Overitelj na Ministrstvu za javno upravo

SIGEN-CA

# PROFILI KVALIFICIRANIH DIGITALNIH POTRDIL IN REGISTRA PREKLICANIH POTRDIL SIGEN-CA IN SIGOV-CA

*PRIPOROČILA ZA APLIKACIJE*

Verzija: 2.1

14. september 2009

**STANJE DOKUMENTA**

| | |
|---|---|
| **Namen dokumenta:** | Uporabnikom digitalnih potrdil SIGEN-CA in SIGOV-CA |
| **Kratek naziv:** | Profili kvalificiranih digitalnih potrdil in registra preklicanih potrdil SIGEN-CA in SIGOV-CA |
| **Vsebina:** | Glej "Vsebina" |
| **Status:** | Končna |
| **Verzija:** | 2.1 |
| **Datum verzije:** | 14. september 2009 |
| **Avtor:** | Overitelj na Ministrstvu za javno upravo |
| **Kontaktni podatki:** | Naslov: Overitelj na Ministrstvu za javno upravo<br>Tržaška cesta 21<br>1000 Ljubljana<br>Slovenija<br>Tel.: (+386) 01 4788 003<br>Fax.: (+386) 01 4788 649<br>Url.: http://www.gov.si/ca<br>E-pošta: sigen-ca@gov.si, sigov-ca@gov.si |

## VSEBINA

# 1. UVOD

Pričujoči dokument vključuje natančen opis digitalnih potrdil izdajateljev SIGEN-CA in SIGOV-CA. Opisuje profile vseh potrdil, s katerimi upravljata SIGEN-CA in SIGOV-CA v skladu s politikami delovanja. Dokument je v prvi vrsti namenjen razvijalcem aplikacij, njihovim snovalcem in samim lastnikom aplikacij oz. tretjim osebam, ki se zanašajo na digitalna potrdila izdajateljev SIGEN-CA in SIGOV-CA.

Pričujoči dokument temelji na objavljenih Politikah delovanja Overitelja na Ministrstvu za javno upravo in predstavlja del Priporočil za aplikacije e-storitev z varnostnimi zahtevami z uporabo kvalificiranih digitalnih potrdil:
**Profil kvalificiranih digitalnih potrdil in registra preklicanih potrdil izdajateljev SIGEN-CA in SIGOV-CA.**

Dokument je v nadaljevanju razdeljen v naslednja poglavja:
1. poglavje: kratek opis Overitelja kvalificiranih digitalnih potrdil in pravni vidiki uporabe kvalificiranih digitalnih potrdil,
2. poglavje: tehnični opis profila digitalnih potrdil SIGEN-CA in SIGOV-CA in registrov preklicanih digitalnih potrdil,
3. poglavje: načini dostopa do digitalnih potrdil,
4. poglavje: razlika med posebnimi in spletnimi digitalnimi potrdili,
5. poglavje: algoritmi, formati itd. infrastrukture Overitelja na MJU.

# 2. OVERITELJ NA MINISTRSTVU ZA JAVNO UPRAVO

Overitelj na Ministrstvu za javno upravo (MJU) izdaja kvalificirana digitalna potrdila in varne časovne žige, 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, 25/2004 in 98/2004) 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 MJU določa namen, delovanje in metodologijo upravljanja s kvalificiranimi digitalnimi potrdili, odgovornost overitelja na MJU ter zahteve, ki jih morajo izpolnjevati imetniki, tretje osebe, ki se zanašajo na kvalificirana digitalna potrdila, in drugi overitelji.

V okviru overitelja na MJU (http://www.gov.si/ca*)* delujeta 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 državne organe 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 MJU, so namenjena:
- za upravljanje, dostop in izmenjavo podatkov, s katerimi upravlja javna uprava,
- za varno elektronsko komuniciranje med imetniki kvalificiranih digitalnih potrdil overitelja na MJU in
- za storitve oz. aplikacije, za katere se zahteva uporaba digitalnih potrdil overitelja na MJU.

SIGEN-CA oz. SIGOV-CA izdajata dve skupini kvalificiranih digitalnih potrdil:
- *Spletna digitalna potrdila* so namenjena za uporabo v spletu po protokolih SSL oziroma TLS, S/MIME ter IPsec. Programska oprema za ta potrdila mora znati tvoriti par 2048-bitnih ključev po algoritmu RSA, zahtevek za digitalno potrdilo po priporočilu PKCS#10 ter vključiti potrdilo, ki ga dobi podpisano od SIGEN-CA oz. SIGOV-CA v formatu PKCS#7. To pa so priporočila, ki jih podpira večina brskalnikov in spletnih strežnikov ter nekateri produkti za vzpostavljanje VPN.
- *Posebna digitalna potrdila* so namenjena predvsem uslužbencem in aplikacijam v državni upravi oziroma pri poslovnih subjektih. Ta oprema mora podpirati ločena para ključev za podpisovanje in šifriranje dolžine 2048 bitov. Omogočati mora tudi regeneriranje zasebnega ključa za šifriranje, če postane nedostopen ali neuporaben iz kakršnegakoli razloga ("key-backup" zasebnega ključa za dešifriranje). To je potrebno zato, da ne bi izgubili pomembnih službenih zašifriranih podatkov. Uporabniki na svojih delovnih postajah uporabljajo programsko opremo Entrust Entelligence, ki deluje na operacijskem sistemu MS Windows, ali drugo programsko opremo »Entrust Ready«.

