CENTER VLADE REPUBLIKE SLOVENIJE
ZA INFORMATIKO

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

PRIPOROČILA ZA APLIKACIJE

Verzija: 1.1

14. oktober 2003

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:	1.1
Datum verzije:	14. oktober 2003
Avtor:	Overitelj na Centru Vlade RS za informatiko
Kontaktni podatki:	Naslov: Center Vlade Republike Slovenije za informatiko Langusova 4 1000 Ljubljana Slovenija Tel.: (+386) 01 4788 600 Fax.: (+386) 01 4788 649 Url.: http://www.gov.si/ca 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 z novimi kot tudi predhodnimi verzijami politik 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 Centru vlade RS za informatiko 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 osebnimi in spletnimi digitalnimi potrdili,
5. poglavje: algoritmi, formati itd. infrastrukture Overitelja na CVI.

2. OVERITELJ NA CENTRU VLADE RS ZA INFORMATIKO

Overitelj na Centru Vlade RS za informatiko (CVI) izdaja kvalificirana digitalna potrdila, za katera velja najvišja stopnja varovanja in načela t.i. močne enkripcije ter deluje v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 57/2000) in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000 in 2/2001), evropskimi direktivami ter drugimi veljavnimi predpisi. Politika delovanja overitelja na CVI določa namen, delovanje in metodologijo upravljanja s kvalificiranimi digitalnimi potrdili, odgovornost overitelja na CVI ter zahteve, ki jih morajo izpolnjevati imetniki, tretje osebe, ki se zanašajo na kvalificirana digitalna potrdila, in drugi overitelji.

Overitelja na CVI (http://www.gov.si/ca*)* predstavljata dva izdajatelja kvalificiranih digitalnih potrdil:
- SIGEN-CA (angl. *Slovenian General Certification Authority*) za državljane in pravne osebe (http://www.sigen-ca.si),
- SIGOV-CA (angl. *Slovenian Governmental Certification Authority*) za upravo Republike Slovenije (http://www.sigov-ca.gov.si).

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

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

SIGEN-CA oz. SIGOV-CA izdajata dve skupini kvalificiranih digitalnih potrdil (odločitev med uporabo osebnih ali spletnih digitalnih potrdil je :
- *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 1024-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.
- *Osebna digitalna potrdila* so namenjena predvsem uslužbencem oziroma aplikacijam v državni upravi. Ta oprema mora podpirati ločena para ključev za podpisovanje in šifriranje. Omogočati mora tudi, da se da zasebni ključ za šifriranje regenerira, 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 zaenkrat uporabljajo programsko opremo Entrust/Entelligence, ki deluje na MS Oknih od 95 navzgor, ali drugo programsko opremo »Entrust Ready«.

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

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

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 CVI 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 CVI

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

Politike delovanja predstavljajo javni del notranjih pravil overitelja. Nove in prejšnje verzije so objavljena na spletni strani http://www.gov.si/ca/cps. V tabeli spodaj so zbrani podatki o vrstah digitalnih potrdil v povezavi z verzijami politik delovanja Overitelja na CVI.

Politika delovanja	*Veljavnost*	*OID politike*	*Vrste potrdil*
Politika SIGEN-CA za fizične osebe	9. 7. 2001 - 14. 7. 2002	1.3.6.1.4.1.6105.2.2.1	• spletna za fizične osebe
Politika SIGEN-CA za fizične osebe	15. 7. 2002 -	1.3.6.1.4.1.6105.2.2.2	• spletna za fizične osebe
Politika SIGEN-CA za pravne in fizične osebe, registrirane za opravljanje dejavnosti	9. 7. 2001 - 14. 7. 2002	1.3.6.1.4.1.6105.2.1.1	• osebna za zaposlene • spletna za zaposlene
Politika SIGEN-CA za pravne in fizične osebe, registrirane za opravljanje dejavnosti	15. 7. 2002 -	1.3.6.1.4.1.6105.2.1.2	• osebna za zaposlene • osebna za splošne nazive • osebna za strežnike • spletna za zaposlene • spletna za splošne nazive • spletna za strežnike • spletna za podpis kode

