Overitelj na Ministrstvu za javno upravo SIGEN-CA

POLITIKA SIGEN-CA

za spletna kvalificirana digitalna potrdila za fizične osebe

Javni del notranjih pravil overitelja na Ministrstvu za javno upravo

veljavnost: od 18. maja 2007
verzija: 3.1

CP_{OID}: 1.3.6.1.4.1.6105.2.2.3.1
CP_{Name}: SIGEN-CA-2

Izdaje politik delovanja SIGEN-CA	
verzija: 3.1, veljavnost**:** od 18. maja 2007	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP_{OID}: 1.3.6.1.4.1.6105.2.2.3.1 CP_{Name}: SIGEN-CA-2	*Spremembe z verzijo 3.1:* - *izdajatelj SIGEN-CA bodočemu imetniku potrdila avtorizacijske kode ne posreduje več po priporočeni pošti temveč z navadno poštno pošiljko;* - *oddaja zahtevka za pridobitev digitalnega potrdila je omogočena tudi na elektronski način z veljavnim kvalificiranim digitalnim potrdilom za fizične osebe, izdanim s strani izdajatelja SIGEN-CA;* - *omogočena je predhodna pridobitev novega potrdila pred potekom veljavnosti prejšnjega;* - *prijavne službe overitelja morajo pri svojem delu upoštevati poslovnike za delo prijavnih služb.*
verzija: 3.0, veljavnost: od 28. februarja 2006	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP_{OID}: 1.3.6.1.4.1.6105.2.2.3 CP_{Name}: SIGEN-CA-2	*Spremembe z verzijo 3.0:* - *uporaba novega naziva za overitelja na Centru Vlade za informatiko, po novem je to »Overitelj na Ministrstvu za javno upravo«;* - *osebna kvalificirana digitalna potrdila se po novem imenujejo »posebna kvalificirana digitalna potrdila«;* - *preklic je po novem mogoč samo v času uradnih ur, razen v nujnih primerih;* - *uporaba novega naziva za imetnike SIGEN-CA, in sicer za imetnike »pravnih in fizičnih oseb, registriranih za opravljanje dejavnosti« uporablja izraz »poslovni subjekti«;* - *struktura dokumenta je v skladu s priporočili RFC 3647.*
verzija: 2, veljavnost: od 15. julija 2002	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP_{OID}: 1.3.6.1.4.1.6105.2.2.2 CP_{Name}: SIGEN-CA-2	/
verzija: 1, veljavnost: od 9. julija 2001	
Politika SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe CP_{OID}: 1.3.6.1.4.1.6105.2.2.1 CP_{Name}: SIGEN-CA-2	/

VSEBINA

POVZETEK

Politike overitelja kvalificiranih digitalnih potrdil in varnih časovnih žigov (v nadaljevanju *overitelj*) na Ministrstvu za javno upravo (v nadaljevanju *MJU*) predstavljajo celoten javni del notranjih pravil overitelja na MJU in določajo namen, delovanje in metodologijo upravljanja s kvalificiranimi digitalnimi potrdili, dodeljevanje časovnih žigov, odgovornost overitelja na MJU ter zahteve, ki jih morajo izpolnjevati uporabniki in tretje osebe, ki uporabljajo in se zanašajo na kvalificirana digitalna potrdila in na varne časovne žige, in drugi overitelji, ki želijo uporabljati storitve overitelja na MJU.

Overitelj na MJU izdaja kvalificirana digitalna potrdila in varne časovne žige, za katera velja najvišja stopnja varovanja ter deluje v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 57/2000, 25/2004 in 98/2004) in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000 in 2/2001), evropskimi direktivami ter drugimi veljavnimi predpisi in priporočili.

Kvalificirana digitalna potrdila, ki jih izdaja overitelj na MJU, so namenjena:
- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba digitalnih potrdil overitelja na MJU,
- 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.

Izdajatelj SIGEN-CA (angl. *Slovenian General Certification Authority*), http://www.sigen-ca.si, izdaja kvalificirana digitalna potrdila za poslovne subjekte in fizične osebe, in deluje v okviru overitelja na MJU, http://www.ca.gov.si.

Izdajatelj SIGEN-CA je registriran v skladu z veljavno zakonodajo in medsebojno priznan z izdajateljem kvalificiranih digitalnih potrdil za državne organe SIGOV-CA (angl. *Slovenian Governmental Certification Authority*), http://www.sigov-ca.gov.si.

Pričujoči dokument določa politike izdajatelja SIGEN-CA za kvalificirana digitalna potrdila za fizične osebe. Na podlagi tega dokumenta SIGEN-CA izdaja spletna kvalificirana digitalna potrdila, ki izpolnjujejo najvišje varnostne zahteve, po politiki CP_{OID}: 1.3.6.1.4.1.6105.2.2.3.1.

Pričujoči dokument nadomešča objavljeni politiki SIGEN-CA za fizične osebe. Vsa kvalificirana digitalna potrdila, izdana po datumu veljavnosti nove politike, se obravnavajo po novi politiki, za vsa ostala pa velja, da se obravnavajo po novi politiki glede tistih določil, ki lahko smiselno nadomestijo oz. dopolnijo določila iz politike, po kateri je bilo kvalificirano digitalno potrdilo izdano (na primer postopek za preklic velja po novi politiki).

Spremembe, ki jih prinaša nova politika, so sledeče:
- V primeru odobrenega zahtevka za pridobitev kvalificiranega digitalnega potrdila izdajatelj SIGEN-CA posreduje bodočemu imetniku potrdila avtorizacijsko kodo z navadno poštno pošiljko in ne več po priporočeni pošti.
- Oddaja zahtevka za pridobitev digitalnega potrdila je omogočena tudi na elektronski način z veljavnim kvalificiranim digitalnim potrdilom za fizične osebe, ki ga je imetniku izdal izdajatelj SIGEN-CA.
- Novo kvalificirano digitalno potrdilo je mogoče pridobiti že pred potekom veljavnosti predhodnega kvalificiranega digitalnega potrdila.
- Organizacije, ki opravljajo naloge prijavne službe, morajo pri svojem delu upoštevati poslovnike za delo prijavnih služb overitelja na MJU.

Kvalificirana digitalna potrdila se pridobijo na podlagi zahtevka, ki ga mora podpisati bodoči imetnik. Izpolnjen zahtevek se odda osebno na prijavno službo (seznam je objavljen na spletni strani http://www.sigen-ca.si/prijavne-slu.htm) ali pa se zahtevek digitalno podpiše z veljavnim kvalificiranim digitalnim potrdilom za fizične osebe, ki ga je imetniku izdal izdajatelj SIGEN-CA. Digitalno podpisan zahtevek se po elektronski poti posreduje izdajatelju SIGEN-CA.

SIGEN-CA na podlagi odobrenega zahtevka pripravi referenčno številko in avtorizacijsko kodo, ki sta unikatni za vsakega bodočega imetnika kvalificiranega digitalnega potrdila in ju bodoči imetnik potrebuje za prevzem svojega potrdila, ki ga opravi na svoji delovni postaji v skladu z navodili izdajatelja SIGEN-CA. Bodoči imetnik prejme referenčno številko po elektronski pošti, avtorizacijsko kodo pa s poštno pošiljko na svoj stalni ali drug izbran naslov.

Spletno kvalificirano digitalno potrdilo je povezano z enim parom ključev, ki se tvori z imetnikovo programsko ali strojno opremo. SIGEN-CA nikoli ne hrani in tudi nima dostopa do zasebnega ključa. Javni ključ se pošlje izdajatelju SIGEN-CA, ki izda potrdilo, katerega sestavni del je javni ključ. Spletno potrdilo se shrani pri imetniku, dostopno pa je tudi v javnem imeniku potrdil.

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

Imetnik mora skrbno varovati zasebne ključe in svoje kvalificirano digitalno potrdilo ter ravnati v skladu s politiko, obvestili izdajatelja SIGEN-CA in veljavno zakonodajo.

1. UVOD

1.1. Pregled

(1) V okviru Ministrstva za javno upravo (v nadaljevanju *MJU*) deluje overitelj digitalnih potrdil in varnih časovnih žigov (v nadaljevanju *overitelj na MJU*), ki je v skladu z Zakonom o državni upravi (Uradni list RS, št. 52/2002, 56/2003, 61/2004, 123/2004; ZDU-1) in Sklepom o spremembah Sklepa o organizaciji in delovnem področju Centra Vlade Republike Slovenije za informatiko (Uradni list RS, št. 132/2004), iz vladne službe Centra Vlade za informatiko prešel pod okrilje novoustanovljenega Ministrstva za javno upravo.

(2) Politike overitelja kvalificiranih digitalnih potrdil in varnih časovnih žigov na Ministrstvu za javno upravo predstavljajo celoten javni del notranjih pravil overitelja na MJU in določajo namen, delovanje in metodologijo upravljanja s kvalificiranimi digitalnimi potrdili, dodeljevanje časovnih žigov, odgovornost overitelja na MJU ter zahteve, ki jih morajo izpolnjevati imetniki, uporabniki in tretje osebe, ki se zanašajo na kvalificirana digitalna potrdila in na varne časovne žige, in drugi overitelji, ki želijo uporabljati storitve overitelja na MJU.

(3) Overitelj na MJU izdaja kvalificirana digitalna potrdila in varne časovne žige, za katera velja najvišja stopnja varovanja ter deluje v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 57/2000, 25/2004 in 98/2004) in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000 in 2/2001), evropskimi direktivami ter drugimi veljavnimi predpisi in priporočili.

(4) Kvalificirana digitalna potrdila (v nadaljevanju *potrdila*), ki jih izdaja overitelj na MJU so namenjena:
- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba potrdil overitelja na MJU,
- za varno elektronsko komuniciranje med imetniki potrdil overitelja na MJU in
- za storitve oz. aplikacije, za katere se zahteva uporaba teh potrdil.

(5) Varni časovni žigi overitelja na MJU so namenjeni:
- zagotavljanju obstoja dokumenta v določenem časovnem trenutku in sicer tako, da se poveže datum in čas žigosanja z vsebino dokumenta na kriptografsko varen način,
- povsod, kjer je potrebno na varen način dokazati časovne lastnosti transakcij in drugih storitev,
- za druge potrebe, kjer se potrebuje varni časovni žig.

(6) Izdajatelj SIGEN-CA (angl. *Slovenian General Certification Authority*), http://www.sigen-ca.si, izdaja kvalificirana digitalna potrdila za poslovne subjekte in fizične osebe, in deluje v okviru overitelja na MJU, http://www.ca.gov.si. Pričujoči dokument določa politike izdajatelja SIGEN-CA za kvalificirana digitalna potrdila za fizične osebe.

(7) Izdajatelj SIGEN-CA je registriran v skladu z veljavno zakonodajo in medsebojno priznan z izdajateljem kvalificiranih digitalnih potrdil za državne organe SIGOV-CA (angl. *Slovenian Governmental Certification Authority*), http://www.sigov-ca.gov.si.

(8) Po pričujoči politiki SIGEN-CA izdaja spletna kvalificirana digitalna potrdila za fizične osebe po CP_{OID}: 1.3.6.1.4.1.6105.2.2.3.1.

(9) Spletna kvalificirana digitalna potrdila SIGEN-CA se lahko uporabljajo za:
- šifriranje podatkov v elektronski obliki,
- overjanje digitalno podpisanih podatkov v elektronski obliki ter izkazovanje istovetnosti imetnika,
- storitve oz. aplikacije, za katere se zahteva uporaba kvalificiranih digitalnih potrdil overitelja na MJU.

(10) Za potrdila, izdana na podlagi tej politike, je potrebno upoštevati priporočila izdajatelja SIGEN-CA za zaščito zasebnih ključev oz. uporabo varnih kriptografskih modulov.

(11) Pričujoča politika je pripravljena skladno s priporočilom RFC 3647 »Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework«.

(12) Medsebojna razmerja med tretjimi osebami, ki se zanašajo na potrdila izdajatelja SIGEN-CA, in overiteljem na MJU izvajajo tudi na podlagi pisnega dogovora.

(13) Overitelj na MJU se lahko povezuje v mrežo overiteljev na horizontalni ali vertikalni ravni, kar se ureja z medsebojnim pisnim dogovorom.

