Državni center za storitve zaupanja

SI-TRUST
SI-TRUST Root

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

PRIPOROČILA ZA APLIKACIJE

Verzija: 3.1

31. maj 2016

STANJE DOKUMENTA

Namen dokumenta:	Pomoč 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:	3.1
Datum verzije:	31. maj 2016
Avtor:	Državni center za storitve zaupanja
Kontaktni podatki:	Naslov: Državni center za storitve zaupanja Ministrstvo za javno upravo Tržaška cesta 21 1000 Ljubljana Slovenija Tel.: (+386) 01 4788 330 Url.: http://www.ca.gov.si 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 Državnega centra za storitve zaupanja oz. Overitelja na Ministrstvu za javno upravo in predstavlja del Priporočil za aplikacije e-storitev z varnostnimi zahtevami za 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 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. DRŽAVNI CENTER ZA STORITVE ZAUPANJA

Državni center za storitve zaupanja oz. 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. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14) in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06), Uredbo (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (eIDAS; Uradni list EU, št. L 257/73), evropskimi direktivami in standardi ETSI ter drugimi veljavnimi predpisi in priporočili. 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.

Znotraj overitelja na MJU deluje korenski izdajatelj digitalnih potrdil SI-TRUST Root (angl. Slovenian Trust Service Root Certification Authority), v nadaljevanju korenski izdajatelj SI-TRUST Root ali kratko SI-TRUST Root (http://www.ca.gov.si). SI-TRUST Root izdaja potrdila v dveh obsegih, znotraj Overitelja na MJU kot korenski izdajatelj, pri povezovanju z zunanjimi izdajatelji pa kot premostitveni izdajatelj.

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, priznana s strani SI-TRUST Root 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.

Overitelj na MJU izdaja tudi normalizirana digitalna potrdila ter digitalna potrdila za posebne namene oz. zaprte sisteme. Normalizirana digitalna potrdila, ki jih izdaja overitelj na MJU, so namenjena:

- izdajateljem potrdil, izdajateljem časovnih žigov, strežnikom oz. informacijskim sistemom, sistemom OCSP, podpisovanju programske kode in registra preklicanih potrdil ter v ostalih primerih, kjer ni možna uporaba kvalificiranih potrdil,
- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba teh potrdil in
- za storitve oz. aplikacije, za katere se zahteva uporaba teh potrdil.

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 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,
- spletna normalizirana digitalna potrdila za strežnike, s katerimi upravljajo organizacije,
- spletna normalizirana digitalna potrdila za podpis kode za potrebe organizacije,
- normalizirana digitalna potrdila za izdajatelje varnih časovnih žigov[1],
- normalizirana digitalna potrdila za sisteme za sprotno preverjanje veljavnosti digitalnih potrdil[2].

SIGEN-CA izdaja 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,
- spletna normalizirana digitalna potrdila za strežnike, s katerimi upravljajo organizacije,
- spletna normalizirana digitalna potrdila za podpis kode za potrebe organizacije,
- spletna kvalificirana digitalna potrdila za fizične osebe.

Izdajatelj SIGEN-CA oz. SIGOV-CA izdaja oz. je izdajal potrdila dveh generacij in sicer potrdila 1. generacije v letih 2001 do 2016 ter potrdila 2. generacije od leta 2016 dalje.

Po Zakonu o elektronskem poslovanju in elektronskem podpisu (ZEPEP) ima elektronski podpis pravno veljavo, če je

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

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

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, uredbo eIDAS, evropskimi direktivami ter drugimi veljavnimi predpisi.

2.1. Hierahija izdajateljev overitelja na MJU

Korenski izdajatelj SI-TRUST Root je ob začetku svojega produkcijskega delovanja tvoril svoje lastno digitalno potrdilo, ki je namenjeno overjanju potrdil, ki jih je SI-TRUST Root izdal podrejenim in povezanim izdajateljem kvalificiranih digitalnih potrdil.