Politika SIGOV-CA za osebna kvalificirana digitalna potrdila za institucije javne uprave	17. 1. 2001 - 14. 7. 2002	1.3.6.1.4.1.6105.1.2.1	• osebna za zaposlene (službena osebna)
Politika SIGOV-CA za spletna kvalificirana digitalna potrdila za institucije javne uprave	17. 1. 2001 - 14. 7. 2002	1.3.6.1.4.1.6105.1.1.1	• spletna za zaposlene (službena spletna) • spletna za strežnike
Politika SIGOV-CA za digitalna potrdila za institucije javne uprave	15. 7. 2002 -	1.3.6.1.4.1.6105.1.2.2	• osebna za zaposlene • osebna za splošne nazive • osebna za strežnike
		1.3.6.1.4.1.6105.1.1.2	• spletna za zaposlene • spletna za splošne nazive • spletna za strežnike • spletna za podpis kode

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

tip potrdila		*št. ključev in potrdil*	*ključi*	*veljavnost*	*"key-backup"*
osebno potrdilo	2 para ključev	par za digitalno podpisovanje/overjanje (osebno 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 (osebno potrdilo – za šifriranje)	zasebni ključ za dešifriranje	3 leta	
			javni ključ za šifriranje	3 leta	
spletno potrdilo	1 par ključev	par 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[1]	*pridobitev*
SIGEN-CA spletna 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[2]	*zbiranje podatkov za pridobitev*
SIGEN-CA spletna 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).

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

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

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 3280 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.

Nazivi polj	*Nazivi polj - angleško*	*Vrednost oz. pomen*
Osnovna polja v potrdilu	Standard fields in cert.	
različica X.509	Version	2 (kar pomeni verzijo 3)
identifikacijska oznaka potrdila	Serial Number	enolična interna številka potrdila (celo število)
algoritem za podpis	Signature algorithm	sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5)
izdajatelj	Issuer	c=si, o=state-institutions, ou=sigen-ca
veljavnost	Validity	Not Before: <pričetek veljavnosti po GMT> Not After: <konec veljavnosti po GMT> (*Glej razd. 3.1*) V formatu UTCTime– oblika LLMMDDUUMMSSZ
imetnik	Subject	<razločevalno ime imetnika, ki vključuje naziv imetnika (in organizacijo) in serijsko številko (*Glej razd. 3.3.3*)> Zapisano kot PrintableString
algoritem za javni ključ	Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
javni ključ	Public Key (... bits)	< modul, eksponent,...>
Razširitve X509v3	X509v3 extensions	
OID 2.5.29.17 alternativno ime	Subject Alternative Name	<elektronski naslov imetnika oz. splošnega naziva oz. strežnika>
OID 2.16.840.1.113730.1.1 netscapeCertType	NetscapeCertType	<spletna>: SSLClient, S/MIME
		<spletna-strežnik>: SSL Server
OID 2.16.840.1.113730.1.2 izhodiščni URL	NetscapeBase URL	http://www.sigen-ca.si/cda-cgi/
OID 2.16.840.1.113730.1.3 URL za preverjanje potrdila	NetscapeRevocation URL	clientcgi?action=checkRevocation&&CRL=cn=CRL1&serial=
OID 2.16.840.1.113730.1.13 opis potrdila	Netscape certificate comment	Opis potrdila, npr: Spletno kvalificirano digitalno potrdilo za pravne osebe SIGEN-CA
OID 2.5.29.31 objava registra preklicanih potrdil	CRL Distribution Points	*Glej razd.3.3.4.*
OID 2.5.29.16 zasebni ključ za podpisovanje velja do	Private Key Usage Period	*Glej razd. 3.1.*
OID 2.5.29.15 uporaba ključa	Key Usage	<spletna>: Digital Signature, Key Encipherment
		<osebna - za verifikacijo podpisa>: Digital Signature
		<osebna - za šifriranje>: Key Encipherment
OID 2.5.29.35 identifikator izdajateljevega ključa	Authority Key Identifier	717B 8A06 1F31 0555 AB60 1277 4720 1E03 8818 EC89
OID 2.5.29.14 identifikator imetnikovega ključa	Subject Key Identifier	<identifikator imetnikovega ključa>