SIGOV-CA izdaja kvalificirana digitalna potrdila za državne organe:
- posebna kvalificirana digitalna potrdila za zaposlene v organizacijah,
- posebna kvalificirana digitalna potrdila za zaposlene v organizacijah z obvezno uporabo pametnih kartic,
- posebna kvalificirana digitalna potrdila za splošne nazive oz. organizacijske enote organizacij,
- posebna kvalificirana digitalna potrdila za splošne nazive oz. organizacijske enote organizacij z obvezno uporabo pametnih kartic,
- spletna kvalificirana digitalna potrdila za zaposlene v organizacijah,
- spletna kvalificirana digitalna potrdila za zaposlene v organizacijah z obvezno uporabo pametnih kartic,
- spletna kvalificirana digitalna potrdila za splošne nazive organizacij oz. organizacijske enote organizacij,
- spletna kvalificirana digitalna potrdila za splošne nazive organizacij oz. organizacijske enote organizacij z obvezno uporabo pametnih kartic,
- posebna kvalificirana digitalna potrdila za strežnike, s katerimi upravljajo organizacije,
- spletna kvalificirana digitalna potrdila za strežnike, s katerimi upravljajo organizacije,
- spletna kvalificirana digitalna potrdila za podpis kode za potrebe organizacije,
- kvalificirana digitalna potrdila za izdajatelje varnih časovnih žigov[1],
- kvalificirana digitalna potrdila za sisteme za sprotno preverjanje veljavnosti digitalnih potrdil[2],
- za druge overitelje digitalnih potrdil.

SIGEN-CA izdaja kvalificirana digitalna potrdila za poslovne subjekte in fizične osebe:
- posebna kvalificirana digitalna potrdila za zaposlene v organizacijah,
- posebna kvalificirana digitalna potrdila za splošne nazive oz. organizacijske enote organizacij,
- spletna kvalificirana digitalna potrdila za zaposlene v organizacijah,
- spletna kvalificirana digitalna potrdila za splošne nazive organizacij oz. organizacijske enote organizacij,
- posebna kvalificirana digitalna potrdila za strežnike, s katerimi upravljajo organizacije,
- spletna kvalificirana digitalna potrdila za strežnike, s katerimi upravljajo organizacije,
- spletna kvalificirana digitalna potrdila za podpis kode za potrebe organizacije,
- spletna kvalificirana digitalna potrdila za fizične osebe,
- za druge overitelje digitalnih potrdil.

Po Zakonu o elektronskem poslovanju in elektronskem podpisu (ZEPEP) ima elektronski podpis pravno veljavo, če je overjen s t.i. kvalificiranim digitalnim potrdilom (*člen 15: "Varen elektronski podpis, overjen s kvalificiranim potrdilom, je glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost.*"). Tak elektronski podpis oz. z njim podpisana pogodba v e-obliki je tako enakovredna lastnoročnemu podpisu na dokumentu v papirni obliki.

Overitelj na MJU izdaja kvalificirana digitalna potrdila, za katera velja najvišja stopnja varovanja in načela t.i. močne enkripcije ter deluje v skladu z ZEPEP in Uredbo, evropskimi direktivami ter drugimi veljavnimi predpisi.

## 3. PROFIL DIGITALNIH POTRDIL OVERITELJA NA MJU

### 3.1. Politike delovanja SIGEN-CA in SIGOV-CA in pripadajoče vrste potrdil

Politike delovanja predstavljajo javni del notranjih pravil overitelja. Aktualne in prejšnje verzije politik so objavljene na spletni strani http://www.gov.si/ca/cps.

Število ključev oz. digitalnih potrdil za posamezne vrste potrdil ter pripadajoče veljavnosti so sledeče.

[1] Potrdila za izdajatelje časovnih žigov se, kjer ni drugače navedeno, obravnavajo kot posebna kvalificirana digitalna potrdila.

[2] Potrdila za sisteme za sprotno preverjanje veljavnosti digitalnih potrdil se, kjer ni drugače navedeno, obravnavajo kot spletna kvalificirana digitalna potrdila.

| *tip potrdila* | | *št. ključev in potrdil* | *ključi* | *veljavnost* | *"key-backup"* |
|---|---|---|---|---|---|
| posebno potrdilo | 2 para ključev | par za digitalno podpisovanje/overjanje (posebno potrdilo – za verifikacijo podpisa) | zasebni ključ za podpisovanje | 3 leta | zasebni ključ za dešifriranje |
| | | | javni ključ za overjanje podpisa | 5 let | |
| | | par za šifriranje/dešifriranje (posebno potrdilo – za šifriranje) | zasebni ključ za dešifriranje | 3 leta | |
| | | | javni ključ za šifriranje | 3 leta | |
| spletno potrdilo | 1 par ključev | par za digitalno podpisovanje/overjanje in šifriranje/dešifriranje | zasebni ključ | 5 let | / |
| | | | javni ključ | 5 let | |

## 3.2. Način pridobitev digitalnih potrdil

Način pridobitev je določen s Politiko delovanja Overitelja. V spodnji tabeli so podani podatki v zvezi z opravljeno osebno identifikacijo imetnikov.

| *vrsta potrdila*[3] | *pridobitev* |
|---|---|
| SIGEN-CA za fizične osebe | osebna identifikacija imetnika na prijavni službi |
| SIGEN-CA za poslovne subjekte | osebna identifikacija pooblaščene osebe za oddajo zahtevka, za istovetnost imetnikov s podpisom jamči odgovorna oseba poslovnega subjekta |
| SIGOV-CA | osebna identifikacija pooblaščene osebe za oddajo zahtevka, za istovetnost imetnikov s podpisom jamči predstojnik institucije |

Podatki, ki se zbirajo ob postopku pridobitve:

| *vrsta potrdila*[4] | *zbiranje podatkov za pridobitev* |
|---|---|
| SIGEN-CA za fizične osebe | Glej zahtevek za PRIDOBITEV (http://www.sigen-ca.si/obrazci-fo.htm) |
| SIGEN-CA za poslovne subjekte | Glej zahtevek za PRIDOBITEV (http://www.sigen-ca.si/obrazci-org.htm) |
| SIGOV-CA | Glej zahtevek za PRIDOBITEV (http://www.sigov-ca.gov.si/obrazci.htm) |

Osebni podatki bodočih imetnikov (EMŠO, davčna številka), podatki o poslovnih subjektih (MŠO, davčna številka, odgovorna oseba poslovnega subjekta) se na prijavni službi preverijo v ustreznih registrih (RDZ; CRP).