Potrdilo SI-TRUST Root vsebuje naslednje podatke:

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. *Version*	3
Identifikacijska oznaka potrdila, angl. *Serial Number*	90AE 7776 0000 0000 571D D06F
Algoritem za podpis, angl. *Signature algorithm*	sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11)
Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Imetnik, angl. *Subject*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SI-TRUST Root
Pričetek veljavnosti, angl. *Validity: Not Before*	Apr 25 07:38:17 2016 GMT
Konec veljavnosti, angl. *Validity: Not After*	Dec 25 08:08:17 2037 GMT
Algoritem za javni ključ, angl. *Subject Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. *RSA Public Key*	*ključ dolžine 3072 bitov*
Razširitve X.509v3	
Uporaba ključa, OID 2.5.29.15, *angl. Key Usage*	Kritično (Critical) Podpis potrdil (keyCertSign), Podpis CRL (cRLSign)
Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	Kritično (Critical) CA: TRUE Brez omejitev dolžine (Path Length Constraint: none)
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. Auth*ority Key Identifier*	4CA3 C368 5E08 0263
Identifikator imetnikovega ključa, OID 2.5.*29.14,* *angl. Subject Key Identifier*	4CA3 C368 5E08 0263
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA1*	3A49 79B4 0FA8 4148 8200 B582 FBEE B63A AB99 19AE

Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA256*	FAD5 4081 1AFA E0DC 767C DF65 72A0 88FA 3CE8 493D D82B 3B86 9A67 D10A AB4E 8124

Za vzpostavljanje zaupanja v digitalna potrdila končnih uporabnikov je potrebno tako na strežnikih kot v brskalnikih ali drugih odjemalcih namestiti celotno verigo potrdil tj. tudi obe povezovalni potrdili izdajatelja SIGEN-CA (ali SIGOV-CA) ter korensko potrdilo izdajatelja SI-TRUST Root. Čeprav se v času izdajanja potrdil 1. generacije korensko potrdilo SI-TRUST Root in povezovalna potrdila niso uporabljala, vseeno priporočamo, da se tako pri potrdilih 1. generacije kot pri potrdilih 2. generacije na strežnikih uporablja celotna veriga potrdil, saj lahko le na ta način zagotovimo, da bodo potrdila končnih uporabnikov prepoznana kot zaupanja vredna ne glede na to, ali je v brskalniku nameščena celotna veriga potrdil ali pa zgolj potrdilo izdajatelja SIGEN-CA oz. SIGOV-CA. Korensko potrdilo izdajatelja SI-TRUST Root ter vsa izdana povezovalna potrdila so dostopna na spletni strani http://www.si-ca.si/identiteta-si-trust-root.php.

V nadaljevanju je prikazan primer konfiguracije z uporabo verige potrdil za spletni strežnik Apache, ki uporablja potrdilo izdajatelja SIGEN-CA G2 ter omogoča prijavo uporabnikov s potrdili izdajateljev SIGEN-CA in SIGOV-CA obeh generacij.

```
SSLCertificateFile /etc/pki/tls/certs/server.crt
```

Datoteka `server.crt` vsebuje potrdilo spletnega strežnika in povezovalno potrdilo njegovega izdajatelja, torej v našem primeru izdajatelja SIGEN-CA G2. Povezovalno potrdilo je lahko vključeno tudi v datoteki, ki jo določa parameter `SSLCertificateChainFile`. Ta paramater se od verzije Apache 2.4.8 več ne uporablja..

```
SSLCACertificateFile /etc/pki/tls/certs/trusted-ca.pem
```

