VLADA REPUBLIKE SLOVENIJE
CENTER ZA INFORMATIKO

POLITIKA SIGEN-CA

za spletna kvalificirana digitalna potrdila za fizične osebe

Javni del notranjih pravil overitelja na Centru Vlade RS za informatiko

Politika je veljavna od 9. julija 2001

CP_{Name}: SIGEN-CA-2
CP_{OID}: 1.3.6.1.4.1.6105.2.2.1

VSEBINA

1. UVOD

(1) Politike overitelja kvalificiranih digitalnih potrdil na Centru Vlade za informatiko (CVI) predstavljajo celoten javni del notranjih pravil overitelja na CVI glede posameznih vrst kvalificiranih digitalnih potrdil in določajo namen, delovanje in metodologijo upravljanja s kvalificiranimi digitalnimi potrdili, odgovornost overitelja na CVI ter varnostne zahteve, ki jih morajo izpolnjevati imetniki, tretje osebe, ki se zanašajo na kvalificirana digitalna potrdila, in drugi overitelji, ki želijo uporabljati storitve overitelja na CVI.

(2) Overitelj na CVI izdaja kvalificirana digitalna potrdila, za katera velja najvišja stopnja varovanja in načela t.i. močne enkripcije ter deluje v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 57/2000) in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000 in 2/2001) ter drugimi veljavnimi predpisi.

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

(4) Glede na to, komu so kvalificirana digitalna potrdila namenjena, ločimo med dvema izdajateljema kvalificiranih digitalnih potrdil overitelja na CVI:
- SIGOV-CA (angl.: Slovenian Governmental Certification Authority) je izdajatelj kvalificiranih digitalnih potrdil overitelja na CVI za institucije javne uprave,
- SIGEN-CA (angl.: Slovenian General Certification Authority) je izdajatelj kvalificiranih digitalnih potrdil overitelja na CVI za pravne in fizične oseb, ki so registrirane za opravljanje dejavnosti ter ostale fizične osebe.

(5) SIGOV-CA izdaja:
- osebna kvalificirana digitalna potrdila za zaposlene v institucijah javne uprave,
- spletna kvalificirana digitalna potrdila za zaposlene v institucijah javne uprave,
- spletna kvalificirana digitalna potrdila za strežnike, s katerimi upravljajo institucije javne uprave.

SIGEN-CA izdaja:
- osebna kvalificirana digitalna potrdila za zaposlene pravnih in fizičnih oseb, registriranih za opravljanje dejavnosti in druge osebe,
- spletna kvalificirana digitalna potrdila za zaposlene pravnih in fizičnih oseb, registriranih za opravljanje dejavnosti,
- spletna kvalificirana digitalna potrdila za fizične osebe.

(6) Osebna kvalificirana digitalna potrdila so namenjena za:
- šifriranje in dešifriranje podatkov v elektronski obliki,
- digitalno podpisovanje podatkov v elektronski obliki ter izkazovanje identitete podpisnika,
- varno brisanje podatkov v elektronski obliki,
- storitve oz. aplikacije, za katere se zahteva uporaba osebnih kvalificiranih digitalnih potrdil overitelja na CVI.

(7) Spletna kvalificirana digitalna potrdila se lahko uporabljajo za:
- varno spletno komuniciranje po protokolih SSL (angl.: Secure Sockets Layer) in TLS (angl.: Transport Layer Security),

- varno pošiljanje elektronske pošte po protokolu S/MIME (angl.: Secure Multipurpose Internet Mail Extensions),
- storitve oz. aplikacije, za katere se zahteva uporaba spletnih kvalificiranih digitalnih potrdil overitelja na CVI.

(8) Politika delovanja overitelja na CVI je definirana z vrstami kvalificiranih digitalnih potrdil:
- Politika SIGOV-CA za osebna kvalificirana digitalna potrdila za institucije javne uprave,
- Politiko SIGOV-CA za spletna kvalificirana digitalna potrdila za institucije javne uprave,
- Politiko SIGEN-CA za kvalificirana digitalna potrdila za pravne in fizične osebe, registrirane za opravljanje dejavnosti,
- Politika SIGEN-CA za kvalificirana spletna digitalna potrdila za fizične osebe.

(9) V primeru kvalificiranih digitalnih potrdil za institucije javne uprave in za pravne in fizične osebe, registrirane za opravljanje dejavnosti ima glede preklica kvalificiranih digitalnih potrdil predstojnik institucije javne uprave oz. pooblaščena oseba pravne ali fizične osebe, registrirane za opravljanje dejavnosti, enake pravice kot ostali imetniki kvalificiranih digitalnih potrdil iz iste institucije oz. pravne ali fizične osebe, registrirane za opravljanje dejavnosti.