1.2. Identifikacijski podatki politike delovanja

(1) Oznaka pričujoče politike delovanja SIGEN-CA je:
- CP_{OID}: 1.3.6.1.4.1.6105.2.2.3.1.

(2) V vsakem potrdilu je navedba ustrezne politike v obliki oznake CP_{OID}, glej razd. 7.1.2.

1.3. Subjekti

1.3.1 Overitelj na MJU in izdajatelj SIGEN-CA

(1) Overitelj na MJU izdaja kvalificirana digitalna potrdila in varne časovne žige, za katera velja najvišja stopnja varovanja ter deluje v skladu z veljavnimi predpisi in priporočili.

(2) Kontaktni podatki overitelja na MJU so podani spodaj:

Naslov:	Overitelj na Ministrstvu za javno upravo Ministrstvo za javno upravo Tržaška cesta 21 1000 Ljubljana
Telefon:	01 4788 600
Fax:	01 4788 649
Spletna stran:	http://www.ca.gov.si

(3) V okviru overitelja na MJU deluje izdajatelj kvalificiranih digitalnih potrdil SIGEN-CA.

(4) Kontaktni podatki izdajatelja SIGEN-CA so podani spodaj:

Naslov:	SIGEN-CA Overitelj na Ministrstvu za javno upravo Ministrstvo za javno upravo Tržaška cesta 21 1000 Ljubljana
E-pošta:	sigen-ca@gov.si
Telefon:	01 4788 600
Fax:	01 4788 649
Spletna stran:	http://www.sigen-ca.si
Dežurna tel. številka za preklice (24 ur vse dni v letu):	01 4788 777
Center za podporo uporabnikom:	01 4788 590 evt@gov.si

(5) Izdajatelj SIGEN-CA opravlja naslednje naloge:
- izdaja kvalificirana digitalna potrdila,
- določa in objavlja svojo politiko delovanja,
- določa obrazce za zahtevke za svoje storitve,
- objavlja navodila in priporočila za varno uporabo svojih storitev,
- skrbi za javni imenik potrdil,
- objavlja register preklicanih potrdil,
- skrbi za nemoteno delovanje svojih storitev v skladu s politiko,
- obvešča svoje uporabnike,
- skrbi za delovanje svoje prijavne službe,
- in opravlja vse ostale storitve v skladu s politiko in ostalimi predpisi.

(6) Izdajatelj SIGEN-CA je ob začetku svojega produkcijskega delovanja generiral svoje lastno digitalno potrdilo, ki je namenjeno overjanju potrdil, ki jih je SIGEN-CA izdal imetnikom.

Potrdilo SIGEN-CA vsebuje naslednje podatke[1]:

Naziv polja	Vrednost potrdila izdajatelja SIGEN-CA
Različica, angl. *Version*	2 (*kar pomeni verzijo 3*)
Identifikacijska oznaka, angl. *Serial Number*	3B3C F9C9
Algoritem podpis, angl. *Signature Algorithm*	sha1WithRSAEncryption
Izdajatelj, angl. *Issuer*	c=si, o=state-institutions, ou=sigen-ca
Imetnik, angl. *Subject*	c=si, o=state-institutions, ou=sigen-ca
Pričetek veljavnosti, angl. *Validity: Not Before*	Jun 29 21:27:46 2001 GMT
Konec veljavnosti, angl. *Validity: Not After*	Jun 29 21:57:46 2021 GMT
Algoritem za javni ključ, angl. *Public Key Algorithm*	rsaEncryption
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritmom RSA, angl. *RSA Public Key*	*ključ dolžine 2048 bitov*
Identiteta ključa (po alg. SHA-1), angl. *Subject Key Identifier*	717B 8A06 1F31 0555 AB60 1277 4720 1E03 8818 EC89
Odtis potrdila (ni del potrdila)	
Odtis potrdila MD-5, angl. *Certificate Fingerprint – MD5*	49EF A6A1 F0DE 8EA7 6AEE 5B7D 1E5F C446
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA1*	3E42 A187 06BD 0C9C CF59 4750 D2E4 D6AB 0048 FDC4
Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA256*	12D4 80C1 A3C6 6478 1B99 D9DF 0E9F AF3F 1CAC EE1B 3C30 C312 3A33 7A4A 454F FED2

[1] Pomen je podan v podpogl. 3.1 in 7.1.

1.3.2 Prijavna služba SIGEN-CA

(1) Organizacije, ki opravljajo naloge prijavne službe, pooblasti overitelj na MJU. Izpolnjevati morajo pogoje za opravljanje nalog prijavnih služb overitelja na MJU ter delovati v skladu z veljavnimi predpisi in poslovniki za delo prijavnih služb overitelja na MJU.

(2) Naloge prijavne službe so:
- preverjanje istovetnosti imetnikov oz. bodočih imetnikov, njihovih podatkov in drugih potrebnih podatkov,
- sprejemanje zahtevkov za pridobitev potrdil,
- sprejemanje zahtevkov za preklic potrdil,
- preverjanje podatkov v zahtevkih,
- izdajanje potrebne dokumentacije imetnikom oz. bodočim imetnikom,
- posredovanje zahtevkov in ostalih podatkov na varen način na SIGEN-CA.

(3) Izdajatelj SIGEN-CA ima vzpostavljene prijavne službe na različnih lokacijah, podatki o tem pa so objavljeni na spletnih straneh SIGEN-CA.

1.3.3 Imetniki potrdil

Imetniki potrdil po tej politiki so vedno fizične osebe (angl. *subject*), glej definicijo v pogl. 1.6

1.3.4 Tretje osebe

(1) Tretje osebe so pravne ali fizične osebe, ki se zanašajo na izdana potrdila izdajatelja SIGEN-CA.

(2) V ta namen se morajo ravnati po navodilih izdajatelja SIGEN-CA in morajo vedno preveriti veljavnost potrdila, namen uporabe potrdila, čas veljavnosti potrdila itd. Podrobnejše obveznosti in odgovornosti tretjih oseb so navedene v razd. 4.5.2 in 9.6.4.

(3) Tretje osebe niso nujno tudi imetniki potrdil izdajatelja SIGEN-CA ali digitalnih potrdil drugih izdajateljev.

(4) Med tretjo osebo in izdajateljem SIGEN-CA oz. overiteljem na MJU se lahko sklene medsebojni pisni dogovor.

1.3.5 Ostali udeleženci

Niso predvideni.

1.4. Namen uporabe

(1) Spletna potrdila SIGEN-CA izdana po pričujoči politiki se lahko uporabljajo za:
- šifriranje podatkov v elektronski obliki,
- overjanje digitalno podpisanih podatkov v elektronski obliki ter izkazovanje istovetnosti podpisnika,
- storitve oz. aplikacije, za katere se zahteva uporaba kvalificiranih digitalnih potrdil overitelja na MJU.

(2) Namen potrdil oz. pripadajočih ključev je podan v potrdilu v polju *namen uporabe* (angl. *key usage*).

1.4.1 Pravilna uporaba potrdil in ključev

Vsakemu imetniku potrdila pripada en par ključev, ki ga sestavljata zasebni in javni ključ, ki sta namenjena za podpisovanje/overjanje podpisa in dešifriranje/šifriranje podatkov.

1.4.2 Nedovoljena uporaba

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

(2) Drugih prepovedi v zvezi z uporabo potrdil izdajatelja SIGEN-CA ni.

1.5. Upravljanje dokumentacije

1.5.1 Upravljavec politik

Z dokumentacijo upravlja izdajatelj SIGEN-CA oz. overitelj na MJU.

1.5.2 Pooblaščene osebe za politiko

Pooblaščene osebe v zvezi s politiko in ostalo dokumentacijo so pooblaščene osebe overitelja na MJU.

1.5.3 Odgovorna oseba glede skladnosti delovanja izdajatelja SIGEN-CA s politiko

Odgovorne osebe glede skladnosti delovanja so pooblaščene osebe overitelja na MJU v skladu z nalogami, ki jih opravljajo v okviru organizacijskih skupin (glej razd. 5.2.1).

1.5.4 Postopek za sprejem nove politike

(1) Overitelj na MJU si pridržuje pravico do spremembe tega dokumenta brez predhodnega obveščanja imetnikov potrdil SIGEN-CA, v kolikor spremembe ne vplivajo na namen uporabe in postopke upravljanja, ki lahko spremenijo nivo zaupanja.

(2) Spremembe politike overitelja na MJU se sedem (7) dni pred veljavo predhodno objavi na spletnih straneh overitelja na MJU pod novo identifikacijsko številko (CP_{OID}) in označenim datumom začetka njene veljavnosti. V tem času lahko imetniki oz. bodoči imetniki podajo svoje pripombe, ki jih obravnavajo pooblaščene osebe overitelja na MJU.

(3) Overitelj lahko izda tudi amandmaje k politiki, glej podpogl. 9.12.

(4) Skladno z ZEPEP se prijava novosti storitev overitelja na MJU opravi tudi na pristojno ministrstvo za register overiteljev v Republiki Sloveniji.

(5) Novo politiko oz. amandmaje potrdi minister za javno upravo.

1.6. Okrajšave in izrazi

1.6.1 Okrajšave

CA	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi, angl. *Certification Authority.*
CP_{Name}	Ime politike delovanja overitelja oz. izdajatelja (angl. *Certification Policy Name*), povezano z mednarodno številko politike delovanja (primerjaj okrajšavo CP_{OID}).
CP_{OID}	Mednarodna številka, ki enolično določa politiko delovanja, v skladu z mednarodnim standardom ITU-T priporočili X.208 (ASN.1), angl. *Certification Policy Object IDentifier.*
CRL	Seznam preklicanih potrdil (CRL, angl. *Certification Revocation List*) (primerjaj izraz *Register preklicanih potrdil*).
DNS	Baza imen računalnikov, ki so vključeni v internet. Omogoča povezave imen računalnikov z njihovimi številkami IP (DNS, angl. *Domain Name System*).
ETSI	Mednarodna priporočila za področje telekomunikacij, angl. *European Telecommunications Standards Institut,* http://www.etsi.org.
LDAP	Protokol, ki določa dostop do imenika in je specificiran po IETF (angl. *Internet Engineering Task Force*) priporočilu RFC 1777 »Leightweight Directory Access Protocol«.
MJU	Ministrstvo za javno upravo, Tržaška cesta 21, 1000 Ljubljana.
PKCS#7 in PKCS#10	Priporočila (angl. *Public Key Cryptography Standards*) podjetje RSA Security za razvijalce računalniških sistemov, ki uporabljajo asimetrične kriptografske algoritme. • PKCS#7 določa sintakso za kriptografsko obdelane podatke, kot so digitalni podpisi in digitalne ovojnice. Uporablja se npr. za pošiljanje digitalnih potrdil in seznamov preklicanih potrdil. • PKCS#10 določa sintakso za zahtevek za overitev javnega ključa, imena in drugih atributov.
PKI	Infrastruktura javnih ključev, angl. *Public Key Infrastructure.*
RFC	Mednarodna priporočila za Internet skupine IETF, angl. *Internet Engineering Task Force* in IESG, angl. *Internet Engineering Steering Group*, angl. *Request for Comments*, http://www.ietf.org/rfc.html.
X.501	Priporočila za razločevalna imena: »ITU-T Recommendation X.501 - Information technology - Open Systems Interconnection - The Directory: Models«.
X.509	Priporočila za profil digitalnih potrdil in registra preklicanih potrdil: RFC 3280: »Internet X.509 Public Key Infrastructure Certificate and CRL Profile«.
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 57/2000, 25/2004 in 98/2004).

1.6.2 Izrazi

(1) Splošni izrazi, ki se uporabljajo v tej politiki, so naslednji.

Digitalni podpis	Varen elektronski podpis, ki izpolnjuje zahteve 2. člena ZEPEP in 25.