Datoteka `trusted-ca.pem` vsebuje potrdila vseh korenskih izdajateljev, ki naj jim strežnik zaupa, v našem primeru torej korensko potrdilo izdajatelja SI-TRUST Root. Priporočamo, da v datoteko vključite tudi vsa pripadajoča povezovalna potrdila, v našem primeru torej štiri povezovalna potrdila, za obe generaciji izdajateljev SIGEN-CA in SIGOV-CA. Povezovalna potrdila se uporabijo za preverjanje verige potrdil v primeru, če brskalnik strežniku pošlje zgolj potrdilo končnega uporabnika.

```
SSLCADNRequestFile /etc/pki/tls/certs/sitrust_xcerts_all.pem
```

Datoteka `sitrust_xcerts_all.pem` vsebuje potrdila izdajateljev, ki naj jih strežnik pošlje brskalniku, da ima uporabnik pri izbiri svojega potrdila omejen nabor izdajateljev. Ker strežnik za oblikovanje nabora izdajateljev uporabi le polje Subject, načeloma lahko uporabite bodisi korenska potrdila bodisi povezovalna potrdila izdajateljev, vendar priporočamo, da zaradi zagotavljanja konsistentnosti uporabljate le slednja (torej tista, ki so vključena tudi v datoteki `trusted-ca.pem`). V našem primeru naj datoteka vsebuje vsa štiri povezovalna potrdila izdajateljev SIGEN-CA in SIGOV-CA.. Če parameter `SSLCADNRequestFile` v konfiguraciji ne obstaja, strežnik uporabi parameter `SSLCACertificateFile`.

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.

Tip potrdila	Par ključev	Ključi	Veljavnost

posebno potrdilo	par za digitalno podpisovanje/overjanje (posebno potrdilo – za overjanje podpisa)	zasebni ključ za podpisovanje	5 let
		javni ključ za overjanje podpisa	5 let
	par za dešifriranje/šifriranje (posebno potrdilo – za šifriranje)	zasebni ključ za dešifriranje	5 let
		javni ključ za šifriranje	5 let
spletno potrdilo	par za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	zasebni ključ	5 let
		javni ključ	5 let
spletno potrdilo za strežnike	par za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	zasebni ključ	3 leta
		javni ključ	3 leta
spletno potrdilo za podpis kode	par za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	zasebni ključ	5 let
		javni ključ	5 let
potrdilo za izdajatelja TSA	par ključev za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	zasebni ključ	3 leta
		javni ključ	5 let
potrdilo za sistem OCSP	par ključev za digitalno podpisovanje/overjanje (potrdilo za overjanje podpisa)	zasebni ključ	3 leta
		javni ključ	3 leta

3.2. Način pridobitve 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 -

[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.

nekateri namesto številke OID izpišejo pripadajoči tekst in vrednost v berljivi obliki, drugi pa navedejo zgolj številko OID in vrednost v šestnajstiškem sistemu. Razširitvi, označeni kot kritični, sta *uporaba ključa* (angl. *Key Usage*) in *razširjena uporaba ključa* (angl. *Extended Key Usage),* kar pomeni, da ju aplikacija ne sme ignorirati, če ju ne zna interpretirati.

3.3.1 Profil digitalnih potrdil SIGEN-CA

Potrdila SIGEN-CA 1. generacije vsebujejo polja, ki so prikazana v spodnji tabeli in razdelkih v nadaljevanju.

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

Identifikator imetnikovega ključa, OID 2.5.*29.14*, *angl. Subject Key Identifier*	*identifikator imetnikovega ključa*
Politike, pod katerimi je bilo izdano potrdilo, OID 2.5.29.32, angl. *certificatePolicies*	Certificate Policy: PolicyIdentifier= *odvisno od vrste potrdila* [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ca.gov.si/cps/
Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. *qcStatement*	*odvisno od vrste potrdila*
Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	*se ne uporablja*
OID 1.2.840.113533.7.65.0 Verzija Entrust angl. *Entrust version extension*	V7.1
Dodatna identifikacija (ni del digitalnega potrdila)	
razpoznavni odtis potrdila-SHA1 angl. *Certificate Fingerprint – SHA1*	*razpoznavni odtis potrdila po SHA1*
razpoznavni odtis potrdila-SHA256 angl. *Certificate Fingerprint – SHA256*	*razpoznavni odtis potrdila po SHA256*

Potrdila SIGEN-CA 2. generacije vsebujejo polja, ki so prikazana v spodnji tabeli in razdelkih v nadaljevanju.