OID 2.5.29.32 politika, pod katero je bilo izdano potrdilo	certificatePolicies	*Glej razd. 3.1.* *npr.* Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6105.2.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.gov.si/ca/cps/
OID 2.5.29.19 osnovne omejitve	Basic Constraints	Če bi imetnik lahko deloval kot overitelj, bi bilo to označeno v tem polju, sedaj je prazno.
OID 1.2.840.113533.7.65.0 verzija Entrust	Entrust version extension	V5.0
Dodatna identifikacija (ni del digitalnega potrdila)		
razpoznavni odtis potrdila- MD5	Certificate Fingerprint – MD5	<razpoznavni odtis potrdila - MD5>
razpoznavni odtis potrdila – SHA1	Certificate Fingerprint – SHA1	<razpoznavni odtis potrdila - SHA1>

3.3.2 Profil digitalnih potrdil SIGOV-CA

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

Nazivi polj	*Nazivi polj - angleško*	*Vrednost oz. pomen*
Osnovna polja v potrdilu	Standard fields in cert.	
različica X.509	Version	2 (kar pomeni verzijo 3)
identifikacijska oznaka potrdila	Serial Number	<enolična interna številka potrdila> (celo število)
algoritem za podpis	Signature algorithm	sha1WithRSAEncryption (OID 1.2.840.113549.1.1.5)
izdajatelj	Issuer	c=si, o=state-institutions, ou=sigov-ca
velja od - do	Validity	Not Before: <pričetek veljavnosti po GMT> Not After: <konec veljavnosti po GMT> (*glej razd. 3.1*) V formatu UTCTime– oblika LLMMDDuummssZ
imetnik	Subject	<razločevalno ime imetnika, ki vključuje naziv imetnika (in institucijo in serijsko številko (*glej razd. 3.3.3)*> Zapisano kot PrintableString
algoritem za javni ključ	Subject Public Key Algorithm	rsaEncryption (OID 1.2.840.113549.1.1.1)
javni ključ	Public Key (... bits)	< modul, eksponent,...>
Razširitve X509v3	X509v3 extensions	
OID 2.5.29.17 alternativno ime	Subject Alternative Name	<elektronski naslov imetnika oz. splošnega naziva oz. strežnika>
OID 2.16.840.1.113730.1.1 netscapeCertType	NetscapeCertType	<spletna>: SSLClient, S/MIME
		<spletna-strežnik>: SSL Server
OID 2.16.840.1.113730.1.2 izhodiščni URL	NetscapeBase URL	http://www.sigov-ca.gov.si/cda-cgi/
OID 2.16.840.1.113730.1.3 URL za preverjanje potrdila	NetscapeRevocation URL	clientcgi?action=checkRevocation&&CRL=cn=CRL1&serial=
OID 2.16.840.1.113730.1.13 opis potrdila	Netscape certificate comment	Opis potrdila, npr: Spletno kvalificirano digitalno potrdilo SIGOV-CA
OID 2.5.29.31 objava registra preklicanih potrdil	CRL Distribution Points	*Glej razd.3.3.4.*
OID 2.5.29.16 zasebni ključ za podpisovanje velja do	Private Key Usage Period	*Glej razd. 3.1.*
OID 2.5.29.15 uporaba ključa	Key Usage	<spletna>: Digital Signature, Key Encipherment
		<osebna - za verifikacijo podpisa>: Digital Signature
		<osebna - za šifriranje>: Key Encipherment
OID 2.5.29.35 identifikator izdajateljevega ključa	Authority Key Identifier	1EF8 D453 6BB3 8306 E904 0657 02F9 A5BF C658 3C72
OID 2.5.29.14 identifikator imetnikovega ključa	Subject Key Identifier	<identifikator imetnikovega ključa>

OID 2.5.29.32 politika, pod katero je bilo izdano potrdilo	certificatePolicies	*Glej razd. 3.1.* *npr.* Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6105.1.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.gov.si/ca/cps/
OID 2.5.29.19 osnovne omejitve	Basic Constraints	Če bi imetnik lahko deloval kot overitelj, bi bilo to označeno v tem polju, sedaj je prazno.
OID 1.2.840.113533.7.65.0 verzija Entrust	Entrust version extension	V5.0
Dodatna identifikacija (ni del digitalnega potrdila)		
razpoznavni odtis potrdila- MD5	Certificate Fingerprint – MD5	<razpoznavni odtis potrdila - MD5>
razpoznavni odtis potrdila – SHA1	Certificate Fingerprint – SHA1	<razpoznavni odtis potrdila - SHA1>