	člena Uredbe.
Kvalificirano digitalno potrdilo	Kvalificirano digitalno potrdilo, ki izpolnjuje zahteve iz 28. člena ZEPEP in ki ga izda overitelj, ki deluje v skladu z zahtevami iz 29. do 36. člena ZEPEP in Uredbo (primerjaj *ZEPEP* in *Uredba*).
Overitelj	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi in ki izpolnjuje zahteve overiteljev kvalificiranih potrdil v skladu z Uredbo in ZEPEP (primerjaj okrajšavo *CA* in izraz *Potrdila*).
Tretja oseba	Pravna ali fizična osebe, ki se zanaša na izdana digitalna potrdila oz. na digitalni podpis, ki ga lahko verificira s pomočjo javnega ključa, ki se nahaja v digitalnem potrdilu.
Uredba	Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000 in 2/2001).

(2) Drugi izrazi so podani v spodnji tabeli.

Imetnik	Fizična oseba, ki želi pridobiti in uporabljati kvalificirana digitalna potrdila (angl. *subject*), in je državljan Republike Slovenije oz. tujec s stalnim ali začasnim prebivališčem v Republiki Sloveniji.
Infrastruktura overitelja na MJU	Vsi prostori overitelja, njegova strojna in programska oprema ter varnostni mehanizmi, ki so potrebni za varno delovanje njegovih izdajateljev.
Interna politika overitelja na MJU	Zaupni del notranjih pravil delovanja overitelja na Ministrstvu za javno upravo v skladu z Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000 in 2/2001).
Izdajatelj SIGEN-CA	V okviru overitelja na MJU deluje več izdajateljev. Le-ti izdajajo bodisi kvalificirana digitalna potrdila bodisi varne časovne žige. (primerjaj izraz *Overitelj na MJU*). SIGEN-CA je izdajatelj potrdil za pravne in fizične osebe, angl. *Slovenian General Certification Authority*, http://www.sigen-ca.si.
Javni imenik	Javni imenik, s katerim upravlja izdajatelj SIGEN-CA, je vzpostavljen na strežniku *x500.gov.si*, in sicer po standardu X.500. V imeniku se objavljajo kvalificirana digitalna potrdila, ki jih izdaja SIGEN-CA, ter register preklicanih potrdil.
Objava SIGEN-CA	Javna objava na spletnih straneh SIGEN-CA oz. na straneh overitelja na MJU, http://www.sigen-ca.si oz. http://www.ca.gov.si.
Obvestila SIGEN-CA	Vsa navodila, pojasnila, seznami, pogoji, posamezna obvestila, priporočila, standardi in drugi dokumenti, ki jih določi ali priporoči SIGEN-CA oz. overitelj na MJU in jih objavi ali kako drugače posreduje svojim uporabnikom, t.j. imetnikom in tretjim osebam.
Overitelj na MJU	Overitelj digitalnih potrdil in varnih časovnih žigov na Ministrstvu za javno upravo. Overitelj se je zaradi reorganizacije v skladu z Zakonom o državni upravi (Uradni list RS, št. 52/2002, 56/2003, 61/2004, 123/2004; ZDU-1) in Sklepa o spremembah Sklepa o organizaciji in delovnem področju Centra Vlade Republike Slovenije za informatiko (Uradni list RS, št. 132/2004) preimenoval iz »Overitelja na Centru Vlade za informatiko« v »Overitelja na Ministrstvu za javno upravo«, http://www.ca.gov.si.
Potrdilo oz. spletno potrdilo	Spletno kvalificirano digitalno potrdilo v elektronski obliki, ki povezuje podatke iz potrdila z imetnikovim zasebnim ključem ter potrjuje imetnikovo istovetnost (angl. *web certificate*).
Prijavna služba SIGEN-CA	Po pooblastilu izdajatelja SIGEN-CA prijavna služba sprejema zahtevke za pridobitev in preklic potrdil ter preverja istovetnosti imetnikov oz. bodočih imetnikov (RA, angl. *Registration Authority*).

Zahtevek	Obrazec SIGEN-CA za pridobivanje ali preklic potrdil, ki je dostopen preko spletne strani SIGEN-CA oz. pri pooblaščenih osebah na prijavnih službah.

2. OBJAVE INFORMACIJ IN JAVNI IMENIK POTRDIL

2.1. Objava dokumentov in javni imenik

(1) Overitelj na MJU je odgovoren, da vse v zvezi z delovanjem SIGEN-CA, obvestila imetnikom in tretjim osebam SIGEN-CA objavlja javno na spletnih straneh SIGEN-CA, http://www.sigen-ca.si.

(2) Javno dostopni dokumenti so naslednji:
- politike delovanja izdajatelja,
- cenik,
- zahtevki za storitve izdajatelja,
- navodila za varno uporabo digitalnih potrdil,
- informacijo o veljavni zakonodaji v zvezi z delovanjem overitelja ter
- ostale informacije v zvezi z delovanjem SIGEN-CA.

(3) Javno pa niso dostopni dokumenti, ki predstavljajo zaupni del notranjih pravil overitelja na MJU.

(4) V strukturi javnega imenika digitalnih potrdil, ki se nahaja na strežniku *x500.gov.si, s*e objavljajo:
- evidenčni podatki o potrdilu (imetnikov naziv, naslov e-pošte, serijska številka ...),
- veljavna digitalna potrdila (podrobneje podana v podpogl. 7.1) in
- register preklicanih digitalnih potrdil (podrobneje podan v podpogl. 7.2).

2.2. Pogostnost objav

(1) Nove politike so objavljene v skladu z navedbo v podpogl. 9.10.

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

(3) Preklicana potrdila se v registru preklicanih potrdil objavijo takoj (podrobno o tem v razd. 4.9.8).

(4) Ostale javno dostopne informacije oz. dokumenti se objavijo po potrebi.

2.3. Dostop do informacij in javnega imenika potrdil

(1) Javni imenik, ki hrani potrdila, je javno dostopen na strežniku *x500.gov.si* po protokolu LDAP.

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

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

(3) Overitelj na MJU oz. izdajatelj SIGEN-CA v skladu z Interno politiko overitelja na MJU skrbi za pooblaščeno in varno dodajanje, spreminjanje ali brisanje podatkov v javnem imeniku potrdil.

3. ISTOVETNOST IMETNIKOV POTRDIL

3.1. Dodelitev imen

3.1.1 Razločevalna imena

(1) Vsako potrdilo vsebuje v skladu z RFC 3280 podatke o imetniku ter izdajatelju v obliki razločevalnega imena, ki je oblikovano v skladu z RFC 3280 in s standardom *X.501.*

(2) V vsakem izdanem potrdilu je naveden izdajatelj le-tega, in sicer v polju *izdajatelj* (angl. *issuer*), glej tabelo v nadaljevanju.

(3) Razločevalno ime imetnikov vsebuje osnovne podatke o imetniku, in sicer v polju *imetnik (*angl. *subject)*, glej tabelo v nadaljevanju.

(4) Vsako razločevalno ime vključuje tudi serijsko številko, ki jo določi izdajatelj SIGEN-CA[2] (glej razd. 3.1.5).

Vrsta potrdila	Naziv polja	Razločevalno ime[3]
potrdilo izdajatelja SIGEN-CA	Izdajatelj, angl. *Issuer* in Imetnik, angl. *Subject*	c=si, o=state-institutions, ou=sigen-ca
spletno potrdilo	Imetnik, angl. *Subject*	c=si, o=state-institutions, ou=sigen-ca, ou=individuals, cn=<ime in priimek>, sn=<serijska številka>

3.1.2 Zahteve pri tvorbi razločevalnega imena

(1) Imetnik potrdila je nedvoumno določen z razločevalnim imenom v skladu s prejšnjim razdelkom.

(2) Podatki o imetniku v razločevalnem imenu vsebujejo črke angleške abecede. Drugi znaki se pretvorijo po pravilih iz spodnje tabele.

Znak	Pretvorba
Č	C
Š	S
Ž	Z
Ü	Ue
Ö	Oe
Ø	Oe
ß	Ss
Ñ	N

[2] Potrdilo izdajatelja SIGEN-CA ne vsebuje serijske številke.
[3] Pomen posameznih označb: država (»c«), organizacija (»o«), organizacijska enota (»ou«), ime (»cn«), serijska številka (»sn«).

Ŕ	Rz

(3) V primeru drugih nepredvidenih znakov izdajatelj določi ustrezno kombinacijo črk iz angleške abecede.

3.1.3 Uporaba anonimnih imen ali psevdonimov

Ni predvidena.

3.1.4 Pravila za interpretacijo razločevalnih imen

Pravila so navedena v razd. 3.1.1 in 3.1.2.

3.1.5 Enoličnost razločevalnih imen

(1) Podeljeno razločevalno ime je enolično za vsako izdano potrdilo.

(2) Enolična je tudi serijska številka, ki je vključena v razločevalno ime.

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

Serijska številka	Pomen	Vrednost
1. mesto	oznaka za potrdilo, ki ga je izdal izdajatelj SIGEN-CA	2
2.- 8. mesto	enolično število imetnika	/
9. - 10. mesto	oznaka za spletno potrdilo za fizično osebo	12
11. – 12. mesto	zaporedno število istovrstnega potrdila	/
13. mesto	kontrolna številka	/

3.1.6 Zaščite imen oz. znamk

(1) Imetniki ne smejo zahtevati imen, ki bi pripadala nekomu drugemu in bi bile s tem kršene avtorske ali druge pravice tretjih oseb.

(2) Morebitne spore rešujeta izključno prizadeta stran in imetnik.

3.2. Preverjanje istovetnosti imetnikov ob prvi izdaji potrdila

3.2.1 Metoda za posedovanju pripadnosti zasebnega ključa

Dokazovanje o posedovanju zasebnega ključa, ki pripada javnemu ključu v potrdilu, je zagotovljeno z varnimi postopki pred in ob prevzemu potrdila ter protokolom PKCS#10.

3.2.2 Preverjanje istovetnosti organizacije

Ni predpisana.

3.2.3 Preverjanje istovetnosti imetnika

(1) Preverjanje istovetnosti imetnikov opravi prijavna služba overitelja na MJU.

(2) Izdajatelj SIGEN-CA preveri osebne podatke o imetniku v ustreznih registrih.

(3) Pri naslovu e-pošte imetnika izdajatelj SIGEN-CA preveri, ali je na zahtevku podani naslov e-pošte veljaven, in sicer na način, da SIGEN-CA pošlje obvestilo bodočemu imetniku ob sprejemu zahtevka. Če je to sporočilo zavrnjeno, prevzem potrdila ni mogoč.

3.2.4 Nepreverjeni podatki v potrdilih

Nepreverjenih podatkov v potrdilu ni.

3.2.5 Preverjanje pooblastil zaposlenih za pridobitev potrdil

Ni predpisano.

3.2.6 Medsebojno priznavanje

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

(2) Overitelj na MJU zagotavlja, da bo izvajal medsebojno priznavanje izključno po podpisu pisne pogodbe z drugimi overitelji, ki pa morajo izpolnjevati raven varnostnih zahtev, ki je primerljiva ali višja, kot jo predpiše overitelj na MJU.

(3) Pooblaščene osebe overitelja na MJU pregledujejo notranja pravila drugega overitelja ter njegovo izpolnjevanje varnostnih zahtev.

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

3.3. Preverjanje imetnikov za ponovno izdajo potrdila

3.3.1 Preverjanje imetnikov pri podaljšanju potrdil

(1) Istovetnost imetnikov pri ponovni izdaji spletnega potrdila se preverja bodisi na prijavni službi overitelja na MJU ali pa se ugotavlja na podlagi že izdanega veljavnega digitalnega potrdila za fizične osebe, ki ga je izdal izdajatelj SIGEN-CA.

(2) Izdajatelj SIGEN-CA preveri osebne podatke o imetniku v ustreznih registrih.

(3) Pri naslovu e-pošte imetnika izdajatelj SIGEN-CA preveri, ali je na zahtevku podani naslov e-pošte veljaven, in sicer na način, da SIGEN-CA pošlje obvestilo bodočemu imetniku ob sprejemu zahtevka. Če je to sporočilo zavrnjeno, prevzem potrdila ni mogoč.

3.3.2 Preverjanje imetnikov za ponovno pridobitev potrdila po preklicu

Preverjanje imetnikov poteka skladno z določili iz razd. 3.2.3.

3.4. Preverjanje istovetnosti ob zahtevi za preklic

(1) Zahtevek za preklic potrdila imetnik odda:
- osebno na prijavno službo, kjer pooblaščene osebe preverijo istovetnost prosilca,
- elektronsko, vendar mora biti zahtevek digitalno podpisan z zaupanja vrednim potrdilom, s tem pa izkazana tudi istovetnost prosilca.