## 3.3. Profil digitalnih potrdil

SIGEN-CA in SIGOV-CA izdajata potrdila po standardu X.509V3 v skladu s priporočili PKIX (angl. Public Key Infrastructure based on X.509). To je predvsem priporočilo RFC 5280 ter druga priporočila, ki jih pripravlja IETF (http://www.ietf.org/html.charters/pkix-charter.html).

V nadaljevanju so predstavljena polja potrdil SIGEN-CA in SIGOV-CA. Prikaz polj se v različnih brskalnikih razlikuje - nekateri namesto številke OID izpišejo pripadajoči tekst in vrednost v berljivi obliki, drugi pa navedejo zgolj številko OID in vrednost v šestnajstiškem sistemu. Nobena od razširitev ni kritična, kar pomeni, da jo aplikacija lahko ignorira, če je ne zna interpretirati.

### 3.3.1 Profil digitalnih potrdil SIGEN-CA

Potrdila SIGEN-CA vsebujejo polja, ki so prikazana v spodnji tabeli in razdelkih v nadaljevanju.

[3] V kolikor ni posebej navedeno, velja razločevalno ime za potrdila izdana po vseh pripadajočih politikah.

[4] V kolikor ni posebej navedeno, velja razločevalno ime za potrdila izdana po vseh pripadajočih politikah.

| Nazivi polja | Vrednost oz. pomen |
|---|---|
| Osnovna polja v potrdilu | |
| Različica,<br>angl. *Version* | 2 (*kar pomeni verzijo 3*) |
| Identifikacijska oznaka potrdila,<br>angl. *Serial Number* | *enolična interna številka potrdila-celo število* |
| Algoritem za podpis,<br>angl. *Signature algorithm* | sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5) |
| Izdajatelj,<br>angl. *Issuer* | c=si, o=state-institutions, ou=sigen-ca |
| Veljavnost,<br>angl. *Validity* | Not Before: <*pričetek veljavnosti po GMT*><br>Not After: <*konec veljavnosti po GMT*><br>*v formatu UTCTime* <LLMMDDuummssZ> |
| Imetnik,<br>angl. *Subject* | *razločevalno ime imetnika, odvisno od vrste potrdila* |
| Algoritem za javni ključ,<br>angl. *Subject Public Key Algorithm* | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ,<br>angl. *Public Key (... bits)* | *modul, eksponent,...* |
| Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA,<br>angl. *RSA Public Key* | *dolžina ključa je min. 2048 bitov* |
| Razširitve X.509v3 | |
| Alternativno ime OID 2.5.29.17,<br>angl. *Subject Alternative Name* | *elektronski naslov imetnika* |
| Objava registra preklicanih potrdil, OID 2.5.29.31,<br>angl. *CRL Distribution Points* | c=si,<br>o=state-institutions,<br>ou=sigen-ca,<br>cn=CRL<*zaporedna številka registra*<br><br>Url: ldap://x500.gov.si/ou=sigen-ca,o=state-institutions,c=si?certificateRevocationList?base<br><br>Url: http://www.sigen-ca.si/crl/sigen-ca.crl |
| Zasebni ključ za podpisovanje velja do, OID 2.5.29.16,<br>angl. *Private Key Usage Period* | *odvisna od vrste potrdila* |
| Uporaba ključa, OID 2.5.29.15,<br>*angl. Key Usage* | *odvisna od vrste potrdila* |
| Razširjena uporaba,<br>OID 2.5.29.37,<br>angl. *Extended Key Usage* | *odvisno od vrste potrdila* |
| Identifikator izdajateljevega ključa,<br>OID 2.5.29.35,<br>angl. Auth*ority Key Identifier* | 717B 8A06 1F31 0555 AB60 1277 4720 1E03 8818 EC89 |
| Identifikator imetnikovega ključa,<br>OID 2.5.*29.14,*<br>*angl. Subject Key Identifier* | *identifikator imetnikovega ključa* |

| | |
|---|---|
| Politike, pod katerimi je bilo izdano potrdilo,<br>OID 2.5.29.32,<br>angl. *certificatePolicies* | Certificate Policy:<br>PolicyIdentifier= *odvisno od vrste potrdila, glej razd.* ***Napaka! Vira sklicevanja ni bilo mogoče najti.*** *in* ***Napaka! Vira sklicevanja ni bilo mogoče najti.***<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>http://www.ca.gov.si/cps/ |
| Oznaka kvalificiranega potrdila,<br>OID 1.3.6.1.5.5.7.1.3,<br>angl. *qcStatement* | *odvisno od vrste potrdila* |
| Osnovne omejitve, OID 2.5.29.19,<br>angl. *Basic Constraints* | *se ne uporablja* |
| OID 1.2.840.113533.7.65.0<br>Verzija Entrust<br>angl. *Entrust version extension* | V7.1 |
| Dodatna identifikacija (ni del digitalnega potrdila) | |
| razpoznavni odtis potrdila-SHA1<br>angl. *Certificate Fingerprint – SHA1* | *razpoznavni odtis potrdila po SHA1* |
| razpoznavni odtis potrdila-SHA256<br>angl. *Certificate Fingerprint – SHA256* | *razpoznavni odtis potrdila po SHA256* |