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Number*	*enolična interna številka potrdila-celo število*
Algoritem za podpis, angl. *Signature algorithm*	sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11)
Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
Veljavnost, angl. *Validity*	Not Before: <*pričetek veljavnosti po GMT*> Not After: <*konec veljavnosti po GMT*> *v formatu UTCTime* <LLMMDDuummssZ>
Imetnik, angl. *Subject*	*razločevalno ime imetnika, odvisno od vrste potrdila v obliki, primerni za izpis*
Algoritem za javni ključ, angl. *Subject Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. *RSA Public Key*	*dolžina ključa je min. 2048 bitov*
Razširitve X.509v3	
Alternativno ime, OID 2.5.29.17, angl. *Subject Alternative Name*	elektronski naslov imetnika ime strežnika pri spletnih potrdilih za strežnike

Objava registra preklicanih potrdil, OID 2.5.29.31, angl. *CRL Distribution Points*	Url: http://www.sigen-ca.si/crl/sigen-ca-g2.crl Url: ldap://x500.gov.si/cn=SIGEN-CA G2, oi=VATSI-17659957, o=Republika Slovenija, c=SI?certificateRevocationList c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2, cn=CRL<*zaporedna številka registra*>
Dostop do podatkov o izdajatelju, OID 1.3.6.1.5.5.7.1.1, angl. *Authority Information Access*	Access Method=OCSP http://ocsp.sigen-ca.si
Uporaba ključa, OID 2.5.29.15, *angl. Key Usage*	*odvisna od vrste potrdila*
Razširjena uporaba ključa, OID 2.5.29.37, angl. *Extended Key Usage*	*odvisno od vrste potrdila*
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. Auth*ority Key Identifier*	4C25 278C A82D 729E
Identifikator imetnikovega ključa, OID 2.5.*29.14,* *angl. Subject Key Identifier*	*identifikator imetnikovega ključa*
Politika, pod katero je bilo izdano potrdilo, OID 2.5.29.32, angl. *certificatePolicies*	Certificate Policy: PolicyIdentifier= *odvisno od vrste potrdila* [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ca.gov.si/cps/
Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. *qcStatement*	*odvisno od vrste potrdila*
Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	CA: FALSE Brez omejitev dolžine (Path Length Constraint: none)
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1 angl. *Certificate Fingerprint – SHA-1*	*razpoznavni odtis potrdila po SHA-1*
Odtis potrdila SHA-256 angl. *Certificate Fingerprint – SHA-256*	*razpoznavni odtis potrdila po SHA-256*

3.3.2 Profil digitalnih potrdil SIGOV-CA

Potrdila SIGOV-CA 1. generacije vsebujejo polja, ki so prikazana v spodnji tabeli in razdelkih v nadaljevanju.

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. *Version*	3
Identifikacijska oznaka potrdila, angl. *Serial Number*	*enolična interna številka potrdila-celo število*