(2) V primeru preklica preko telefona na dežurno telefonsko številko izdajatelja SIGEN-CA mora imetnik navesti v ta namen izbrano geslo.

(3) Podroben postopek za preklic je podan v razd. 4.9.3.

4. UPRAVLJANJE S POTRDILI

4.1. Pridobitev potrdila

4.1.1 Kdo lahko pridobi potrdilo

Bodoči imetniki potrdil so vedno fizične osebe, glej definicijo v podpogl. 1.6.

4.1.2 Postopek bodočega imetnika za pridobitev potrdila in odgovornosti

(1) Za pridobitev potrdila mora bodoči imetnik pravilno izpolniti in podpisati zahtevek za pridobitev potrdila. V primeru, da je bodoči imetnik oseba, ki nima procesne sposobnosti, mora s svojim podpisom na zahtevku dati soglasje z zahtevkom tudi njegov zakoniti zastopnik.

(2) Ob osebni oddaji zahtevka na prijavni službi morata biti prisotna bodoči imetnik in njegov zakoniti zastopnik.

(3) Bodoči imetnik lahko izdajatelju SIGEN-CA po elektronski poti posreduje zahtevek, digitalno podpisan z njegovim veljavnim kvalificiranim digitalnim potrdilom za fizične osebe, ki mu ga je izdal izdajatelj SIGEN-CA.

(4) Zahtevki za pridobitev so dostopni na prijavnih službah oz. pri drugih pooblaščenih osebah izdajatelja SIGEN-CA in na spletnih straneh SIGEN-CA.

(4) Bodoči imetnik je za pridobitev potrdila dolžan:
- izpolniti zahtevek za pridobitev potrdila z resničnimi in pravilnimi podatki,
- zahtevek oddati na prijavno službo osebno ali izdajatelju SIGEN-CA po elektronski poti posredovati zahtevek, digitalno podpisan z njegovim veljavnim digitalnim potrdilom za fizične osebe, ki mu ga je izdal izdajatelj SIGEN-CA,
- opraviti prevzem potrdila na varen način po navodilih izdajatelja SIGEN-CA.

4.2. Postopek ob sprejemu zahtevka za pridobitev potrdila

4.2.1 Preverjanje istovetnosti bodočega imetnika

(1) V primeru osebne oddaje zahtevka na prijavni službi pooblaščena oseba na prijavni službi preveri istovetnost bodočega imetnika v skladu z 31. členom in drugimi določili ZEPEP. Bodoči imetnik mora izkazati svojo istovetnost z veljavnim osebnim dokumentom.

(2) V primeru oddaje zahtevka na elektronski način pooblaščena oseba izdajatelja SIGEN-CA opravi overjanje elektronskega podpisa. Istovetnost bodočega imetnika se izkaže z veljavnostjo njegovega elektronskega podpisa.

(3) Preveriti je potrebno istovetnost bodočega imetnika oz. vse tiste podatke, ki so navedeni v zahtevku in so dostopni v uradnih evidencah oz. drugih uradnih veljavnih dokumentih.

4.2.2 Odobritev/zavrnitev zahtevka

(1) Zahtevek za pridobitev potrdila odobrijo oz. v primeru nepravilnih ali pomanjkljivih podatkov ali neizpolnjevanja obveznosti zavrnejo pooblaščene osebe izdajatelja SIGEN-CA.

(2) O odobritvi oz. zavrnitvi je bodoči imetnik nemudoma obveščen po e-pošti.

(3) V primeru odobritve izdajatelj SIGEN-CA pred izdajo potrdila obvesti bodočega imetnika z vso potrebno dokumentacijo v skladu s 36. členom ZEPEP.

4.2.3 Čas za izdajo potrdila

SIGEN-CA na podlagi odobrenega zahtevka opravi rezervacijo potrdila najkasneje v desetih (10) dneh od odobritve zahtevka.

4.3. Izdaja potrdila

4.3.1 Postopek izdajatelja SIGEN-CA

(1) V primeru odobrenega zahtevka SIGEN-CA posreduje bodočemu imetniku potrdila referenčno številko (angl. *reference number*) in avtorizacijsko kodo (angl. *authorization code*) po dveh ločenih poteh: referenčno številko po elektronski pošti, avtorizacijsko kodo pa s poštno pošiljko, izjemoma pa ju lahko pooblaščena oseba SIGEN-CA preda tudi osebno.

(2) Po prevzemu potrdila postaneta referenčna številka in avtorizacijska koda neuporabni.

(3) Potrdila se izdajajo izključno na infrastrukturi overitelja na MJU.

4.3.2 Obvestilo imetnika o izdaji

Glej prejšnji razdelek.

4.4. Prevzem potrdila

4.4.1 Postopek prevzema potrdila

(1) Za prevzem potrdila bodoči imetnik potrebuje referenčno številko in avtorizacijsko kodo, ki mu ju izda SIGEN-

CA, glej podpogl. 4.3.

(2) Način in podrobna navodila za prevzem potrdil po tej politiki so opisana na spletni strani http://www.sigen-ca.si. Prav tako so na spletni strani objavljene tudi vse novosti v zvezi z načinom prevzema potrdil.

(3) Imetnik mora takoj po prevzemu potrdila preveriti podatke v tem potrdilu. Če izdajatelja SIGEN-CA ne obvesti o morebitnih napakah, se smatra, da se z vsebino strinja in da soglaša s pogoji delovanja in prevzemom obveznosti in odgovornosti.

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

4.4.2 Objava potrdila

Glede objave potrdila glej pogl. 2.

4.5. Obveznosti in odgovornosti uporabnikov glede uporabe potrdil

4.5.1 Obveznosti imetnika potrdila

(1) Imetnik oziroma bodoči imetnik potrdila je dolžan:
- seznaniti se in ravnati v skladu s politiko pred izdajo potrdila,
- ravnati v skladu s politiko in ostalimi veljavnimi predpisi,
- po prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti SIGEN-CA oziroma zahtevati preklic potrdila,
- če po oddaji zahtevka za pridobitev potrdila oz. drugo storitev od izdajatelja SIGEN-CA ne prejme obvestila po e-pošti, ki jo je navedel v zahtevku, potem se mora obrniti na pooblaščene osebe izdajatelja SIGEN-CA,
- spremljati vsa obvestila SIGEN-CA in ravnati v skladu z njimi,
- v skladu z obvestili ustrezno posodabljati potrebno strojno in programsko opremo za varno delo s potrdili,
- nemudoma sporočiti SIGEN-CA vse spremembe, ki so povezane s potrdilom,
- zahtevati preklic potrdila, če je bil zasebni ključ ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe,
- uporabljati potrdilo za namen, določen v potrdilu (glej podpogl. 7.1), in na način, ki je določen s politiko SIGEN-CA,
- skrbeti za originalno podpisane dokumente in arhiv teh dokumentov.

(2) Imetnik oziroma bodoči imetnik potrdila je glede varovanja zasebnega ključa dolžan tudi:
- podatke za prevzem potrdila skrbno varovati pred nepooblaščenimi osebami,
- hraniti zasebni ključ in potrdilo na način in na sredstvih za varno hranjenje zasebnih ključev v skladu z obvestili in priporočili SIGEN-CA,
- zasebni ključ in vse druge zaupne podatke ščititi s primernim geslom v skladu s priporočili SIGEN-CA ali na drug način tako, da ima dostop do njih samo imetnik,
- skrbno varovati gesla za zaščito zasebnega ključa,
- po preteku veljavnosti oz. preklicu potrdila ravnati v skladu z obvestili SIGEN-CA.

4.5.2 Obveznosti za tretje osebe

(1) Tretja oseba, ki se zanaša na potrdilo, mora:
- ravnati in uporabljati potrdila v skladu in namenom s politiko in ostalimi veljavnimi predpisi,

- skrbno proučiti vse možnosti tveganja in odgovornosti pri uporabi potrdil in določiti politiko za način uporabe,
- obvestiti SIGEN-CA, če izve, da so bili zasebni ključi imetnika potrdila, na katerega se zanaša, ogroženi na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, navedeni v potrdilu,
- skrbeti za arhiv dokumentov,
- se zanašati na potrdilo samo za namen, določen v potrdilu (glej razd. 6.1.7), in na način, ki je določen s politiko,
- v času uporabe potrdila preveriti, če potrdilo ni v registru preklicanih potrdil,
- v času uporabe potrdila preveriti, če je bil digitalni podpis kreiran v času veljavnosti in z ustreznim namenom potrdila,
- v času uporabe potrdila preveriti podpis izdajatelja potrdila SIGEN-CA, ki je objavljen v tej politiki in tudi na spletnih straneh SIGEN-CA oz. drugih izdajateljev potrdil overitelja na MJU,
- upoštevati druge določbe, v kolikor je z overiteljem na MJU oz. izdajateljem SIGEN-CA sklenila dogovor o uporabi potrdil.

(2) Tretja oseba mora za overjanje podpisa oz. druge kriptografske operacije uporabljati programsko in strojno opremo, s katero lahko na verodostojen način preveri vse zgoraj navedene zahteve za varno uporabo potrdil.

4.6. Ponovna izdaja potrdila brez spremembe javnega ključa

Postopek ponovne izdaje potrdila brez spremembe javnega ključa izdajatelj SIGEN-CA ne podpira.

4.7. Regeneriranje ključev

4.7.1 Razlogi za regeneracijo

Ni podprto.

4.7.2 Kdo zahteva regeneracijo

Ni podprto.

4.7.3 Postopek za izdajo zahtevka za regeneracijo

Ni podprto.

4.8. Sprememba potrdila

(1) Če pride do spremembe podatkov, ki vplivajo na veljavnost razločevalnega imena oz. drugih podatkov v potrdilu, je potrebno potrdilo preklicati.

(2) Za pridobitev novega potrdila je potrebno ponoviti postopek za pridobitev novega potrdila, kot je naveden v podpogl. 4.1.

4.8.1 Okoliščina za spremembo potrdila

Ni podprta.

4.8.2 Kdo zahteva spremembo

Ni podprto.

4.8.3 Postopek ob zahtevku za spremembo

Ni podprt.

4.8.4 Obvestilo o izdaji novega potrdila

Ni podprto.

4.8.5 Prevzem spremenjenega potrdila

Ni podprt.

4.8.6 Objava spremenjenega potrdila

Ni podprta.

4.8.7 Obvestilo drugih subjektov o spremembi

Ni podprto.

4.9. Preklic in suspenz potrdila

4.9.1 Razlogi za preklic

(1) Preklic potrdila mora imetnik zahtevati v primeru:
- če je bil zasebni ključ imetnika potrdila ogrožen na način, ki vpliva na zanesljivost uporabe,
- če obstaja nevarnost zlorabe zasebnega ključa ali potrdila imetnika,
- če so se spremenili oz. so napačni ključni podatki, navedeni v potrdilu.

(2) Izdajatelj SIGEN-CA prekliče potrdilo tudi brez zahteve imetnika takoj, ko izve:
- da je podatek v potrdilu napačen ali je bilo potrdilo izdano na podlagi napačnih podatkov,
- da je prišlo do napake pri preverjanju istovetnosti podatkov na prijavni službi,
- da so se spremenile druge okoliščine, ki vplivajo na veljavnost potrdila,
- za neizpolnjevanje obveznosti imetnika,
- da niso poravnani morebitni stroški za upravljanje digitalnih potrdil,
- da je bila infrastruktura overitelja na MJU ogrožena na način, ki vpliva na zanesljivost potrdila,
- da je bil zasebni ključ imetnika potrdila ogrožen na način, ki vpliva na zanesljivost uporabe,
- da bo SIGEN-CA prenehal z izdajanjem potrdil ali da je bilo overitelju na MJU prepovedano upravljanje s

potrdili in njegove dejavnosti ni prevzel drug overitelj,
- da je preklic odredilo pristojno sodišče ali upravni organ.

4.9.2 Kdo zahteva preklic

Preklic potrdila lahko zahteva:
- pooblaščena oseba izdajatelja SIGEN-CA,
- imetnik,
- pristojno sodišče ali
- upravni organ.