### 3.3.2 Profil digitalnih potrdil SIGOV-CA

Potrdila SIGOV-CA vsebujejo polja, ki so prikazana v spodnji tabeli in razdelkih v nadaljevanju.

| Nazivi polja | Vrednost oz. pomen |
|---|---|
| Osnovna polja v potrdilu | |
| Različica,<br>angl. *Version* | 2 (*kar pomeni verzijo 3*) |
| Identifikacijska oznaka potrdila,<br>angl. *Serial Number* | *enolična interna številka potrdila-celo število* |
| Algoritem za podpis,<br>angl. *Signature algorithm* | sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5) |
| Izdajatelj,<br>angl. *Issuer* | c=si, o=state-institutions, ou=sigov-ca |
| Veljavnost,<br>angl. *Validity* | Not Before: <*pričetek veljavnosti po GMT*><br>Not After: <*konec veljavnosti po GMT*><br>*v formatu UTCTime* <LLMMDDuummssZ> |
| Imetnik,<br>angl. *Subject* | *razločevalno ime imetnika, odvisno od vrste potrdila* |
| Algoritem za javni ključ,<br>angl. *Subject Public Key Algorithm* | rsaEncryption (OID 1.2.840.113549.1.1.1) |
| Javni ključ,<br>angl. *Public Key (... bits)* | *modul, eksponent,...* |
| Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA,<br>angl. *RSA Public Key* | *dolžina ključa je min 2048 bitov* |
| Razširitve X.509v3 | |
| Alternativno ime OID 2.5.29.17,<br>angl. *Subject Alternative Name* | *elektronski naslov* |

| | |
|---|---|
| Objava registra preklicanih potrdil, OID 2.5.29.31,<br>angl. *CRL Distribution Points* | c=si,<br>o=state-institutions,<br>ou=sigov-ca,<br>cn=CRL<*zaporedna številka registra*<br><br>Url: ldap://x500.gov.si/ou=sigov-ca,o=state-institutions,c=si?certificateRevocationList?base<br><br>Url: http://www.sigov-ca.gov.si/crl/sigov-ca.crl |
| Zasebni ključ za podpisovanje velja do,<br>OID 2.5.29.16,<br>angl. *Private Key Usage Period* | *odvisna od vrste potrdila* |
| Uporaba ključa, OID 2.5.29.15,<br>*angl. Key Usage* | *odvisna od vrste potrdila* |
| Razširjena uporaba,<br>OID 2.5.29.37,<br>angl. *Extended Key Usage* | *odvisno od vrste potrdila* |
| Identifikator izdajateljevega ključa,<br>OID 2.5.29.35,<br>angl. Auth*ority Key Identifier* | 1EF8 D453 6BB3 8306 E904 0657 02F9 A5BF C658 3C72 |
| Identifikator imetnikovega ključa,<br>OID 2.5.*29.14,*<br>*angl. Subject Key Identifier* | *identifikator imetnikovega ključa* |
| Politika, pod katero je bilo izdano potrdilo,<br>OID 2.5.29.32,<br>angl. *certificatePolicies* | Certificate Policy:<br>PolicyIdentifier= *odvisno od vrste potrdila, glej razd.* ***Napaka! Vira sklicevanja ni bilo mogoče najti.*** *in* ***Napaka! Vira sklicevanja ni bilo mogoče najti.***<br>[1,1]Policy Qualifier Info:<br>Policy Qualifier Id=CPS<br>Qualifier:<br>http://www.ca.gov.si/cps/ |
| Oznaka kvalificiranega potrdila,<br>OID 1.3.6.1.5.5.7.1.3,<br>angl. *qcStatement* | *odvisna od vrste potrdila* |
| Osnovne omejitve, OID 2.5.29.19,<br>angl. *Basic Constraints* | *se ne uporablja* |
| OID 1.2.840.113533.7.65.0<br>Verzija Entrust<br>angl. *Entrust version extension* | V7.1 |
| Dodatna identifikacija (ni del digitalnega potrdila) | |
| razpoznavni odtis potrdila-SHA1<br>angl. *Certificate Fingerprint – SHA1* | *razpoznavni odtis potrdila po SHA1* |
| razpoznavni odtis potrdila-SHA256<br>angl. *Certificate Fingerprint – SHA256* | *razpoznavni odtis potrdila po SHA256* |

### 3.3.3 Enolično razločevalno ime digitalnih potrdil SIGOV-CA, SIGEN-CA in serijske številke

Digitalna potrdila vsebujejo razločevalno ime tako za izdajatelja potrdil v poljih "issuer" in za imetnike v poljih "subject". Razločevalna imena so oblikovana v skladu s standardom X.501, za posamezno vrsto digitalnih potrdil pa so podana v spodnji tabeli. Nekateri brskalniki namesto sn (*serial Number*) za serijsko številko navajajo OID 2.5.4.5.

| *vrsta potrdila*[5] | *razločevalno ime* |
|---|---|
| potrdilo izdajatelja SIGEN-CA | c=si,<br>o=state-institutions, |

[5] V kolikor ni posebej navedeno, velja razločevalno ime za potrdila izdana po vseh pripadajočih politikah razen izjem, ki so posebej označena.