Algoritem za podpis, angl. *Signature algorithm*	sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5)
Izdajatelj, angl. *Issuer*	c=si, o=state-institutions, ou=sigov-ca
Veljavnost, angl. *Validity*	Not Before: <*pričetek veljavnosti po GMT*> Not After: <*konec veljavnosti po GMT*> *v formatu UTCTime* <LLMMDDuummssZ>
Imetnik, angl. *Subject*	*razločevalno ime imetnika, odvisno od vrste potrdila*
Algoritem za javni ključ, angl. *Subject Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)
Javni ključ, angl. *Public Key (... bits)*	*modul, eksponent,...*
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA, angl. *RSA Public Key*	*dolžina ključa je min 2048 bitov*
Razširitve X.509v3	
Alternativno ime OID 2.5.29.17, angl. *Subject Alternative Name*	*elektronski naslov*
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. *CRL Distribution Points*	c=si, o=state-institutions, ou=sigov-ca, cn=CRL<*zaporedna številka registra* 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
Zasebni ključ za podpisovanje velja do, OID 2.5.29.16, angl. *Private Key Usage Period*	*odvisna od vrste potrdila*
Uporaba ključa, OID 2.5.29.15, *angl. Key Usage*	*odvisna od vrste potrdila*
Razširjena uporaba, OID 2.5.29.37, angl. *Extended Key Usage*	*odvisno od vrste potrdila*
Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. Auth*ority Key Identifier*	1EF8 D453 6BB3 8306 E904 0657 02F9 A5BF C658 3C72
Identifikator imetnikovega ključa, OID 2.5.*29.14,* *angl. Subject Key Identifier*	*identifikator imetnikovega ključa*
Politika, pod katero je bilo izdano potrdilo, OID 2.5.29.32, angl. *certificatePolicies*	Certificate Policy: PolicyIdentifier= *odvisno od vrste potrdila* [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ca.gov.si/cps/
Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. *qcStatement*	*odvisna od vrste potrdila*
Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	*se ne uporablja*

OID 1.2.840.113533.7.65.0 Verzija Entrust angl. *Entrust version extension*	V7.1
Dodatna identifikacija (ni del digitalnega potrdila)	
razpoznavni odtis potrdila-SHA1 angl. *Certificate Fingerprint – SHA1*	*razpoznavni odtis potrdila po SHA1*
razpoznavni odtis potrdila-SHA256 angl. *Certificate Fingerprint – SHA256*	*razpoznavni odtis potrdila po SHA256*

Potrdila SIGOV-CA 2. generacije vsebujejo polja, ki so prikazana v spodnji tabeli in razdelkih v nadaljevanju.

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Number*	*enolična interna številka potrdila-celo število*
Algoritem za podpis, angl. *Signature algorithm*	sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11)
Izdajatelj, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGOV-CA
Veljavnost, angl. *Validity*	Not Before: <*pričetek veljavnosti po GMT*> Not After: <*konec veljavnosti po GMT*> *v formatu UTCTime* <LLMMDDuummssZ>
Imetnik, angl. *Subject*	*razločevalno ime imetnika, odvisno od vrste v obliki, primerni za izpis*
Algoritem za javni ključ, angl. *Subject Public Key Algorithm*	rsaEncryption (OID 1.2.840.113549.1.1.1)
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. *RSA Public Key*	*dolžina ključa je min 2048 bitov*
Razširitve X.509v3	
Alternativno ime, OID 2.5.29.17, angl. *Subject Alternative Name*	*elektronski naslov* *ime strežnika pri spletnih potrdilih za strežnike*
Objava registra preklicanih potrdil, OID 2.5.29.31, angl. *CRL Distribution Points*	Url: http://www.sigov-ca.gov.si/crl/sigov-ca2.crl Url: ldap://x500.gov.si/cn=SIGOV-CA, oi=VATSI-17659957, o=Republika Slovenija, c=SI?certificateRevocationList c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGOV-CA, cn=CRL<*zaporedna številka registra*>
Dostop do podatkov o izdajatelju, OID 1.3.6.1.5.5.7.1.1, angl. *Authority Information Access*	Access Method=OCSP http://ocsp.sigov-ca.gov.si
Uporaba ključa, OID 2.5.29.15, *angl. Key Usage*	*odvisna od vrste potrdila*
Razširjena uporaba ključa, OID 2.5.29.37, angl. *Extended Key Usage*	*odvisno od vrste potrdila*