4.9.3 Postopki za preklic

(1) Preklic lahko imetnik zahteva:
- osebno v času uradnih ur na prijavni službi,
- elektronsko štiriindvajset (24) ur na dan vse dni v letu, če gre za možnost zlorabe ali nezanesljivosti potrdila, sicer v času, ki po veljavni zakonodaji velja za poslovni čas državnih organov,
- telefonsko štiriindvajset (24) ur na dan vse dni v letu, če gre za možnost zlorabe ali nezanesljivosti potrdila, sicer v času, ki po veljavni zakonodaji velja za poslovni čas državnih organov.

(2) Če se preklic zahteva:
- osebno, je potrebno izpolniti ustrezen zahtevek za preklic potrdila ter ga oddati na prijavno službo;
- elektronsko, mora imetnik poslati na SIGEN-CA elektronsko sporočilo z zahtevkom za preklic, ki mora biti digitalno podpisan z zaupanja vrednim potrdilom za njegovo overjanje. Ob tem mora izdajatelj zahtevka za preklic hkrati o tem telefonsko obvestiti SIGEN-CA na dežurno telefonsko številko za preklice (glej razd. 1.3.1);
- telefonsko, mora imetnik poklicati na dežurno telefonsko številko za preklice (glej razd. 1.3.1), ob tem mora navesti geslo, ki ga je v ustreznem zahtevku za pridobitev potrdila imetnik podal kot geslo za preklic potrdila oz. ga je drugače varno posredoval SIGEN-CA. Brez gesla za preklic imetnik ne more telefonsko preklicati potrdila.

(4) O datumu ter času preklica, izdajatelju zahtevka za preklic ter vzrokih za preklic mora biti imetnik vedno obveščen.

(5) Sodišča in upravni organi, ki tudi lahko zahtevajo preklic, storijo to po veljavnih postopkih.

4.9.4 Čas za izdajo zahtevka za preklic

Zahtevek za preklic je potrebno zahtevati nemudoma, če gre za možnost zlorabe ali nezanesljivosti ipd. nujne primere, sicer pa prvi delovni dan v času, ki velja za poslovni čas državnih organov oz. uradnih ur na prijavnih službah (glej naslednji razdelek).

4.9.5 Čas od prejetega zahtevka za preklic do izvedbe preklica

(1) Overitelj na MJU po prejemu veljavne zahteve za preklic:
- najkasneje v štirih (4) urah prekliče potrdilo, če gre za preklic zaradi nevarnosti zlorabe ali nezanesljivosti ipd.,
- sicer pa prvi delovni dan po prejetju zahtevka za preklic.

(2) Po preklicu je tako potrdilo takoj dodano v register preklicanih potrdil in brisano iz javnega imenika potrdil[4].

4.9.6 Zahteve po preverjanju registra preklicanih potrdil za tretje osebe

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

4.9.7 Pogostnost objave registra preklicanih potrdil

Register preklicanih potrdil se osvežuje (za dostop do registra glej razd. 7.2.3):
- po vsakem preklicu potrdila,
- enkrat dnevno, če ni novih zapisov oz. sprememb v registru preklicanih potrdil, in sicer približno štiriindvajset (24) ur po zadnjem osveževanju.

4.9.8 Čas objave registra preklicanih potrdil

Objava novega registra preklicanih potrdil se izvede:
- v javnem imeniku na strežniku *x500.gov.si* takoj,
- na spletni strani pa z zakasnitvijo največ desetih (10) minut.

4.9.9 Sprotno preverjanje statusa potrdil

(1) Protokol za sprotno preverjanje statusa OCSP (angl. *Online Certificate Status* Protocol) ni podprt.

(2) Možno je sprotno preverjanje veljavnosti posameznega potrdila prek spletnega vmesnika. Potrdilo se poišče z iskalnikom na spletni strani, podrobno o tem glej podpogl. 7.3.

4.9.10 Zahteve za sprotno preverjanje statusa potrdil

Tretje osebe morajo ob uporabi potrdila vedno preveriti, ali je potrdilo, na katerega se zanašajo, preklicano.

4.9.11 Drugi načini za dostop do statusa potrdil

Niso podprti.

4.9.12 Posebne zahteve pri zlorabi zasebnega ključa

Niso določene.

4.9.13 Razlogi za suspenz

Ni podprto.

[4] V javnem imeniku ostanejo samo evidenčni podatki o potrdilu.

4.9.14 Kdo zahteva suspenz

Ni podprto.

4.9.15 Postopek za suspenz

Ni podprto.

4.9.16 Čas suspenza

Ni podprto.

4.10. Preverjanje statusa potrdil

4.10.1 Dostop za preverjanje

Register preklicanih potrdil je objavljen v javnem imeniku na strežniku *x500.gov.si*, podrobnosti o objavi in dostopu pa so v podpogl. 7.2 in 7.3.

4.10.2 Razpoložljivost

Preverjanje statusa potrdil je stalno na razpolago štiriindvajset (24) ur vse dni v letu.

4.10.3 Druge informacije za preverjanje statusa

Niso predpisane.

4.11. Prekinitev razmerja med imetnikom in overiteljem

Razmerje med imetnikom in overiteljem na MJU se prekine, če
- imetnikovo potrdilo preteče in ga le-ta ne podaljša,
- je potrdilo preklicano, imetnik pa ne zaprosi za novega.

4.12. Odkrivanje kopije ključev za dešifriranje

4.12.1 Razlogi za odkrivanje kopije ključev za dešifriranje

Ni podprto.

4.12.2 Kdo zahteva odkrivanje kopije ključev za dešifriranje

Ni podprto.

4.12.3 Postopek ob zahtevku za odkrivanje kopije ključev za dešifriranje

Ni podprto.

5. UPRAVLJANJE IN VARNOSTNI NADZOR INFRASTRUKTURE

5.1. Fizično varovanje

(1) Oprema overitelja na MJU je varovana z večnivojskim sistemom fizičnega in elektronskega varovanja.

(2) Varovanje infrastrukture overitelja na MJU se izvaja v skladu s priporočili stroke za najvišji nivo varovanja.

(3) Celoten opis infrastrukture overitelja na MJU in postopki upravljanja ter varovanje le-te so določeni z Interno politiko overitelja na MJU.

5.1.1 Lokacija in zgradba overitelja na MJU

(1) Oprema overitelja na MJU je postavljena v posebnih, varovanih, ločenih prostorih v okviru infrastrukture Direktorata za e-upravo in upravne procese Ministrstva za javno upravo.

(2) Zavarovana je z večnivojskim sistemom fizičnega in elektronskega varovanja.

(3) Podrobna določila so v Interni politiki overitelja na MJU.

5.1.2 Fizični dostop do infrastrukture overitelja na MJU

(1) Dostop do infrastrukture overitelja na MJU oz. izdajatelja je omogočen samo pooblaščenim osebam overitelja na MJU skladno z njihovimi nalogami in pooblastili, glej razd. 5.2.1.

(2) Vsi dostopi so varovani v skladu z zakonodajo in priporočili.

(3) Podrobna določila so v Interni politiki overitelja na MJU.

5.1.3 Napajanje in prezračevanje

(1) Infrastruktura overitelja ima zagotovljeno neprekinjeno napajanje in ustrezne klimatske sisteme.

(2) Podrobno o tem je določeno v Interni politiki overitelja na MJU.

5.1.4 Zaščita pred poplavo

(1) Infrastruktura overitelja na MJU ni izpostavljena nevarnosti poplav, razen v primeru višje sile.

(2) Podrobno o tem je določeno v Interni politiki overitelja na MJU.

5.1.5 Zaščita pred požari

(1) Prostori overitelja so varovani pred morebitnim izbruhom požara.

(2) Podrobno o tem je določeno v Interni politiki overitelja na MJU.

5.1.6 Hramba nosilcev podatkov

(1) Nosilci podatkov, bodisi v papirnati ali elektronski obliki, se hranijo varno v zaščitenih objektih.

(2) Varnostne kopije programske opreme in šifriranih baz overitelja na MJU se redno obnavljajo in shranjujejo v dveh ločenih in fizično varovanih prostorih, na različnih lokacijah.

5.1.7 Odstranjevanje odpadkov

(1) Overitelj na MJU zagotavlja varno odstranjevanje in uničevanje dokumentov v fizični in elektronski obliki.

(2) Odstranjevanje odpadkov izvaja posebna komisija v skladu z Interno politiko overitelja na MJU.

(3) Podrobno o tem je določeno v Interni politiki overitelja na MJU.

5.1.8 Hramba na oddaljeni lokaciji

Glej razd. 5.1.6.

5.2. Organizacijska struktura izdajatelja oz. overitelja

5.2.1 Skupine overitelja na MJU

(1) Operativno, organizacijsko in strokovno pravilno delovanje overitelja na MJU vodi vodja notranje organizacijske enote, ki je odgovorna za upravljanje digitalnih potrdil v okviru Direktorata za e-upravo in upravne procese Ministrstva za javno upravo.

(2) Med pooblaščene osebe overitelja na MJU spadajo:
- zaposleni pri overitelju na MJU in
- prijavne službe.

(3) Zaposleni pri overitelju na MJU so razporejeni v štiri organizacijske skupine, ki pokrivajo naslednja vsebinska področja:
- upravljanje z informacijskim sistemom,
- upravljanje s kvalificiranimi potrdili,
- varovanje in kontrola,
- pravno-administrativno.

Organizacijska skupina	Vloga	Osnovne naloge	Število oseb
Upravljanje z informacijskim	Upravljavec sistema	Strategija delovanja overitelja na MJU Določevanje prvega varnostnega	2

sistemom		inženirja Operativno vodenje overitelja na MJU	
Upravljanje s kvalificiranimi potrdili	Prvi varnostni inženir	Določevanje in izvajanje pravil varnega delovanja sistema za podeljevanje potrdil Določevanje drugih varnostnih inženirjev	1
	Drugi varnostni inženirji	Določevanje in izvajanje pravil varnega delovanja sistema za podeljevanje potrdil	2
	Administratorji potrdil	Upravljanje s potrdili	2
Varovanje in kontrola	Varnostni administrator	Upravljanje s telekomunikacijami (sistem za preprečevanje in odkrivanje vdorov, požarna pregrada, ...) Vzdrževanje varnostnih kopij	1
Pravno-administrativno	Pravnik		1

5.2.2 Število oseb za posamezne naloge

(1) Posamezne občutljive naloge mora skladno z Uredbo in Interno politiko delovanja overitelja na MJU opravljati več oseb hkrati.

(2) Na infrastrukturi je zagotovljeno, da varnostne ali kritične postopke odobrita dve pooblaščeni osebi istočasno.

(3) Navedeno število oseb v tabeli v razd. 5.2.1 predstavlja minimalno število oseb.

5.2.3 Izkazovanje istovetnosti za opravljanje posameznih nalog

Izkazovanje istovetnosti in pravice dostopov za opravljanje posameznih nalog skladno z vlogo posamezne organizacijske skupine kot tudi za opravljanje nalog prijavne službe je zagotovljena z varnostnimi mehanizmi in kontrolnimi postopki na programski opremi overitelja na MJU.

5.2.4 Nezdružljivost nalog

(1) Vse organizacijske skupine overitelja na MJU, navedene v tabeli razd. 5.2.1, so med seboj nezdružljive.

(2) Ob pomanjkanju ustrezno usposobljenega kadra se lahko zaradi podobne vrste opravil združi osebje določenih skupin z enakimi oz. podobnimi privilegiji delovanja.

(3) Vloge posameznih organizacijskih skupin so določene z Interno politiko overitelja na MJU.

5.3. Nadzor nad osebjem

V skladu z Uredbo so podrobnejša določila glede nadzora osebja določena v Interni politiki overitelja na MJU.

5.3.1 Potrebne kvalifikacije in izkušnje osebja

Osebje overitelja ima skladno z zahtevami ZEPEP in Uredbo ustrezne kvalifikacije in izkušnje.

5.3.2 Primernost osebja

Osebje overitelja ima skladno z zahtevami ZEPEP in Uredbo ustrezne kvalifikacije in izkušnje.