| | |
|---|---|
| | ou=sigen-ca |
| SIGEN-CA spletna za fizične osebe | c=si,<br>o=state-institutions,<br>ou=sigen-ca,<br>ou=individuals,<br>cn=<ime in priimek>,<br>sn=<serijska številka> |
| posebna potrdila za zaposlene in splošne nazive organizacij oz. organizacijske enote organizacij | c=si,<br>o=state-institutions,<br>ou=sigen-ca,<br>ou=companies (*ali* ou=org)<br>ou=<oznaka organizacije>-<davčna št. organizacije>,<br>cn=<naziv>,<br>sn=<serijska številka> |
| spletna potrdila za zaposlene in splošne nazive organizacij oz. organizacijske enote organizacij | c=si,<br>o=state-institutions,<br>ou=sigen-ca,<br>ou=companies-web (*ali* ou=org-web)<br>ou=<oznaka organizacije>-<davčna št. organizacije>,<br>cn=<naziv>,<br>sn=<serijska številka> |
| spletna potrdila za strežnike | c=si,<br>o=state-institutions,<br>ou=sigen-ca,<br>ou=companies-web (*ali* ou=org-web)<br>ou=< oznaka organizacije>-<davčna št. organizacije>,<br>cn=<naziv>,<br>sn=<serijska številka> |
| spletna potrdila za podpis kode | c=si,<br>o=state-institutions,<br>ou=sigen-ca,<br>ou=companies-web (*ali* ou=org-web)<br>ou=<oznaka organizacije>-<davčna št. organizacije>,<br>cn=<naziv>,<br>sn=<serijska številka> |
| potrdilo izdajatelja SIGOV-CA | c=si,<br>o=state-institutions,<br>ou=SIGOV-CA |
| posebna potrdila za zaposlene in splošne nazive organizacij oz. organizacijske enote organizacij | c=si,<br>o=state-institutions,<br>ou=certificates,<br>ou=<oznaka organizacije>,<br>cn=<naziv>,<br>sn=<serijska številka> |
| spletna potrdila za zaposlene in splošne nazive organizacij oz. organizacijske enote organizacij | c=si,<br>o=state-institutions,<br>ou=web-certificates,<br>cn=<naziv>,<br>sn=<serijska številka> |
| spletna potrdila za strežnike | c=si,<br>o=state-institutions,<br>ou=web-certificates,<br>ou=servers,<br>cn=<naziv>,<br>sn=<serijska številka> |
| spletna potrdila za podpis kode | c=si,<br>o=state-institutions,<br>ou=web-certificates, |

| | |
|---|---|
| | ou=codesign,<br>cn=<naziv>,<br>sn=<serijska številka> |

**Opozoriti je potrebno sledeče:**

- imena (ime, priimek, splošni nazivi, oznake organizacij in institucij) lahko vključujejo črke angleške abecede, številke in naslednje posebne znake:
  - . : & * @ ! $ #
- vrstni red v razločevalnem imenu je zgolj ilustrativen in je odvisen od orodja oz. aplikacije. Prav tako se namesto ločila "," lahko uporablja oz. prikaže drug znak, npr. "\".

### 3.3.3.1 Serijska številka digitalnega potrdila

Vsakemu digitalnemu potrdilu je v razločevalnem imenu dodeljena serijska številka. Serijska številka je 13-mestno število, sestavljeno na naslednji način:

1: oznaka izdajatelja (za SIGOV-CA: 1, SIGEN-CA: 2)
2-8: št. imetnika (xxxxxxx)
9-10: tip potrdila (podane v spodnji tabeli)
11-12: zaporedna št. istovrstnega potrdila (yy)
13: kontrolno število v skladu s 4. členom Uredbe o načinu določanja osebne identifikacijske številke- Ur.l.RS, št. 8-345/99 (z).

| *vrsta potrdila* | *serijska številka* |
|---|---|
| SIGEN-CA spletna za fizične osebe | 2xxxxxx12yyz |
| SIGEN-CA spletna za zaposlene | 2xxxxxx16yyz |
| SIGEN-CA spletna za splošne nazive | 2xxxxxx18yyz |
| SIGEN-CA spletna za strežnik | 2xxxxxx10yyz |
| SIGEN-CA spletna za podpis kode | 2xxxxxx19yyz |
| SIGEN-CA posebna za zaposlene | 2xxxxxx20yyz |
| SIGEN-CA posebna za splošne nazive | 2xxxxxx22yyz |
| SIGEN-CA posebna za strežnik | 2xxxxxx24yyz |
| SIGOV-CA spletna za zaposlene | 1xxxxxx14yyz |
| SIGOV-CA spletna za splošne nazive | 1xxxxxx18yyz |
| SIGOV-CA spletna za strežnik | 1xxxxxx10yyz |
| SIGOV-CA spletna za podpis kode | 1xxxxxx19yyz |
| SIGOV-CA posebna za zaposlene | 1xxxxxx20yyz |
| SIGOV-CA posebna za splošne nazive | 1xxxxxx22yyz |
| SIGOV-CA posebna za strežnik | 1xxxxxx24yyz |
| SIGOV-CA posebna za strežnike za TSA | 1xxxxxx26yyz |
| SIGOV-CA spletna za strežnike za OCSP | 1xxxxxx18yyz |

**Opozoriti je potrebno sledeče:**

- v primeru službenih potrdil (SIGOV-CA, poslovni subjekti SIGEN-CA) je št. imetnika (xxxxxxx) enaka za vsa digitalna potrdila tega imetnika znotraj ene organizacije/institucije,
- v primeru potrdil za fizične osebe je št. imetnika (xxxxxxx) enaka za vsa spletna digitalna potrdila SIGEN-CA za to fizično osebo.