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 "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[3]	*razločevalno ime*
SIGEN-CA spletna za fizične osebe	c=si, o=state-institutions, ou=sigen-ca, ou=individuals, cn=<ime in priimek>, sn=<serijska številka>
SIGEN-CA spletna za zaposlene	c=si, o=state-institutions, ou=sigen-ca, ou=companies-web (*ali* ou=org-web), ou=<kratica org.>-<dav.št.>, cn=<ime in priimek>, sn=<serijska številka>
SIGEN-CA spletna za zaposlene (na področju lokalne samouprave, izobraževanja, zdravstava,…- samo za potrdila izdana po politiki 1.3.6.1.4.1.6105.2.1.1)	c=si, o=state-institutions, ou=sigen-ca, ou=org-web, ou=lsg (*ali* ou=edu *ali* ou=hlth), ou=<oznaka org.>-<dav.št.>, cn=<ime in priimek>, sn=<serijska številka>
SIGEN-CA spletna za spl. nazive	c=si, o=state-institutions, ou=sigen-ca, ou=companies-web (*ali* ou=org-web), ou=<oznaka org.>-<dav.št.>, cn=<sploš. naziv>, sn=<serijska številka>
SIGEN-CA spletna za strežnik	c=si, o=state-institutions, ou=sigen-ca, ou=companies-web (*ali* ou=org-web), ou=<oznaka org.>-<dav.št.>, cn=<sploš. naziv>, sn=<serijska številka>
SIGEN-CA osebna za zaposlene	c=si, o=state-institutions, ou=sigen-ca, ou=companies (*ali* ou=org), ou=<oznaka org.>-<dav.št.>, cn=<ime in priimek>, sn=<serijska številka>
SIGEN-CA osebna za zaposlene (na področju lokalne samouprave, izobraževanja, zdravstava,…- samo za potrdila izdana po politiki 1.3.6.1.4.1.6105.2.1.1)	c=si, o=state-institutions, ou=sigen-ca, ou=org, ou=lsg (*ali* ou=edu *ali* ou=hlth), ou=<oznaka org.>-<dav.št.>, cn=<ime in priimek>, sn=<serijska številka>
SIGEN-CA osebna za spl. nazive	c=si, o=state-institutions, ou=sigen-ca, ou=companies (*ali* ou=org), ou=<oznaka org.>-<dav.št.>, cn=<sploš. naziv>, sn=<serijska številka>
SIGOV-CA spletna za zaposlene	c=si, o=state-institutions, ou=web-certificates, cn=<ime in priimek>, sn=<serijska številka>
SIGOV-CA spletna za spl. nazive	c=si, o=state-institutions, ou=web-certificates, cn=<sploš. naziv>, sn=<serijska številka>
SIGOV-CA spletna za strežnik	c=si, o=state-institutions, ou=web-certificates, ou=servers, cn=<ime DNS>, sn=<serijska številka>
SIGOV-CA osebna za zaposlene	c=si, o=state-institutions, ou=certificates, ou=<oznaka inst.>, cn=<ime in priimek>, sn=<serijska številka>
SIGOV-CA osebna za spl. nazive	c=si, o=state-institutions, ou=certificates, ou=< oznaka inst.>, cn=<sploš. naziv>, sn=<serijska številka>

Opozoriti je potrebno sledeče:

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

- 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 osebna za zaposlene	2xxxxxx20yyz
SIGEN-CA osebna za splošne nazive	2xxxxxx22yyz
SIGEN-CA osebna 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 osebna za zaposlene	1xxxxxx20yyz
SIGOV-CA osebna za splošne nazive	1xxxxxx22yyz
SIGOV-CA osebna za strežnik	1xxxxxx24yyz
SIGOV-CA osebna za strežnike za TSA[4]	1xxxxxx26yyz

Opozoriti je potrebno sledeče:

- v primeru službenih potrdi (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.

[4] storitev omogočena z naslednjo verzijo politike SIGOV-CA

- 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 CVI. Serijska številka je namenjena predvsem za namen avtentikacije oz. vzpostavitve sheme dostopnih pravic.

3.3.4 Objava registra preklicanih potrdil

Glej razdelek 3.4.