5.3.3 Dodatno izobraževanje osebja

Osebam, ki opravljajo naloge zgoraj navedenih organizacijskih skupin in naloge prijavne službe, se zagotavlja vsa potrebna izobraževanja.

5.3.4 Zahteve za redna usposabljanja

Osebje se usposablja glede na potrebe oz. novosti v zvezi z delovanjem infrastrukture izdajatelja SIGEN-CA.

5.3.5 Menjava nalog

Ni predpisana.

5.3.6 Sankcije

Sankcije v primeru nepooblaščenega ali malomarnega izvajanja nalog se za pooblaščene osebe overitelja na MJU izvajajo skladno z veljavno zakonodajo, ki velja za javne uslužbence in drugo veljavno zakonodajo.

5.3.7 Zahteve za zunanje izvajalce

Za morebitne zunanje izvajalce veljajo enake zahteve kot za pooblaščene osebe overitelja na MJU.

5.3.8 Dostop osebja do dokumentacije

Pooblaščenim osebam overitelja je na voljo vsa potrebna dokumentacija skladno z njihovimi zadolžitvami in nalogami.

5.4. Varnostni pregledi sistema

5.4.1 Vrste dnevnikov

(1) Izdajatelj SIGEN-CA skladno z Uredbo preverja vse, kar določa:
- varnost infrastrukture,
- nemoteno delovanje vseh varnostnih sistemov in
- ali je v vmesnem času prišlo do vdora ali poskusa vdora nepooblaščenih oseb do opreme ali podatkov.

(2) Podrobni podatki o tem so skladno z Uredbo določeni v Interni politiki overitelja na MJU.

5.4.2 Pogostost pregledov dnevnikov

Izdajatelj SIGEN-CA opravlja varnostne preglede svoje infrastrukture oz. dnevnikov dnevno.

5.4.3 Čas hrambe dnevnikov

Dnevniki se hranijo trajno.

5.4.4 Zaščita dnevnikov

(1) Dnevniki so varovani v skladu z varnostnimi mehanizmi, ki zagotavljajo najvišji nivo varnosti.

(2) Podrobnosti so v skladu z Uredbo določene v Interni politiki overitelja na MJU.

5.4.5 Varnostne kopije dnevnikov

(1) Varnostne kopije dnevnikov se izvajajo dnevno.

(2) Podrobnosti so v skladu z Uredbo določene v Interni politiki overitelja na MJU.

5.4.6 Zbiranje podatkov za dnevnike

(1) Podatki se zbirajo bodisi avtomatsko ali pa ročno, odvisno od vrste podatkov.

(2) Podrobnosti so v skladu z Uredbo določene v Interni politiki overitelja na MJU.

5.4.7 Obveščanje povzročitelja dogodka

Povzročitelja dogodkov ni potrebno obveščati.

5.4.8 Ocena ranljivosti sistema

(1) Analiza dnevnikov in nadzor nad izvajanjem vseh postopkov se izvaja redno s strani pooblaščenih oseb overitelja na MJU ali pa avtomatsko z drugimi varnostnimi mehanizmi na vseh računalniško-komunikacijskih napravah v pristojnosti overitelja na MJU.

(2) Ocena ranljivosti se izvaja na podlagi analize dnevnikov.

(3) Podrobnosti so v skladu z Uredbo določene v Interni politiki overitelja na MJU.

5.5. Arhiviranje podatkov

5.5.1 Vrste arhivskih podatkov

Izdajatelj SIGEN-CA skladno z Uredbo hrani naslednje podatke oz. dokumente:

- dnevnike,
- zapisnike,
- vsa dokazila o opravljenem preverjanju istovetnosti imetnikov,

- vse zahtevke,
- potrdila in register preklicanih potrdil,
- politike delovanja,
- objave in obvestila SIGEN-CA,
- zasebne ključe za dešifriranje v skladu z razd. 6.1.1 ter
- druge dokumente v skladu z veljavnimi predpisi.

5.5.2 Čas hrambe

Izdajatelj SIGEN-CA arhivske podatke hrani trajno.

5.5.3 Zaščita arhivskih podatkov

(1) Arhivski podatki so varno shranjeni.

(2) V skladu z Uredbo je podrobno to določeno v Interni politiki overitelja na MJU.

5.5.4 Varnostna kopija arhiva

(1) Kopija arhivskih podatkov se varno hrani.

(2) V skladu z Uredbo je to podrobno določeno v Interni politiki overitelja na MJU.

5.5.5 Zahteva po časovnem žigosanju

Ni predpisana.

5.5.6 Način zbiranja podatkov

(1) Podatki se zbirajo na način, skladen z vrsto dokumenta.

(2) V skladu z Uredbo je to podrobno določeno v Interni politiki overitelja na MJU.

5.5.7 Postopek za dostop do arhivskih podatkov in njihova verifikacija

(1) Dostop do arhivskih podatkov je možen samo pooblaščenim osebam.

(2) V skladu z Uredbo je to podrobno določeno v Interni politiki overitelja na MJU.

5.6. Sprememba javnega ključa izdajatelja SIGEN-CA

V primeru novega izdanega potrdila izdajatelja SIGEN-CA se postopek objavi na spletnih straneh SIGEN-CA.

5.7. Okrevalni načrt

5.7.1 Postopek v primeru vdorov in zlorabe

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

5.7.2 Postopek v primeru okvare programske opreme, podatkov

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

5.7.3 Postopek v primeru ogroženega zasebnega ključa izdajatelja SIGEN-CA

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

5.7.4 Okrevalni načrt

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

5.8. Prenehanje delovanja SIGEN-CA

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

6. TEHNIČNE VARNOSTNE ZAHTEVE

6.1. Generiranje in namestitev ključev

6.1.1 Generiranje ključev

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

(2) Ključi imetnikov se generirajo pri imetniku.

6.1.2 Dostava zasebnega ključa imetnikom

Zasebni ključ se generira pri imetniku in se ne prenaša.

6.1.3 Dostava javnega ključa izdajatelju potrdil

Imetniki v postopku prevzema dostavijo svoj javni ključ v podpis izdajatelju SIGEN-CA po protokolu PKCS#7.

6.1.4 Dostava izdajateljevega javnega ključa

Potrdilo z javnim ključem izdajatelja SIGEN-CA je imetniku dostavljeno oz. tretjim osebam dostopno:

- v javnem imeniku x500.gov.si po protokolu LDAP (glej podpogl. 2.3),

- preko spletne strani https://www.sigen-ca.si/cda-cgi/clientcgi?action=caCert,
- v obliki PEM na naslovu https://www.sigen-ca.si/sigen-ca.pem,
- v obliki PEM na naslovu http://www.sigen-ca.si/sigen-ca.pem, pri čemer mora dodatno preveriti verodostojnost potrdila,
- preko protokola PKCS#7.

6.1.5 Dolžina ključev

Potrdilo	Dolžina ključa po RSA [bit]
potrdilo izdajatelja SIGEN-CA	2048
potrdilo za imetnike	1024[5]

6.1.6 Generiranje in kakovost parametrov javnih ključev

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

6.1.7 Namen ključev in potrdil

(1) Namen uporabe ključev oz. potrdil je v skladu z *X.509 v.3* določen v potrdilu v polju *uporaba ključa* (angl. *keyUsage)* in *razširjena uporaba ključa* (angl. *extended keyUsage)*[6].

(2) Za podpis potrdil in registra preklicanih potrdil je namenjen zasebni ključ izdajatelja SIGEN-CA, za overjanje pa javni ključ v izdajateljevem potrdilu.

(3) Profil potrdil je podan v podpogl. 7.1.

6.2. Zaščita zasebnega ključa

6.2.1 Standardi za kriptografski modul

Zasebni ključ izdajatelja SIGEN-CA je zaščiten v programski opremi, ki je certificirana v skladu s FIPS 140-1 nivo 2 in Common Criteria EAL4+.

6.2.2 Nadzor zasebnega ključa s strani pooblaščenih oseb

Določila glede dostopa do zasebnega ključa izdajatelja SIGEN-CA so v skladu z Uredbo določena v Interni politiki overitelja na MJU.

6.2.3 Odkrivanje kopije zasebnega ključa

Ni predpisano.

[5] Vrednost pomeni minimalno predpisano dolžino.
[6] Za potrdila SIGEN-CA se to polje ne uporablja.

6.2.4 Varnostna kopija zasebnega ključa

Ni predpisano.

6.2.5 Arhiviranje zasebnega ključa

Ni predpisano.

6.2.6 Prenos zasebnega ključa iz/v kriptografski modul

Zasebni ključ imetnika se generira pri imetniku s programsko ali strojno opremo, ki je v pristojnosti imetnika.

6.2.7 Postopek za aktiviranje zasebnega ključa

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

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

6.2.8 Postopek za deaktiviranje zasebnega ključa

(1) Ob zaustavitvi delovanja izdajatelja SIGEN-CA programska oprema SIGEN-CA deaktivira zasebni ključ SIGEN-CA.

(2) SIGEN-CA imetnikom priporoča uporabo programskega okolja, ki ob odjavi ali po določenem pretečenem času onemogoči dostop do njihovega zasebnega ključa brez vnosa ustreznega gesla.

6.2.9 Postopek za uničenje zasebnega ključa

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

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

6.2.10 Lastnosti kriptografskega modula

Strojni varnostni modulu ustrezajo standardom, podanim v razd. 6.2.1.

6.3. Ostali aspekti upravljanja ključev

6.3.1 Arhiviranje javnega ključa

Izdajatelj SIGEN-CA arhivira svoj javni ključ in javne ključe imetnikov, kot je podano v podpogl. 5.5.

6.3.2 Obdobje veljavnosti za javne in zasebne ključe

Veljavnost potrdil in ključev je podana po spodnji tabeli.

Tip potrdila	Par ključev	Ključi	Veljavnost
spletno potrdilo	par za digitalno podpisovanje/overjanje in dešifriranje/šifriranje	zasebni ključ	5 let
		javni ključ	5 let

6.4. Gesla za dostop do potrdil oz. ključev

6.4.1 Generiranje gesel

(1) Aktivacijska podatka za prevzem potrdila, t.j. referenčna številka in avtorizacijska koda, ki ju imetniki potrebujejo za prevzem potrdil, se ustvarita na strani SIGEN-CA. Podatka sta unikatna.

(2) Imetniki sami določijo geslo, s katerim zaščitijo dostop do svojih zasebnih ključev.

(3) SIGEN-CA priporoča uporabo varnih gesel:
- mešano uporaba velikih in malih črk, števil in posebnih znakov,
- dolžine vsaj 8 znakov,
- odsvetuje se uporabo besed, ki so zapisane v slovarjih.

6.4.2 Zaščita gesel

(1) Aktivacijska podatka za prevzem potrdila se kreirata varno pri izdajatelju SIGEN-CA.

(2) SIGEN-CA posreduje bodočemu imetniku potrdila referenčno številko in avtorizacijsko kodo po dveh ločenih poteh:
- referenčno številko po elektronski pošti,
- avtorizacijsko kodo s poštno pošiljko,
- izjemoma pa ju preda tudi osebno.

(3) Do prevzema potrdila mora bodoči imetnik skrbno varovati aktivacijska podatka za prevzem potrdila, po prevzemu potrdila postaneta neuporabna in ju imetnik lahko zavrže.

(4) SIGEN-CA priporoča, da se geslo za dostop do zasebnega ključa ne shranjuje oz. se shrani na varno mesto in da ima do njega dostop le imetnik.

(5) Izdajatelj SIGEN-CA imetnikom priporoča zamenjavo gesla vsaj vsakih šest (6) mesecev.

6.4.3 Drugi aspekti gesel

Niso predpisani.

6.5. Varnostne zahteve za računalniško opremo izdajatelja

6.5.1 Specifične tehnične varnostne zahteve

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

6.5.2 Nivo varnostne zaščite

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

6.6. Tehnični nadzor življenjskega cikla izdajatelja

6.6.1 Nadzor razvoja sistema

SIGEN-CA uporablja programsko opremo proizvajalca Entrust, ki je certificirana v skladu s FIPS 140-1 nivo 2 in Common Criteria EAL4+.

6.6.2 Upravljanje varnosti

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

6.6.3 Nadzor življenjskega cikla

Podrobne tehnične zahteve so določene v Interni politiki overitelja na MJU.