### 3.3.3.2 Serijska številka vs. identifikacijska oznaka potrdila

Razlike med serijsko številko in identifikacijsko oznako so sledeče:

- Identifikacijska oznaka je interna enolična številka potrdila, ki se dodeli avtomatsko pri postopku generiranja ključa oz. prevzemu digitalnega potrdila skladno s standardom X.509V.3. V registru CRL se preklicano potrdilo identificira samo s to oznako.
- Serijska številka pa je del razločevalnega imena in jo dodeljena na podlagi namena in vrste potrdil. Format serijske številke je določen s politikami delovanja overitelja na MJU. Serijska številka je namenjena predvsem za namen avtentikacije oz. vzpostavitve sheme dostopnih pravic.

## 3.4. Register preklicanih digitalnih potrdil SIGOV-CA, SIGEN-CA

SIGEN-CA in SIGOV-CA izdajata register preklicanih potrdil po standardu X.509v2 CRL. Vsebuje sledeča polja:

CRL za SIGEN-CA:

| Nazivi polj | Nazivi polj - angleško | Vrednost oz. pomen |
|---|---|---|
| Osnovna polja v CRL | Standard fields in CRL | |
| X.509 V2 za CRL | Version | 1 (kar pomeni verzijo 2) |
| algoritem za podpis | Signature Algorithm | sha1WithRSAEncryption |
| izdajateljev podpis | Signature | podpis SIGEN-CA |
| razločevalno ime izdajatelja | Issuer | c=si, o=state-institutions, ou=sigen-ca |
| čas izdaje registra | thisUpdate ozir. Effective Date ozir. Last Update | Last Update: <čas izdaje po GMT> |
| čas izdaje naslednjega registra | nextUpdate | Next Update: <čas naslednje izdaje po GMT> |
| identifikacijske oznake preklicanih potrdil in čas preklica | revokedCertificate | Serial Number: <identifikacijska oznaka preklicanega dig. potrdila><br>Revocation Date: <čas preklica po GMT> |
| Razširitve X.509v2 CRL | X509v2 CRL extensions | |
| identifikator izdajateljevega ključa | Authority Key Identifier (OID 2.5.29.35) | 717B 8A06 1F31 0555 AB60 1277 4720 1E03 8818 EC89 |
| 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* |

CRL za SIGOV-CA:

| Nazivi polj | Nazivi polj - angleško | Vrednost oz. pomen |
|---|---|---|
| Osnovna polja v CRL | 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><br>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* |

### 3.4.1 Objava registra CRL v javnem imeniku in v digitalnih potrdilih

SIGEN–CA in SIGOV-CA objavljata register v javnem imeniku na strežniku X500.gov.si, dostopna pa sta po protokolih LDAP in HTTP. Objavljata tako posamične registre kot tudi kombiniran oz. celotni register na enem mestu. Dostop in objavo prikazuje spodnja tabela.

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

### 3.4.2 Čas objave CRL

CRL se v imeniku objavlja enkrat dnevno oziroma po vsakem preklicu digitalnega potrdila. Polje "nextUpdate" tako dejansko označuje veljavnost registra (3 dni) in ne čas naslednje objave registra. Novi CRL se torej vedno objavi pred iztekom starega, v primeru preklica potrdila najkasneje v 4 urah po prejetem zahtevku za preklic. Kako pogosto se izvaja osveževanje lokalne kopije, je stvar odločitve lastnika aplikacije oz. tretje osebe. Po naših izkušnjah je lahko dober kompromis osveževanje CRL enkrat do nekajkrat na uro. Seveda pa je pri tem pomembno natančno proučiti in določiti politiko oz. pogoje v zvezi s storitvijo oz. transakcijo (ali obstaja možnost zlorabe zaradi neažurnega CRL oz. kakšna je lahko škoda, ...), upoštevati pa je treba tudi obremenjenost strežnikov, ipd.

### 3.4.3 CRL in pretečena potrdila

Preklicana digitalna potrdila, katerim veljavnost je potekla, se odstranijo iz celotnega registra CRL, ostanejo pa zapisana v posamičnih registrih.

### 3.4.4 Strežnik za OCSP

Sprotno preverjanje preklicanih potrdil po protokolu OCSP (angl. *On-line Certificate Status Protocol*) zaenkrat še ni omogočeno, vendar v prihodnje načrtujemo tudi uvedbo tega sistema.

### 3.5. Dostop do osebnih podatkov imetnikov digitalnih potrdil (prevajalna tabela baze MULTI)

Imetnik digitalnega potrdila je nedvoumno določen z razločevalnim imenom oz. s serijsko številko digitalnega potrdila. Digitalna potrdila pa ne vključujejo osebnih podatkov njihovih imetnikov. Podatki o imetnikih potrdil (osebni podatki) in podatki o organizacijah so zbrani v prevajalni tabeli baze MULTI, s katero upravlja MJU in enolično povezani s serijsko številko digitalnega potrdila. Dostop do teh podatkov je ob ustrezni zakonski podlagi mogoč za institucije javne uprave, ostali uporabniki pa lahko preko spletne strani https://storitve-ca.gov.si/ preverjajo identifikacijske podatke imetnikov potrdil, vezane na digitalno potrdilo, in sicer bodisi preko spletnega obrazca bodisi preko spletne storitve.