Identifikator izdajateljevega ključa, OID 2.5.29.35, angl. Authority *Key Identifier*	465E 40E5 53ED FEFE
Identifikator imetnikovega ključa, OID 2.5.*29.14,* *angl. Subject Key Identifier*	*identifikator imetnikovega ključa*
Politika, pod katero je bilo izdano potrdilo, OID 2.5.29.32, angl. *certificatePolicies*	Certificate Policy: PolicyIdentifier= *odvisno od vrste potrdila* [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ca.gov.si/cps/
Oznaka kvalificiranega potrdila, OID 1.3.6.1.5.5.7.1.3, angl. *qcStatement*	*odvisna od vrste potrdila*
Osnovne omejitve, OID 2.5.29.19, angl. *Basic Constraints*	CA: FALSE Brez omejitev dolžine (Path Length Constraint: none)
Odtis potrdila (ni del potrdila)	
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA-1*	*razpoznavni odtis potrdila po SHA-1*
Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA-256*	*razpoznavni odtis potrdila po SHA-256*

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]	*1. generacija*	*2. generacija*
potrdilo izdajatelja SIGEN-CA	c=si, o=state-institutions, ou=sigen-ca	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2
SIGEN-CA spletna za fizične osebe	c=si, o=state-institutions, ou=sigen-ca, ou=individuals, cn=<ime in priimek>, sn=<serijska številka>	c=SI, st=Slovenija, ou=individuals, cn=<ime in priimek>, gn=<ime>, surname=<priimek>, sn=<serijska številka>
posebna potrdila za zaposlene in splošne nazive organizacij oz. organizacijske enote organizacij	c=si, o=state-institutions, ou=sigen-ca, ou=companies (*ali* ou=org) ou=<oznaka organizacije>-<davčna št. organizacije>, cn=<naziv>, sn=<serijska številka>	c=SI, st=Slovenija, o=<oznaka organizacije>, oi=VATSI-<davčna št. organizacije>, cn=<naziv>, gn=<ime>, surname=<priimek>, sn=<serijska številka>
spletna potrdila za zaposlene in splošne nazive organizacij oz. organizacijske enote organizacij	c=si, o=state-institutions, ou=sigen-ca, ou=companies-web (*ali* ou=org-web)	c=SI, st=Slovenija, o=<oznaka organizacije>, oi=VATSI-<davčna št. organizacije>,

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

	ou=<oznaka organizacije>-<davčna št. organizacije>, cn=<naziv>, sn=<serijska številka>	cn=<naziv>, gn=<ime>, surname=<priimek>, sn=<serijska številka>
spletna potrdila za strežnike	c=si, o=state-institutions, ou=sigen-ca, ou=companies-web (*ali* ou=org-web) ou=< oznaka organizacije>-<davčna št. organizacije>, cn=<naziv>, sn=<serijska številka>	c=SI , st=Slovenija, o=<oznaka organizacije>, oi=VATSI- <davčna št. organizacije>, cn=<naziv>, sn=<serijska številka>
spletna potrdila za podpis kode	c=si, o=state-institutions, ou=sigen-ca, ou=companies-web (*ali* ou=org-web) ou=<oznaka organizacije>-<davčna št. organizacije>, cn=<naziv>, sn=<serijska številka>	c=SI, st=Slovenija, o=<oznaka organizacije>, oi=VATSI- <davčna št. organizacije>, cn=<naziv>, sn=<serijska številka>
potrdilo izdajatelja SIGOV-CA	c=si, o=state-institutions, ou=SIGOV-CA	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGOV-CA
posebna potrdila za zaposlene in splošne nazive organizacij oz. organizacijske enote organizacij	c=si, o=state-institutions, ou=certificates, ou=<oznaka organizacije>, cn=<naziv>, sn=<serijska številka>	c=SI, o=state authorities, ou=certificates, cn=<naziv>, gn=<ime>, surname=<priimek>, sn=<serijska številka>
spletna potrdila za zaposlene in splošne nazive organizacij oz. organizacijske enote organizacij	c=si, o=state-institutions, ou=web-certificates, cn=<naziv>, sn=<serijska številka>	c=SI, o=state authorities, ou=web-certificates, cn=<naziv>, gn=<ime>, surname=<priimek>, sn=<serijska številka>
spletna potrdila za strežnike	c=si, o=state-institutions, ou=web-certificates, ou=servers, cn=<naziv>, sn=<serijska številka>	c=SI, o=state authorities, ou=servers, cn=<naziv>, sn=<serijska številka>
spletna potrdila za podpis kode	c=si, o=state-institutions, ou=web-certificates, ou=codesign, cn=<naziv>, sn=<serijska številka>	c=SI, o=state authorities, ou=codesign, cn=<naziv>, sn=<serijska številka>