6.7. Varnostna kontrola računalniške mreže

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

6.8. Časovno žigosanje

Ni predpisano.

7. PROFIL POTRDIL IN REGISTRA PREKLICANIH POTRDIL

7.1. Profil potrdil

(1) Na podlagi pričujoče politike SIGEN-CA izdaja spletna potrdila za fizične osebe.

(2) Vsa potrdila vključujejo podatke, ki so skladno z ZEPEP določena za kvalificirana potrdila.

(3) Potrdila izdajatelja SIGEN-CA sledijo standardu *X.509.*

7.1.1 Različica potrdil

Vsa potrdila izdajatelja SIGEN-CA sledijo standardu *X.509*, in sicer različici 3.

7.1.2 Profil potrdil z razširitvami

(1) Podatki v potrdilu so navedeni spodaj.

Nazivi polja	Vrednost oz. pomen
Osnovna polja v potrdilu	
Različica, angl. *Version*	2 (*kar pomeni verzijo 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, ki vključuje ime imetnika in serijsko številko (glej razd. 3.1.1), v obliki, primerni za izpis*
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 1024 bitov, glej razd. 6.1.5*
Razširitve X.509v3	
Alternativno ime OID 2.5.29.17, angl. *Subject Alternative Name*	*elektronski naslov imetnika, glej razd. 7.1.2.1*
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, glej razd. 7.2.3*> 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*	*glej razd. 6.3.2*
Uporaba ključa, OID 2.5.29.15, *angl. Key Usage*	Digital Signature, Key Encipherment
Razširjena uporaba, OID 2.5.29.37, angl. *Extended Key Usage*	*se ne uporablja*
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*

Politika, pod katero je bilo izdano potrdilo, OID 2.5.29.32, angl. *certificatePolicies*	Certificate Policy: PolicyIdentifier=1.3.6.1.4.1.6105.2.2.3.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.ca.gov.si/cps/
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*	V7.0
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*

(2) Polje *namen uporabe* (angl. *Key Usage*) je označeno kot kritično (angl. *critical*).

(3) Imetnik ima lahko eno samo veljavno istovrstno potrdilo, razen v času šestdeset (60) dni pred potekom veljavnosti tega potrdila, ko lahko imetnik pridobi novo potrdilo.

7.1.2.1 Zahteve za elektronski naslov

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

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

7.1.3 Identifikacijske oznake algoritmov

(1) Potrdila, ki jih izdaja SIGEN-CA, so s strani izdajatelja podpisana z algoritmom, določenim v polju s*ignature algorithm*: vrednost »sha1WithRSAEncryption, identifikacijska oznaka: OID 1.2.840.113549.1.1.5«.

(2) Celoten nabor algoritmov, formatov podatkov in protokolov je na razpolago pri pooblaščenih osebah izdajatelja SIGEN-CA.

7.1.4 Oblika razločevalnih imen

Glej razd. 3.1.1.

7.1.5 Omejitve glede imen

Omejitve glede imen (polje v potrdilu angl. *nameConstraints*) niso predpisane.

7.1.6 Označba politike potrdila

Glej razd. 7.1.2.

7.1.7 Omejitve uporabe

Omejitve uporabe (polje v potrdilu angl. *usage policy constraints extension*) niso predpisane.

7.2. Profil registra preklicanih potrdil

7.2.1 Različica

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

(2) Register preklicanih potrdil je stalno dostopen v javnem imeniku potrdil (glej podpogl. 2.3):
- po protokolu LDAP in
- po protokolu HTTP.

7.2.2 Vsebina registra in razširitve

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

Naziv polja	Vrednost oz. pomen
Osnovna polja v CRL	
Različica, angl. *Version*	1 (*kar pomeni verzijo 2*)
Algoritem za podpis, angl. *Signature Algorithm*	sha1WithRSAEncryption
Izdajateljev podpis, angl. *Signature*	p*odpis SIGEN-CA*
Razločevalno ime izdajatelja, angl. *Issuer*	c=si, o=state-institutions, ou=sigen-ca
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*>
Razširitve X.509v2 CRL	
identifikator izdajateljevega ključa, angl. *Authority Key Identifier* *(OID 2.5.29.35)*	717B 8A06 1F31 0555 AB60 1277 4720 1E03 8818 EC89

številka za posamične registre (CRL1, CRL2,....), angl. *CRLnumber* *(OID 2.5.29.20)*	*zaporedna številka posamičnega registra*
angl. *issuerAltName* *(OID 2.5.28.18)*	*se ne uporablja*
angl. *deltaCRLindicator* *(OID 2.5.29.27)*	*se ne uporablja*
angl. *issuingDistribuitionPoint* *(OID 2.5.29.28)*	*se ne uporablja*

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

7.2.3 Objava registra preklicanih potrdil

(1) SIGEN-CA objavlja register v javnem imeniku na strežniku *X500.gov.si*, dostopen pa je po protokolih LDAP in http.

(2) Objavljeni so tako posamični registri kot tudi celotni register (na enem mestu). Dostop in objavo prikazuje spodnja tabela[7].

Objava CRL		Dostop do CRL
posamični registri	c=si, o=state-institutions, ou=sigen-ca, cn=CRL<*zaporedna številka registra*>	1. 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")*	ldap://x500.gov.si/ou=sigen-ca,o=state-institutions, c=si?certificateRevocationList?base http://www.sigen-ca.si/crl/sigen-ca.crl

7.3. Profil sprotnega preverjanja statusa potrdil

(1) Protokol za sprotno preverjanje statusa OCSP (angl. *Online Certificate Status Protocol*) ni podprt.

(2) Možno je sprotno preverjanje veljavnosti posameznega potrdila prek spletnega vmesnika. Potrdilo se poišče z iskalnikom na spletni strani:

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

in potem se izbere "verification of Certificate".

7.3.1 Verzija sprotnega preverjanje statusa

Protokol OCSP ni podprt.

7.3.2 Profil sprotnega preverjanje statusa

Protokol OCSP ni podprt.

[7] Potrdila, izdana po starejši politiki, t.j. OID=1.3.6.1.4.1.6105.2.2.1, nimajo navedbe dostopa po protokolu HTTP in zato avtomatski dostop za ta potrdila ni mogoč.

8. INŠPEKCIJSKI NADZOR

8.1. Pogostnost inšpekcijskega nadzora

Pogostnost inšpekcijskega nadzora je v pristojnosti inšpekcijske službe, ki je pristojna v skladu z ZEPEP.

8.2. Inšpekcijska služba

Izvajanje določb ZEPEP overitelja na MJU skladno z ZEPEP opravlja pristojna inšpekcijska služba v skladu z veljavno zakonodajo za inšpekcijski nadzor.

8.3. Neodvisnost inšpekcijske služba

Inšpekcijska služba je organ, pristojen v skladu z ZEPEP.

8.4. Področja inšpekcijskega nadzora

Področja nadzora so določena z veljavno zakonodajo in predpisi.

8.5. Ukrepi overitelja

V primeru ugotovljenih pomanjkljivosti ali napak si izdajatelj SIGEN-CA oz. overitelj prizadeva za odpravo le-teh v najkrajšem možnem času.

8.6. Objava rezultatov inšpekcijskega nadzora

Overitelj na MJU javno objavi povzetek sklepov inšpekcijskega nadzora na svojih spletnih straneh.

9. FINANČNE IN OSTALE PRAVNE ZADEVE

9.1. Cenik

9.1.1 Cena izdaje potrdil in podaljšanja

Stroški upravljanja s potrdili se obračunavajo po objavljenem ceniku na spletni strani http://www.sigen-ca.si/cenik.htm.

9.1.2 Cena dostopa do potrdil

Dostop do javnega imenika potrdil je brezplačen, razen če se stranki dogovorita drugače.

9.1.3 Cena dostopa do statusa potrdila in registra preklicanih potrdil

Dostop do statusa potrdila in registra preklicanih potrdil je brezplačen, razen če se stranki dogovorita drugače.

9.1.4 Cene drugih storitev

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

9.1.5 Povrnitev stroškov

Ni predpisana.

9.2. Finančna odgovornost

9.2.1 Zavarovalniško kritje

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

9.2.2 Drugo kritje

Ni predpisano.

9.2.3 Zavarovanje imetnikov

Ni predpisano.

9.3. Varovanje poslovnih podatkov

9.3.1 Varovani podatki

(1) Izdajatelj SIGEN-CA ravna zaupno z naslednjimi podatki:
- z vsemi zahtevki za pridobitev potrdila ali druge storitve
- vse morebitne zaupne podatke v zvezi s finančnimi obveznostmi,
- vse morebitne zaupne podatke, ki so predmet medsebojne pogodbe s tretjimi osebami ter
- vse ostale zadeve, ki so v skladu z Uredbo zavedene v Interni politiki delovanja overitelja na MJU.

(2) Z vsemi morebitnimi zaupnimi podatki o imetnikih in tretjih osebah, ki so nujno potrebni za storitve upravljanja s potrdili, izdajatelj SIGEN-CA ravna v skladu z veljavno zakonodajo.

9.3.2 Nevarovani podatki

Izdajatelj SIGEN-CA javno objavlja samo take poslovne podatke, ki v skladu z veljavno zakonodajo niso zaupne

narave.

9.3.3 Odgovornost glede varovanja

Izdajatelj SIGEN-CA ne posreduje drugih podatkov, razen teh, ki niso navedeni v potrdilu ali morebitnem medsebojnem dogovoru, razen če se določeni podatki posebej zahtevajo za izvajanje specifičnih storitev oz. aplikacij, povezanih s potrdili. Podatki se posredujejo tudi brez pisne privolitve, če to določa zakonodaja oz. veljavni predpisi.

9.4. Varovanje osebnih podatkov

9.4.1 Načrt varovanja osebnih podatkov

Z vsemi osebnimi in zaupnimi podatki o imetnikih potrdil, ki so nujno potrebni za storitve upravljanja s potrdili, izdajatelj SIGEN-CA ravna v skladu z veljavno zakonodajo.

9.4.2 Varovani osebni podatki

Varovani podatki so vsi osebni podatki, ki jih izdajatelj SIGEN-CA pridobi na zahtevkih za svoje storitve ali v ustreznih registrih za dokazovanje istovetnosti imetnika.

9.4.3 Nevarovani osebni podatki

Drugih morebitnih nevarovanih osebnih podatkov, razen teh, ki so navedeni v potrdilu in registru preklicanih potrdil, ni.

9.4.4 Odgovornost glede varovanja osebnih podatkov

Overitelj na MJU je odgovoren v skladu z Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 86/2004) in drugo veljavno zakonodajo glede varovanja osebnih podatkov.

9.4.5 Pooblastilo glede uporabe osebnih podatkov

Imetnik pooblasti overitelja na MJU oz. izdajatelja SIGEN-CA za uporabo osebnih podatkov na zahtevku za pridobitev potrdila ali kasneje v pisni obliki.

9.4.6 Posredovanje osebnih podatkov

(1) Overitelj na MJU ne posreduje drugih podatkov o imetnikih potrdil, ki niso navedeni v potrdilu, razen če se določeni podatki posebej zahtevajo za izvajanje specifičnih storitev oz. aplikacij, povezanih s potrdili, ter je overitelja na MJU imetnik pooblastil za to (glej prejšnji razdelek), ali na zahtevo pristojnega sodišča ali upravnega organa.

(2) Podatki se posredujejo tudi brez pisne privolitve, če to določa zakonodaja oz. veljavni predpisi.

9.4.7 Druga določila glede varovanja osebnih podatkov

Niso predpisana.