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> 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> 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. 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:* • 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?base • Url: http://www.sigen-ca.si/crl/sigen-ca.crl
SIGOV-CA	*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?base • Url: http://www.sigov-ca.gov.si/crl/sigov-ca.crl

V samih digitalnih potrdilih je objava registrov CRL prikazana spodnji tabeli.

potrdila po politiki (OID)	*objavljeno v potrdilu*
SIGEN-CA • •	• 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
SIGEN-CA • •	• 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
SIGOV-CA • •	• 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
SIGOV-CA • •	• 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

3.4.2 Čas objave CRL

CRL se v imeniku objavlja enkrat dnevno oziroma po vsakem preklicu digitalnega potrdila. Čas izdaje naslednjega registra ("nextUpdate") je lahko nerelevanten, če pride do novega preklica potrdila. Novi CRL se v takem primeru objavi pred iztekom starega, 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, ostanejo objavljena na registru CRL.

3.4.4 "OCSP"

Preverjanja CRL po protokolu OCSP (angl. *On-line Certificate Status Protocol*) zaenkrat še ni omogočeno.

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 CVI in enolično povezani s serijsko številko digitalnega potrdila. Dostop do teh podatkov je mogoč za tretje osebe ob zakonski podlagi in ob sklenitvi medsebojnih razmerij v obliki pogodbe.

vrsta potrdila[5]	*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 strežnik	serijska številka – davčna št. skrbnika – EMŠO skrbnika – davčna št. organizacije – matična št. organizacije
SIGOV-CA za zaposlene	serijska številka – davčna št. imetnika – EMŠO imetnika - davčna št. institucije – matična št. institucije
SIGOV-CA za splošne nazive	serijska številka – davčna št. skrbnika – EMŠO skrbnika – davčna št. institucije – matična št. institucije
SIGOV-CA za strežnik	serijska številka – davčna št. skrbnika – EMŠO skrbnika – davčna št. institucije – matična št. institucije

Specifikacije za dostop do podatkov za tretje osebe so določene ob sklenitvi medsebojne pogodbe oz. drugače določenega dogovora.

4. HRAMBA DIGITALNIH POTRDIL

Na strani uporabnika so kriptografski ključi in digitalna potrdila hranjena 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** - osebna digitalna potrdila prevzeta z programsko opremo Entrust/Entelligence,
- **Microsoft Certificate Store** – spletna digitalna potrdila prevzeta z brskalnikom Microsoft IE,
- **Netscape Navigator Certificate Store** – spletna potrdila prevzeta z brskalniki Netscape 4.X,
- **Network Security Services (NSS)** – spletna digitalna potrdila prevzeta z Netscape 6/7 in brskalniki Mozilla,
- **Pametne kartice** – digitalna potrdila prevzeta z Entrust/Entelligence, brskalniki Microsoft IE Netscape.

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 Certificate Store	Microsoft CryptoAPI

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

Netscape Navigator Certificate Store	Netscape API
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 kot datoteko na disku (končnica .epf), ali pa na pametni kartici. Entrust aplikacije uporabljajo PKCS#11 standard 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 MS IE spletne brskalnike in MS operacijske sisteme (Windows 95, 98, 2000, NT, XP).

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 brskalniki MS IE in Netscape ter uvoz na pametne kartice.

4.5. Network Security Services (NSS)

Network Security Services (NSS) opensource koda vsebuje nabor knjižnic, ko omogočajo razvoj za razvoj cross-platform aplikacij, tako na strani odejmalca, 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 osebnih potrdil (Entrust Enterprise ID) hranjenih na pametnih karticah v

aplikacijah MS CryptoAPI[6]

Osebna potrdila shranjena na pametni kartici (Entrust Enterprise ID profil shranjen na pametni kartici) je možno uporabiti tudi v aplikacijah MS CAPI. To je možno le, če so izpolnjeni sledeči pogoji:

- Osebno potrdilo je prevzeto na kartico z odjemalcem Entrust Entelligence verzije 6.1 SP1 ali novejšim;
- Uporabljena pametna kartica podpira tako imenovani dual-head, oziroma hkratni dostop do kartice preko PKCS#11 in MS CryptoAPI.