Opozoriti je potrebno sledeče:

- imena (ime, priimek, splošni nazivi, oznake organizacij in institucij) v potrdilih 1. generacije lahko vključujejo črke angleške abecede, številke in nekatere posebne znake (- . : & * @ ! $ #), medtem ko imena v potrdilih 2. generacije lahko vsebujejo tudi znake iz kodne tabele UTF-8,
- 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
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 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:

Naziv polja	Vrednost oz. pomen
Osnovna polja v CRL	
Različica, angl. *Version*	2
Izdajateljev podpis, angl. *Signature*	p*odpis SIGEN-CA*
Razločevalno ime izdajatelja, angl. *Issuer*	c=si, o=state-institutions, ou=sigen-ca *(1. generacija)* c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGEN-CA G2 *(2. generacija)*
Čas izdaje CRL, angl. *thisUpdate*	Last Update: <*čas izdaje po GMT*>
Čas izdaje naslednjega CRL, angl. *nextUpdate*	Next Update: <*čas naslednje izdaje po GMT*>
Identifikacijske oznake preklicanih potrdil in čas preklica, angl. *revokedCertificate*	Serial Number: <*identifikacijska oznaka preklicanega dig. potrdila*> Revocation Date: <*čas preklica po GMT*>
Algoritem za podpis, angl. *Signature Algorithm*	sha1WithRSAEncryption *(1. generacija)* sha256WithRSAEncryption *(2. generacija)*
Razširitve X.509v2 CRL	
Identifikator izdajateljevega ključa, angl. *Authority Key Identifier* *(OID 2.5.29.35)*	*identifikator izdajateljevega ključa*
Številka za posamične registre (CRL1, CRL2,....), angl. *CRLnumber* *(OID 2.5.29.20)*	*zaporedna številka posamičnega registra*
Alternativno ime izdajatelja angl. *issuerAltName* *(OID 2.5.28.18)*	*se ne uporablja*
Oznaka seznama sprememb angl. *deltaCRLindicator* *(OID 2.5.29.27)*	*se ne uporablja*
Objava seznama sprememb angl. *issuingDistribuitionPoint* *(OID 2.5.29.28)*	*se ne uporablja*

CRL za SIGOV-CA:

Naziv polja	Vrednost oz. pomen
Osnovna polja v CRL	
Različica, angl. *Version*	2
Izdajateljev podpis, angl. *Signature*	p*odpis SIGOV-CA*
Razločevalno ime izdajatelja, angl. *Issuer*	c=si, o=state-institutions, ou=sigov-ca *(1. generacija)* c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGOV-CA *(2. generacija)*
Čas izdaje CRL, angl. *thisUpdate*	Last Update: <*čas izdaje po GMT*>
Čas izdaje naslednjega CRL, angl. *nextUpdate*	Next Update: <*čas naslednje izdaje po GMT*>

