeli samo en par ključev, in sicer par ključev za digitalno podpisovanje/overjanje.

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

Par ključev za dešifriranje/šifriranje 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 SIGOV-CA. SIGOV-CA izda osebno potrdilo za šifriranje, katerega sestavni del je ključ za šifriranje. Osebno potrdilo za šifriranje se objavi v javnem imeniku potrdil.

(4) 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.

(5) Poleg osnovnih podatkov iz razd. 7.1.1 osebno potrdilo za šifriranje, objavljeno v javnem imeniku, vključuje še podatke, navedene v spodnji tabeli.

Podatek	Vrednost osebnega potrdila za šifriranje
	zaposleni, strežnik, splošni naziv
Namen uporabe, angl. *Key Usage*	Key Encipherment
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA, angl. *RSA Public Key*	dolžine 1024 bitov
Politika, pod katero je bilo izdano potrdilo (OID), in iz katere je razvidno tudi, da gre za kvalificirano potrdilo, angl. *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.1.2.3 Policy: 1.3.6.1.4.1.6105.1.4.1(*strežnik)*

(6) Poleg osnovnih podatkov iz razd. 7.1.1 osebno potrdilo za overjanje podpisa, ki ga hrani imetnik, vključuje še podatke, navedene v spodnji tabeli.

Podatek	Vrednost osebnega potrdila za overjanje podpisa	
	zaposleni, strežnik, splošni naziv,	strežnik TSA
Namen uporabe, angl. *Key Usage*	Digital Signature	
Razširjen namen uporabe, angl. *Extended Key Usage*	/	Time Stamping
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA, angl. *RSA Public Key*	dolžin ključa je 1024 bitov	dolžin ključa je 2048 bitov
Politika, pod katero je bilo izdano potrdilo (OID), in iz katere je razvidno tudi, da gre za kvalificirano potrdilo, angl. *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.1.2.3 Policy: 1.3.6.1.4.1.6105.1.4.1(*strežnik*)	Policy: 1.3.6.1.4.1.6105.1.5.1

(7) SIGOV-CA lahko izda tudi osebno potrdilo za strežnik. Tako potrdilo lahko vključuje tudi druge, tehnično pogojene podatke.

7.1.3 Lastnosti spletnega potrdila

(1) Vsak imetnik spletnega potrdila ima en par ključev, ki ga sestavljata zasebni in javni ključ. Par ključev se tvori z imetnikovo programsko opremo. Zasebni ključ ima samo imetnik. SIGOV-CA nikoli ne hrani in tudi nima dostopa do imetnikovega zasebnega ključa. Javni ključ se pošlje SIGOV-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 osnovnih podatkov iz razd. 7.1.1 vključuje spletno potrdilo še podatke, navedene v spodnji tabeli.

Podatek	Vrednost spletnega potrdila		
	zaposleni, splošni naziv	strežnik	podpis kode
Namen uporabe, angl. *Key Usage*	Digital Signature, Key Encipherment		Digital Signature
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA, angl. *RSA Public Key*	dolžin ključa je 1024 bitov		
Vrsta potrdila, angl. *Netscape Cert Type*	SSLClient, S/MIME	SSL Server	Object Signing
Politike, pod katero je bilo izdano potrdilo (OID), in iz katere je razvidno tudi, da gre za kvalificirano potrdilo, angl. *Certificate Policies*	Policy: 1.3.6.1.4.1.6105.1.1.3	Policy: 1.3.6.1.4.1.6105.1.3.1	

7.1.4 Zahteve za elektronski naslov

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

(2) SIGOV-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.

7.2. Profil registra preklicanih potrdil

7.2.1 Verzija

(1) Register preklicanih potrdil ustreza priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:1997, vključno z ver. 2.

(2) Register preklicanih potrdil je stalno dostopen v javnem imeniku potrdil (glej razd. 2.6.2):
- po protokolu LDAP in
- po protokolu HTTP.

(3) 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.

7.2.2 Vsebina registra in razširitve

Register preklicanih potrdil poleg ostalih podatkov v skladu s priporočilom X.509 vsebuje (osnovna polja in razširitve so podrobneje prikazana tabeli spodaj):
- identifikacijske oznake preklicanih potrdil in
- čas in datum preklica.

Naziv polja	Nazivi polj - angleško	Vrednost oz. pomen
Osnovna polja v CRL	angl. Standard fields in CRL	
V2	Version	1 (kar pomeni verzijo 2)
algoritem za podpis	Signature Algorithm	sha1WithRSAEncryption
izdajateljev podpis	Signature	podpis SIGOV-CA
razločevalno ime izdajatelja	Issuer	c=si, o=state-institutions, ou=sigov-ca
čas izdaje CRL	thisUpdate	Last Update: <čas izdaje po GMT>
čas izdaje naslednjega CRL	nextUpdate	Next Update: <čas naslednje izdaje po GMT>

identifikacijske oznake preklicanih potrdil in čas preklica	revokedCertificate	Serial Number: <identifikacijska oznaka preklicanega dig. potrdila> Revocation Date: <čas preklica po GMT>
Razširitve X.509v2 CRL	X509v2 CRL extensions	
identifikator izdajateljevega ključa	Authority Key Identifier (OID 2.5.29.35)	1EF8 D453 6BB3 8306 E904 0657 02F9 A5BF C658 3C72
številka za posamične registre (CRL1, CRL2,....)	CRLnumber (OID 2.5.29.20)	zaporedna številka posamičnega registra
	issuerAltName (OID 2.5.28.18)	*se ne uporablja*
	deltaCRLindicator (OID 2.5.29.27)	*se ne uporablja*
	issuingDistribuitionPoint (OID 2.5.29.28)	*se ne uporablja*

(2) Preklicana digitalna potrdila, katerih veljavnost je potekla, ostanejo objavljena v registru.