| *vrsta potrdila*[6] | *podatki v prevajalni tabeli MULTI* |
|---|---|
| SIGEN-CA za fizične osebe | serijska številka – davčna št. imetnika – EMŠO imetnika |
| SIGEN-CA za zaposlene | serijska številka – davčna št. imetnika – EMŠO imetnika – davčna št. organizacije – matična št. organizacije |
| SIGEN-CA za splošne nazive | serijska številka – davčna št. skrbnika – EMŠO skrbnika – davčna št. organizacije – matična št. organizacije |
| SIGEN-CA za strežnike | serijska številka – davčna št. skrbnika – EMŠO skrbnika – davčna št. organizacije – matična št. organizacije |
| SIGOV-CA za zaposlene | serijska številka – davčna št. imetnika – EMŠO imetnika (neobvezno) |
| SIGOV-CA za splošne nazive | serijska številka – davčna št. skrbnika – EMŠO skrbnika (neobvezno) |
| SIGOV-CA za strežnike | serijska številka – davčna št. skrbnika – EMŠO skrbnika (neobvezno) |

## 4. HRAMBA DIGITALNIH POTRDIL

Na strani uporabnika so kriptografski ključi in digitalna potrdila hranjeni na različne načine, ki so odvisni od "platforme", programske opreme in strojne opreme, ki jo je uporabnik uporabil za tvorjenje ključev in pridobitev digitalnega potrdila. Najpogostejši načini hranjenja so:

- **Entrust profil** - posebna digitalna potrdila prevzeta z programsko opremo Entrust Entelligence,
- **Microsoft Certificate Store** – spletna digitalna potrdila prevzeta z brskalnikom Microsoft IE,
- **Network Security Services (NSS)** – spletna digitalna potrdila prevzeta z brskalniki Netscape 6/7, Mozilla…,
- **Pametne kartice** – digitalna potrdila prevzeta z Entrust Entelligence, brskalniki Microsoft IE, Mozilla...

Način dostopa do kriptografskih ključev in digitalnih potrdil oziroma kriptografskih servisov je za posamezen način hranjenja možen preko aplikativnih programskih vmesnikov (API):

| *hramba* | *API* |
|---|---|
| Entrust profil | Entrust Authority™ Toolkits<br>(https://www.entrust.com/support/toolkits/index.htm) |
| Microsoft Certificate Store | Microsoft CryptoAPI |
| Network Security Services (NSS) | Mozilla NSS Open Source Crypto Libraries |
| Pametne kartice | PKCS#11<br>Microsoft CryptoAPI |

### 4.1. Entrust profil

Entrust profil je format, ki ga uporabljajo Entrust in Entrust/Ready aplikacije. V Entrust profilu so shranjeni podatki o uporabnikovi identiteti, dešifrirni ključ, zgodovina dešifrirnih ključev, podpisni ključ, uporabnikova digitalna potrdila in overiteljevo digitalno potrdilo. Entrust profil zagotavlja zaupnost in integriteto podatkov vsebovanih v profilu. Možno ga je hraniti v shrambi brskalnika MS Internet Explorer ali pa na pametni kartici. Entrust aplikacije uporabljajo standard PKCS#11 za dostop do pametne kartice.

[6] V kolikor ni posebej navedeno, velja razločevalno ime za potrdila izdana po vseh pripadajočih politikah.

### 4.2. PKCS #11

PKCS #11 (Public Key Cryptographic Standard 11) definira aplikativni programski vmesnik (API), imenovan tudi "Cryptoki". PKCS#11 vmesnik omogoča aplikacijam dostop do kriptografskih servisov (npr. šifriranje, dešifriranje, digitalni podpis, generiranje ključev, ...) na pametni kartici. Razvit je bil v RSA Laboratories v sodelovanju z drugimi podjetji in je postal industrijski standard, ki ga podpira večina vodilnih proizvajalcev in aplikacij.

### 4.3. MS CryptoAPI

Microsoft (MS) Cryptographic API (MS CryptoAPI) je alternativni vmesnik za dostop do kriptografskih servisov. Omogoča dostop do kriptografskih servisov, podobno kot PKCS#11, ter funkcije za delo z digitalnimi potrdili. MS CryptoAPI modularna arhitektura omogoča vstavitev (plug in) alternativnih kriptografskih modulov (cryptographic service provides – CSP), na primer modulov za pametne kartice posameznih proizvajalcev. MS CryptoAPI je vgrajen v spletni brskalnik MS IE in operacijske sisteme MS.

### 4.4. PKCS#12

PKCS#12 je standard, ki se uporablja za varno hranjenje in prenos kriptografskih ključev in digitalnih potrdil. PKCS#12 standard podpira zaupnost (šifriranje z javnim ključem, ali geslom) in integriteto (digitalni podpis, ali MAC) hranjenih, oziroma prenesenih podatkov. Z uporabo formata PKCS#12 je na primer možen prenos (izvoz/uvoz) ključev in digitalnih potrdil med različnimi brskalniki ter njihov uvoz na pametne kartice.

### 4.5. Network Security Services (NSS)

Network Security Services (NSS) je nabor odprtokodnih knjižnic, ki omogočajo razvoj cross-platform aplikacij, tako na strani odjemalca, kot tudi na strani strežnika. Aplikacije razvite z uporabo NSS razvojnih orodij lahko podpirajo uporabo asimetričnih ključev in digitalnih potrdil za SSL v2 in v3, TLS, PKCS #5, PKCS #7, PKCS #11, PKCS #12, S/MIME, X.509 v3 in nekaterih drugih varnostnih standardov.

### 4.6. Uporaba posebnih potrdil (Entrust Enterprise ID) hranjenih na pametnih karticah v spletnih brskalnikih

Posebna potrdila, shranjena na pametni kartici (Entrust Enterprise ID profil shranjen na pametni kartici), je možno uporabiti tudi v spletnih brskalnikih, če uporabljena pametna kartica podpira tako imenovani dual-head oziroma hkratni dostop do kartice preko PKCS#11 in MS CryptoAPI.