identifikacijske oznake preklicanih potrdil in čas preklica, angl. *revokedCertificate*	Serial Number: <*identifikacijska oznaka preklicanega dig. potrdila*> Revocation Date: <*čas preklica po GMT*>
Algoritem za podpis, angl. *Signature Algorithm*	sha1WithRSAEncryption *(1. generacija)* sha256WithRSAEncryption *(2. generacija)*
Razširitve X.509v2 CRL	
Identifikator izdajateljevega ključa, angl. *Authority Key Identifier* *(OID 2.5.29.35)*	*identifikator izdajateljevega ključa*
Številka za posamične registre (CRL1, CRL2,....), angl. *CRLnumber* *(OID 2.5.29.20)*	*zaporedna številka posamičnega registra*
Alternativno ime izdajatelja angl. *issuerAltName* *(OID 2.5.28.18)*	*se ne uporablja*
Oznaka seznama sprememb angl. *deltaCRLindicator* *(OID 2.5.29.27)*	*se ne uporablja*
Objava seznama sprememb angl. *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 *(1. generacija)*	*posamični registri:* • 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: • 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 • Url: http://www.sigen-ca.si/crl/sigen-ca.crl
SIGEN-CA G2 *(2. generacija)*	*posamični registri:* • c=SI, o=Republika Slovenija, oi=VATSI-7659957, cn=SIGEN-CA G2, cn=CRL <zaporedna številka registra>	• Url: ldap://x500.gov.si/ cn=CRL<zaporedna številka registra>/cn=SIGEN-CA G2, oi=VATSI-17659957, o=Republika Slovenija, c=SI
	celotni register: • c=SI, o=Republika Slovenija, oi=VATSI-7659957, cn=SIGEN-CA G2 (v polju "CertificationRevocationList")	• Url: ldap://x500.gov.si/cn=SIGEN-CA G2, oi=VATSI-17659957, o=Republika Slovenija, c=SI?certificateRevocationList • Url: http://www.sigen-ca.si/crl/sigen-ca-g2.crl
SIGOV-CA *(1. generacija)*	*posamični registri:* • 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: • 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 • Url: http://www.sigov-ca.gov.si/crl/sigov-ca.crl

SIGOV-CA *(2. generacija)*	*posamični registri:* • c=SI, o=Republika Slovenija, oi=VATSI-7659957, cn=SIGOV-CA, cn=CRL <zaporedna številka registra>	• Url: ldap://x500.gov.si/ cn=CRL<zaporedna številka registra>/cn=SIGOV-CA, oi=VATSI-17659957, o=Republika Slovenija, c=SI
	celotni register: • c=SI, o=Republika Slovenija, oi=VATSI-7659957, cn=SIGOV-CA (v polju "CertificationRevocationList")	• Url: ldap://x500.gov.si/cn=SIGOV-CA, oi=VATSI-17659957, o=Republika Slovenija, c=SI?certificateRevocationList • Url: http://www.sigov-ca.gov.si/crl/sigov-ca2.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*) je dostopno na naslednjih spletnih naslovih:

- http://ocsp.sigen-ca.si (SIGEN-CA)
- http://ocsp.sigov-ca.gov.si (SIGOV-CA)
- http://ocsp.ca.gov.si (SI-TRUST Root)

Profil sporočil OCSP (zahtevek/odgovor) storitve za sprotno preverjanje statusa potrdil je v skladu s priporočilom RFC 2560. Sporočila OCSP podpirajo razširitev Nonce, ki ni označena kot kritična.

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

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, 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	*podatki v prevajalni tabeli*
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 Security Provider,
- **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 Security Provider, 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 (https://www.entrust.com/support/toolkits/index.htm) Microsoft CryptoAPI
Microsoft Certificate Store	Microsoft CryptoAPI
Network Security Services (NSS)	Mozilla NSS Open Source Crypto Libraries
Pametne kartice	PKCS#11 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.

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.

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 zašifriranih podatkov. Uporabniki na svojih delovnih postajah uporabljajo programsko opremo Entrust Security Provider, 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-256 z RSA s parom ključev dolžine 3072 bitov,
- za šifriranje podatkov algoritme AES 256 (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 Overitelja 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.