7.2.3 Objava registra CRL v javnem imeniku in v digitalnih potrdilih

SIGOV-CA objavlja register v javnem imeniku na strežniku X500.gov.si. Objavlja tako posamične registre kot tudi kombiniran oz. celotni register na enem mestu. Dostop in objavo prikazuje spodnja tabela[16].

objava CRL		dostop do CRL
posamični registri	c=si, o=state-institutions, ou=sigov-ca, cn=CRL<zaporedna številka registra>	• ldap://x500.gov.si/ cn=CRL<zaporedna številka registra>/ou=sigov-ca,o=state-institutions,c=si
celotni register	c=si, o=state-institutions, ou=sigov-ca (v polju "CertificationRevocationList")	• ldap://x500.gov.si/ou=sigov-ca,o=state-institutions, c=si?certificateRevocationList?base • http://www.sigov-ca.gov.si/crl/sigov-ca.crl

8. UPRAVLJANJE DOKUMENTACIJE

(1) Overitelj na CVI si pridržuje pravico do spremembe tega dokumenta brez predhodnega obveščanja imetnikov kvalificiranih digitalnih potrdil, v kolikor spremembe ne vplivajo na način upravljanja s potrdili.

(2) Spremembe politike overitelja na CVI, ki bistveno vplivajo na način upravljanja s potrdili, 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. Skladno z ZEPEP se prijava novosti storitev overitelja na CVI opravi tudi na pristojno ministrstvo za register overiteljev v Republiki Sloveniji.

(3) Veljavna kvalificirana digitalna potrdila pri tem ostanejo v veljavi do konca preteka veljavnosti po veljavni politiki ob njihovi izdaji oz. podaljšanju potrdil. Vsa kvalificirana digitalna potrdila izdana oz. podaljšana po tem datumu se obravnavajo po novi politiki.

[16] Potrdila, izdana po starejših politikah, t.j. OID=1.3.6.1.4.1.6105.1.1.1 in 1.3.6.1.4.1.6105.1.2.1, nimajo navedbe dostopa po protokolu http in zato avtomatski dostop za ta potrdila ni mogoč.

9. POJMI IN OZNAKE

9.1. Pomen pojmov

Izraz	Pomen
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 institucij oz. organizacijske enote institucij 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 SIGOV-CA.
Institucija	Institucija javne uprave, ki je v informacijsko-telekomunikacijskem omrežju državnih organov, katere predstojnik je naročnik digitalnih potrdil.
Izdajatelj varnih časovnih žigov	Zaupanja vredna institucija, ki izdaja varne časovne žige (TSA, angl. *Time Stamping Authority*).
Javni imenik potrdil	Javni imenik na CVI po standardu X.500, kjer so shranjena potrdila po standardu X.509 ver. 3.
Overitelj	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi. (CA, angl. *Certification Authority*).
PKIX-CMP	angl. Public Key Infrastructure X.509 - Certificate Management Protocols – protokol za izmenjavo ključev in upravljanje certifikatov
Politika SIGOV-CA	Javni del notranjih pravil Overitelja na CVI za izdajatelja kvalificiranih digitalnih potrdil SIGOV-CA za institucije javne uprave.
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)*. Kvalificirano digitalno potrdilo izpolnjuje zahteve iz 28. člena ZEPEP in ki ga izda overitelj, ki deluje v skladu z zahtevami iz 29. do 36. člena ZEPEP in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje.
Predstojnik	Fizična oseba, ki je pooblaščena za zastopanje institucije v pravnem prometu.
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 institucij. (*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.
RFC 2527	Priporočilo, ki določa elemente, ki naj bodo zajeti v politiki overitelja. V pripravi je dopolnitev tega dokumenta. (angl. *Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practice Framework*).
Serijska številka	Enolično 13-mestno število, ki ga potrdilu podeli SIGOV-CA. Prvo mesto določa potrdilo izdajatelja SIGOV-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.

9.2. Okrajšave

Okrajšava	Pomen
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*).
ETSI TS 101 456	Priporočila »Policy requirements for certification authorities issuing qualified certificates« za izdelavo politike za overitelja kvalificiranih digitalnih potrdil. (angl. *European Telecommunications Standards Institute).*
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*).
PKCS#7,	Priporočila (angl. *Public Key Cryptography Standards*) podjetje RSA Security za razvijalce računalniških sistemov, ki uporabljajo asimetrične kriptografske algoritme. • PKCS#7 določa sintakso za kriptografsko obdelane podatke, kot so digitalni

PKCS#10	podpisi in digitalne ovojnice. Uporablja se npr. za pošiljanje digitalnih potrdil in seznamov preklicanih potrdil. • PKCS#10 določa sintakso za zahtevek za overitev javnega ključa, imena in drugih atributov.
PKIX-CMP	Določa postopek za izmenjavo podatkov, ki se nanašajo na digitalna potrdila med entitetami infrastrukture overitelja. Zajema tudi de-facto standarda PKCS#7 in PKCS#10. Trenutno je objavljen kot RFC 2510, v pripravi pa je nova verzija. (angl. *Public Key Infrastructure (based on) X.509 - Certificate Management Protocols*).
RFC 2527	Priporočilo, ki določa elemente, ki naj bodo zajeti v poltiki overitelja. V pripravi je dopolnitev tega dokumenta. (angl. *Request for Comments*, *Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practice Framework*).
RA	Prijavna služba overitelja na Centru Vlade RS za informatiko. (angl. registration authority)
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).
TSA	Izdajatelj varnih časovnih žigov (TSA, angl. *Time stamping Authority*).
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 57/2000).