Po sinhronizaciji posebnih potrdil na kartici s shrambo potrdil brskalnika (Certificate Store), je iz aplikacij, ki podpirajo MS CryptoAPI oziroma PKCS#11, možno uporabiti obe posebni potrdili (potrdilo za preverjanje podpisa in potrdilo za šifriranje). Pri sinhronizaciji potrdil na kartici s shrambo potrdil se iz kartice prenesejo v shrambo potrdil samo potrdila, zasebni ključi pa ostanejo na pametni kartici. Aplikacije dostopajo do kriptografskih servisov, ki uporabljajo zasebni ključ, na kartici preko modula MS CryptoAPI CSP (Cryptographic Service Provider) oziroma PKCS#11 za specifično pametno kartico.

## 5. IZBIRA MED POSEBNIMI IN SPLETNIMI DIGITALNIMI POTRDILI

### 5.1. Spletna potrdila

Spletna digitalna potrdila so namenjena za uporabo v spletu po protokolih SSL oziroma TLS, S/MIME ter IPsec.

Programska oprema za ta potrdila mora znati tvoriti par 2048-bitnih ključev po algoritmu RSA, zahtevek za digitalno potrdilo po priporočilu PKCS#10 ter vključiti potrdilo, ki ga dobi podpisano od SIGEN-CA oz. SIGOV-CA v formatu PKCS#7. To pa so priporočila, ki jih podpira večina brskalnikov, spletnih strežnikov ter nekateri usmerjevalniki.

Sporočila v obliki S/MIME so standardna, ne glede na to, ali se uporabi spletno ali posebno digitalno potrdilo. Tako lahko za S/MIME sporočilo, podpisano in/ali šifrirano s spletnim digitalnim potrdilom, preveri podpis in/ali ga dešifrira odjemalec, ki uporablja posebno digitalno potrdilo.

Spletna digitalna potrdila znajo uporabljati:
- MS Internet Explorer,
- Netscape,
- Mozilla,
- Opera,
- Chrome,
- Safari,
- Lotus Notes / Domino,
- vsi produkti, ki uporabljajo open_ssl:
    - spletni strežnik Apache z modulom mod_ssl,
    - sendmail seja SSL,
    - openldap seja SSL,
    - postfix seja SSL,
    - freeswan IPSEC/VPN ,
    - cyrus imap4 deamon (seja SSL),
- in še mnogo drugih produktov.

## 5.2. Posebna potrdila

Posebna digitalna potrdila so namenjena aplikacijam v državni upravi in pri poslovnih subjektih. Uporabna so tudi za sporočila S/MIME in (ob upoštevanju zgoraj navedenega) tudi v spletnih brskalnikih. Aplikacija mora podpirati ločena para ključev za podpisovanje in šifriranje. Omogočati mora tudi regeneriranje zasebnega ključa za dešifriranje, če postane neuporaben. To je potrebno zato, da ne bi izgubili pomembnih službenih zašifriranih podatkov. Uporabniki na svojih delovnih postajah uporabljajo programsko opremo Entrust Entelligence, ki deluje na operacijskem sistemu MS.

Posebno digitalno potrdilo je tehnično gledano sestavljeno iz dveh potrdil X.509:
Par ključev za digitalno podpisovanje/overjanje sestavlja:
- zasebni ključ za podpisovanje (se hrani pri uporabniku) ter
- javni ključ za overjanje podpisa (se hrani pri uporabniku, pri vsakem podpisanem dokumentu ali sporočilu S/MIME).

Par ključev za šifriranje/dešifriranje sestavlja:
- zasebni ključ za dešifriranje (se hrani pri uporabniku in izdajatelju) ter
- javni ključ za šifriranje (se hrani pri uporabniku in v javnem imeniku X500).

V primeru, da se zasebni ključ za dešifriranje izgubi/uniči, se preko posebnega postopka, ki je podoben prevzemu digitalnega potrdila, regenerira posebno digitalno potrdilo, kar pomeni, da se:
- iz SIGEN-CA oz. SIGOV-CA k imetniku prenese zgodovina starih zasebnih ključev za dešifriranje. Tako so dokumenti, zašifrirani s starim digitalnim potrdilom, zopet dostopni.
- za par za podpisovanje se generira nov par ključev.

Teh lastnosti spletno digitalno potrdilo nima, zato je potreben posebni odjemalec. Za informacijo o razvojnih orodjih za uporabo posebnih digitalnih potrdil se obrnite na pooblaščene osebe Overitelja.

Razlike med posebnimi in spletnimi digitalnim potrdili oz. njihove lastnosti so zbrane na spletnih straneh:

- http://www.sigov-ca.gov.si/vrste-potrdil.htm in
- http://www.sigen-ca.si/vrste-potrdil.htm.

## 6. ŠIFRIRNI ALGORITMI, FORMATI PODATKOV IN PROTOKOLI INFRASTRUKTURE OVERITELJA NA MJU

Overitelj na MJU uporablja:

- za protokol za upravljanje ključev in digitalnih potrdil priporočila PKIX-CMP (angl. *Public Key Infrastructure based on X509 Certificate Managemenet Protocol*),
- za podpisovanje potrdil in registra preklicanih potrdil algoritem SHA-1 z RSA s parom ključev dolžine 2048 bitov,
- za šifriranje podatkov algoritme AES, 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, RFC 1422 in RFC 1423 za 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 v. 2,
- protokol LDAP ustreza priporočilu RFC 1777,
- hranjenje zasebnega ključa ustreza priporočiloma PKCS#5 in PKCS#8,
- komunikacija med programsko opremo (starejših verzij) 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.