Po sinhronizaciji osebnih potrdil na kartici z MS shrambo potrdil (Certificate Sote), je iz aplikacij, ki podpirajo MS CryptoAPI, možno uporabiti obe osebni potrdili (potrdilo za preverjanje podpisa in potdilo za šifriranje). Pri sinhronizaciji potrdil na kartici z MS shrambo potrdil, se iz kartice prenesejo v MS shrambo potrdil samo potrdila. Zasebni ključi ostanejo na pametni kartici. Aplikacije dostopajo do kriptografskih servisov, ki uporabljajo zasebni ključ, na kartici preko modula MS CryptoAPI CSP (Cryptographic Service Provider) za specifično pametno kartico.

5. IZBIRA MED OSEBNIMI 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 1024-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 S/MIME obliki so standardna, ne glede ali se uporabi spletno ali "osebno" digitalno potrdilo. Tako lahko S/MIME za sporočilo, podpisano in/ali šifrirano s spletnim digitalnim potrdilom, preveri podpis in/ali ga dešifrira odjemalec, ki uporablja osebno digitalno potrdilo.

Spletna digitalna potrdila znajo uporabljati:

- Netscape Communicator v 4.x (Linux, različne verzije unix-ov, MS Win, ...)
- MS Internet Explorer v 5.x in višje
- Netscape 7.x
- Mozilla 1.x in višje
- Opera 6.x in višje
- Lotus Notes Domino
- MS Information Server
- vsi produkti, ki uporabljajo open_ssl:
    - spletni strežnik Apache z modulom mod_ssl,
    - sendmail seja SSL,
    - openldap seja SSL,
    - posfix seja SSL,
    - freeswan IPSEC/VPN ,
    - cyrus imap4 deamon (seja SSL).
- in še mnogo drugih produktov.

5.2. Osebna potrdila

Osebna digitalna potrdila so namenjena aplikacijam v državni upravi in pri poslovnih subjektih. Uporabna so tudi za S/MIME. Ta oprema mora podpirati ločena para ključev za podpisovanje in šifriranje. Omogočati mora tudi, da se da

[6] deluje tudi z Entrust 5.X CA-jem, sinhronizacija, oziroma export v PKCS#12 je možen od CA v6 dalje

zasebni ključ za šifriranje restavrirati, če postane neuporaben. To je potrebno zato, da ne bi izgubili pomembnih službenih zašfriranih podatkov. Uporabniki na svojih delovnih postajah zaenkrat uporabljajo programsko opremo Entrust/Entelligence, ki deluje na Oknih od 95 navzgor, poleg tega še na Macintosh Power PC od 7.5 navzgor. V kratkem pa bo omogočen tudi izvoz osebnih potrdil v format PKCS#12, ali MS CAPI, kar pomeni tudi možnost uporabe po ustreznih protokolih oz. odjemalcih (npr. brskalnikih,...):

- Izvoz v format PKCS#12 ali MS CAPI je možen le za osebno potrdilo (Entrust ID), shranjeno na disku (datoteka epf). Pogoj je ustrezna infrastruktura Overitelja (Entrust/Authority v6.X, ki pa trenutno še ni uporabljena) in uporabe programske opreme Entelligence v6.X.
- Osebno potrdilo, shranjeno na pametni kartici, je možno uporabljati tudi v aplikacijah, ki podpirajo MS CAPI. To je možno, če so izpolnjeni sledeči pogoji: pametna kartica podpira "dual-head" (hkraten dostop do podatkov na kartici preko PKCS#11 in MS CAPI), osebno potrdilo pa mora biti prevzeto na pametno kartico z Entelligence v 6.1 SP1 (CA je lahko 5.X).

Osebno 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 javnem imeniku X500).

V primeru, da se zasebni ključ za dešifriranje izgubi/uniči, se preko posebnega postopka, ki je podoben prevzemu digitalnega potrdila, regenerira osebno 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 zgenerira nov par ključev.

Teh lastnosti spletno digitalno potrdilo nima, tudi jih nima noben neplačljiv produkt, zato je potrebno imeti poseben odjemalec. Za informacijo o razvojnih orodjih za uporabo osebnih digitalnih potrdil se obrnite na pooblaščene osebe Overitelja.

Razlike med osebnimi 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 CVI

Overitelj na CVI 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 Triple DES, CAST-128 in RC2, (standardi FIPS PUB 81, ANSI X3.106 in ISO/IEC 10116), AES (od v6.0 dalje)
- 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.