9.5. Določbe glede pravic intelektualne lastnine

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

9.6. Obveznosti in odgovornosti

9.6.1 Obveznosti in odgovornosti overitelja na MJU

(1) Overitelj na MJU oz. izdajatelj SIGEN-CA je dolžan:
- delovati v skladu s svojimi notranjimi pravili in ostalimi veljavnimi predpisi in zakonodajo,
- delovati v skladu z mednarodnimi priporočili,
- objavljati vse pomembne dokumente, ki določajo njegovo delovanje (politike delovanja, zahtevke, cenik, navodila za varno uporabo kvalificiranih digitalnih potrdil ipd.),
- objavljati na svojih spletnih straneh vse informacije o tistih spremembah glede dejavnosti overitelja, ki kakorkoli vplivajo na imetnike potrdil in tretje osebe,
- zagotoviti delovanje prijavnih služb v skladu z določili SIGEN-CA in ostalimi veljavnimi predpisi,
- spoštovati določila glede varnega ravnanja z osebnimi, poslovnimi in zaupnimi podatki o overitelju, imetnikih potrdil ali tretjimi osebami,
- preklicati potrdilo in objaviti preklicano potrdilo v registru preklicanih potrdil, ko ugotovi, da so podani razlogi po tej politiki ali drugih veljavnih predpisih,
- izdajati kvalificirana digitalna potrdila v skladu s to politiko in ostalimi predpisi ter priporočili.

(2) Overitelj na MJU oz. izdajatelj SIGEN-CA je dolžan:
- zagotoviti pravilnost podatkov izdanih potrdil,
- zagotoviti, da ima imetnik potrdila v času izdaje le-tega zasebni ključ pripadajoč v potrdilu navedenemu javnemu ključu,
- zagotoviti pravilnost objave registra preklicanih potrdil,
- zagotoviti enoličnost razločevalnih imen,
- zagotoviti primerno fizično varnost prostorov in dostopov do samih prostorov izdajatelja,
- kot dober gospodar skrbeti za nemoteno delovanje in čim večjo razpoložljivost storitve,
- kot dober gospodar skrbeti za čim večjo dostopnost storitev,
- kot dober gospodar skrbeti za nemoteno delovanje vseh ostalih spremljajočih storitev,
- poskušati odpraviti nastale probleme po najboljših močeh in v najkrajšem času,
- skrbeti za optimizacijo strojne in programske opreme in
- obveščati uporabnike o pomembnih zadevah ter
- izpolnjevati vse druge zahteve v skladu s to politiko.

(3) Overitelj na MJU oz. izdajatelj SIGEN-CA zagotavlja čim večjo dostopnost svojih storitev, in sicer 24ur/7dni/365dni, pri čemer pa se ne upošteva naslednje primere:
- načrtovane in vnaprej napovedane tehnične ali servisne posege na infrastrukturi,
- nenačrtovane tehnične ali servisne posege na infrastrukturi kot posledica nepredvidenih okvar,
- tehnične ali servisne posege zaradi okvare infrastrukture izven pristojnosti izdajatelja SIGEN-CA in

- nedostopnost kot posledica višje sile ali izrednih dogodkov.

(4) Vzdrževalna dela ali nadgradnje infrastrukture mora overitelj na MJU oz. SIGEN-CA najaviti vsaj tri (3) dni pred pričetkom del.

(5) Overitelj na MJU je odgovoren za vse navedbe v tem dokumentu in za izvajanje vseh določil iz te politike.

(6) Ostale obveznosti oz. odgovornosti izdajatelja SIGEN-CA oz. overitelja na MJU so določene z morebitnim medsebojnim dogovorom s tretjo osebo.

9.6.2 Obveznost in odgovornost prijavne službe

(1) Prijavna služba je dolžna:
- preverjati istovetnost imetnikov oz. bodočih imetnikov,
- sprejemati zahtevke za storitve SIGEN-CA,
- preverjati zahtevke,
- izdajati potrebno dokumentacijo imetnikom oz. bodočim imetnikom,
- posredovati zahtevke in ostale podatke na varen način na SIGEN-CA.

(2) Prijavna služba je odgovorna za izvajanje vseh določil iz teh politik in drugih zahtev, ki jih dogovorita z overiteljem na MJU.

9.6.3 Obveznosti in odgovornost imetnika potrdila

(1) Imetnik odgovarja za:
- nastalo škodo v primeru zlorabe potrdila od prijave preklica do preklica,
- vsako škodo, ki je bodisi posredno ali neposredno povzročena zato, ker je bila omogočena uporaba oz. zloraba imetnikovega potrdila s strani nepooblaščenih oseb,
- vsako drugo škodo, ki izvira iz neupoštevanja določil te politike in drugih obvestil SIGEN-CA ter veljavnih predpisov.

(2) Obveznosti imetnikov so glede uporabe potrdil določena v razd. 4.5.1.

9.6.4 Obveznosti in odgovornost tretjih oseb

(1) Tretje osebe morajo proučiti vse zahteve in okoliščine, preden se odločijo za zanašanja na potrdila, ki jih izda SIGEN-CA.

(2) Tretje osebe, ki se zanašajo na izdana potrdila SIGEN-CA, morajo:
- upoštevati tudi vsa navodila oz. priporočila SIGEN-CA glede zanesljive uporabe, določene tudi v razd. uporabe oz. zanašanja na potrdila glede uporabe potrdil so določena v razd. 4.5.2,
- ob morebitnih napakah ali problemih takoj obvestiti izdajatelja SIGEN-CA,
- seznaniti se s to politiko in upoštevati vsa določila glede njihove obveznosti, odgovornosti ter omejitve glede zaupanja in uporabe potrdil,
- spremljati vsa obvestila in objave SIGEN-CA in ravnati v skladu z le-temi,
- upoštevati morebitna druga pravila, ki so izven pristojnosti izdajatelja in so določena drugje.

(3) Tretje osebe nosijo vse posledice, ki bi nastale zaradi morebitnega neupoštevanja določil te politike, morebitnega dogovora z overiteljem in veljavne zakonodaje.

9.6.5 Obveznosti in odgovornost drugih oseb

Niso predpisani.

9.7. Omejitev odgovornosti

Overitelj na MJU ni odgovoren za škodo, ki bi nastala zaradi:

- uporabe potrdil za namen in na način, ki ni izrecno predviden v tej politiki,
- nepravilnega ali pomanjkljivega varovanja gesel ali zasebnih ključev imetnikov, izdajanja zaupnih podatkov ali ključev tretjim osebam in neodgovornega ravnanja imetnika,
- zlorabe oz. vdora v informacijski sistem imetnika potrdila in s tem do podatkov o potrdilih s strani nepooblaščenih oseb,
- nedelovanja ali slabega delovanja informacijske infrastrukture imetnika potrdila ali tretjih oseb,
- nepreverjanja podatkov in veljavnosti potrdil v registru preklicanih potrdil,
- nepreverjanja časa veljavnosti potrdila,
- ravnanja imetnika potrdila ali tretje osebe v nasprotju z obvestili SIGEN-CA, politiko in drugimi predpisi,
- omogočene uporabe oz. zlorabe imetnikovega potrdila nepooblaščenim osebam,
- izdanega potrdila z napačnimi podatki in neverodostojnimi podatki ali drugih dejanj imetnika ali overitelja,
- uporabe potrdil ter veljavnosti potrdil ob spremembah podatkov iz potrdila, elektronskih naslovov ali spremembah imen imetnikov,
- izpada infrastrukture, ki ni v domeni upravljanja overitelja na MJU,
- podatkov, ki se šifrirajo ali podpisujejo z uporabo potrdil,
- ravnanja imetnikov pri uporabi potrdil, in sicer tudi v primeru, če je imetnik ali tretja oseba spoštoval vsa določila te politike, obvestila SIGEN-CA ali druge veljavne predpise,
- uporabe in zanesljivosti delovanja strojne in programske opreme imetnikov potrdil.

9.8. Omejitev glede uporabe

Izdajatelj SIGEN-CA oz. overitelj na MJU jamči za vrednost posameznega pravnega posla glede na vrsto potrdila do vrednosti do višine 200.000,00 SIT.

9.9. Poravnava škode

Za škodo odgovarja stranka, ki je le-to povzročila zaradi neupoštevanja določil iz te politike in veljavne zakonodaje.

9.10. Veljavnost politike

9.10.1 Čas veljavnosti

(1) Nova verzija oz. spremembe politike overitelja na MJU se sedem (7) dni pred veljavo predhodno objavi na spletnih straneh overitelja na MJU pod novo identifikacijsko številko (CP_{OID}) in označenim datumom začetka njene veljavnosti.

(2) Konec veljavnosti politike ni določen in povezan z veljavnostjo potrdil, izdanih na podlagi politike.

9.10.2 Konec veljavnosti politike

(1) Ob objavi nove politike ostanejo za vsa potrdila, izdana na podlagi te politike, v veljavi tista določila, ki se smiselno ne morejo nadomestiti z ustreznimi določili po novi politiki (na primer postopek, ki določa način, po katerem je bilo to potrdilo izdano ipd.).

(2) Izdajatelj lahko za posamezna določila veljavne politike izda amandmaje, kot je to podano v podpogl. 9.12.

9.10.3 Učinek poteka veljavnosti politike

(1) Ob izdaji nove politike se vsa kvalificirana digitalna potrdila izdana po tem datumu obravnavajo po novi politiki.

(2) Nova politika ne vpliva na veljavnost potrdil, ki so bila izdana po prejšnjih politikah. Taka potrdila ostanejo v veljavi do konca preteka veljavnosti, pri čemer se, kjer je to možno, obravnavajo po novi politiki.

9.11. Komuniciranje med subjekti

(1) Kontaktni podatki overitelja oz. izdajatelja so objavljeni na spletnih straneh in podani v razd. 1.3.1.

(2) Kontaktni podatki imetnikov so podani v zahtevkih v zvezi s potrdili.

(3) Kontaktni podatki tretjih oseb so podani v morebitnem medsebojnem dogovoru med tretjo osebo in izdajateljem na MJU.

9.12. Amandmaji

9.12.1 Postopek za sprejem amandmajev

(1) Spremembe ali dopolnitve k pričujoči politiki lahko izdajatelj objavi v obliki amandmajev k tej politiki, kadar ne gre za bistvene spremembe v delovanju overitelja.

(2) Amandmaji se sprejmejo po enakem postopku kot politika.

(3) Če amandma bistveno vpliva na delovanje overitelja, se o tem obvesti pristojno ministrstvo po enakem postopku, kot to velja za politiko.

(4) Način za označevanje amandmajev določi izdajatelj SIGEN-CA.

9.12.2 Veljavnost in objava amandmajev

(1) Izdajatelja SIGEN-CA določi pričetek in konec veljavnosti amandmajev.

(2) Amandma se sedem (7) dni pred pričetkom veljavnosti objavi na spletnih straneh SIGEN-CA.

9.12.3 Sprememba identifikacijske številke politike

Če sprejeti amandma vpliva na uporabo potrdil, potem lahko izdajatelj SIGEN-CA določi novo identifikacijsko oznako politike (CP_{OID}) oz. amandmajev.

9.13. Postopek v primeru sporov

Stranke si bodo prizadevale za sporazumno reševanje sporov, če pa to ne bi bilo mogoče, je za reševanje sporov pristojno sodišče v Ljubljani. Stranke za reševanje sporov dogovorijo izključno uporabo predpisov Republike Slovenije.

9.14. Veljavna zakonodaja

(1) Overitelj na MJU in izdajatelj SIGEN-CA delujeta v skladu z:
- ZEPEP,
- Uredbo,
- evropskimi direktivami,
- Zakonom o varstvu osebnih podatkov,
- priporočili ETSI in RFC
- in drugimi veljavnimi predpisi.

(2) Oblika in vsebina te politike je usklajena z:
- RFC 3647 »Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework«,
- ETSI TS 101 456 v 1.3.1. »Policy requirements for certification authorities issuing qualified certificates«.

9.15. Skladnost z veljavno zakonodajo

(1) Nadzor nad skladnostjo delovanja overitelja na MJU oz. izdajatelja SIGEN-CA z veljavno zakonodajo in predpisi, določenimi v podpogl. 9.14, izvaja pristojna inšpekcijska služba.

(2) Notranje preverjanje skladnosti delovanja izvajajo pooblaščene osebe v okviru overitelja na MJU.

9.16. Splošne določbe

Z ostalimi subjekti izdajatelj SIGEN-CA lahko sklene medsebojne dogovore, če to določa veljavna zakonodaja oz. drugi predpisi.

9.17. Ostale določbe

(1) Izdajatelj SIGEN-CA deluje skladno s priporočili ETSI in RFC.

(2) Oblika in vsebina te politike je usklajena z
- RFC 3647 »Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework«,
- ETSI TS 101 456 v 1.4.2. »Policy requirements for certification authorities issuing qualified certificates«.