(10) Overitelj na CVI si pridržuje pravico do spremembe te politike in nadgradnje infrastrukture brez predhodnega obveščanja imetnikov kvalificiranih digitalnih potrdil. Veljavna kvalificirana digitalna potrdila pri tem ostanejo v veljavi do konca preteka veljavnosti po veljavni politiki ob njihovi izdaji oz. podaljšanju potrdil. Nova verzija politike overitelja na CVI se sedem (7) dni pred veljavo predhodno objavi na spletnih straneh overitelja na CVI pod novo identifikacijsko številko (CP_{OID}) in označenim datumom začetka njene veljavnosti. Vsa kvalificirana digitalna potrdila izdana oz. podaljšana po tem datumu se obravnavajo po novi politiki.

(11) Overitelj na CVI se lahko povezuje v mrežo overiteljev na horizontalni ali vertikalni ravni, to je ustanavlja in overja podrejene ali priznava enakovredne overitelje ter se povezuje v hierarhično globalno strukturo overiteljev.

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

2. SPLOŠNE DOLOČBE

(1) Pričujoča politika (CP_{OID} = 1.3.6.1.4.1.6105.2.2.1) definira delovanje overitelja na CVI za spletna kvalificirana digitalna potrdila za fizične osebe.

(2) Posamezni izrazi imajo v nadaljevanju te politike naslednji pomen:
- **SIGEN-CA** je izdajatelj kvalificiranih digitalnih potrdil za fizične osebe v okviru delovanja overitelja na CVI,
- **potrdilo** je spletno kvalificirano digitalno potrdilo (angl.: qualified digital certificate) v elektronski obliki, ki povezuje podatke iz potrdila z imetnikovim zasebnim ključem ter potrjuje imetnikovo identiteto.
- **imenik** je javni imenik potrdil overitelja na CVI,
- **objava SIGEN-CA** je javna objava na spletnih straneh SIGEN-CA,
- **vloge** so obrazci SIGEN-CA za izdajo in preklic, ki so objavljeni na spletnih straneh SIGEN-CA in pri pooblaščenih osebah na prijavnih službah,

- **obvestila SIGEN-CA** so vsa navodila, pojasnila, seznami, pogoji, posamezna obvestila, priporočila, standardi in drugi dokumenti, ki jih določi ali priporoči SIGEN-CA in jih objavi ali kako drugače posreduje imetnikom potrdil ali tretjim osebam.

(3) Ta politika določa upravljanje (rezervacijo, izdajanje in overjanje, preklicevanje, hranjenje in objavljanje) potrdil za imetnike potrdil, ki so lahko:
- fizične osebe ali
- drugi overitelji potrdil.

(4) Stroške potrebne strojne ali programske opreme, ki jo zahteva oz. predlaga SIGEN-CA za varno shranjevanje in uporabo potrebnih podatkov potrdila na strani imetnika potrdila, krije imetnik potrdila.

(5) Vsak imetnik oz. bodoči imetnik potrdila ima pravico pritožbe glede kateregakoli postopka SIGEN-CA. Pritožbo v roku 15 dni v pisni obliki poda Komisiji za pritožbe SIGEN-CA osebno, digitalno podpisano na elektronski naslov *komisija.sigen-ca@gov.si* ali v pisni obliki na naslov:

Komisija za pritožbe SIGEN-CA
Center Vlade za informatiko
Langusova 4
1000 Ljubljana

(6) Komisijo za pritožbe SIGEN-CA sestavljajo predsednik in štirje člani. Vsaj dva člana nista zaposlena na CVI. Nihče od članov Komisije za pritožbe ni iz osebja overitelja na CVI.

(7) Komisijo za pritožbe SIGEN-CA imenuje direktor CVI. Komisija je pri svojem delu neodvisna in samostojna. Strokovno, tehnično in administrativno podporo Komisiji za pritožbe nudi CVI.

(8) Komisija za pritožbe SIGEN-CA odloči o vsaki prejeti pritožbi z večino glasov opredeljenih članov v roku 30 dni. O postopkovnih vprašanjih odloča z večino glasov vseh članov. Odločitev Komisije za pritožbe SIGEN-CA je dokončna in jo je overitelj na CVI dolžan izvršiti.

(9) Komisija za pritožbe SIGEN-CA deluje v skladu s poslovnikom, ki ga odobri direktor CVI.

3. RAZPOZNAVNI PODATKI SIGEN-CA

3.1. Identiteta SIGEN-CA

Enolično ime:	**ou=SIGEN-CA, o=state-institutions, c=si**
Naslov:	**SIGEN-CA** **Center Vlade RS za informatiko** **Langusova 4** **1000 Ljubljana** **Slovenija** **Tel.: (+386) 01 4788 600** **Fax: (+386) 01 4788 649** **E-pošta: SIGEN-CA@GOV.SI**
Dežurna številka za preklice:	**Tel.: (+386) 01 4788 777**

Osnovne informacije o SIGEN-CA so na voljo na spletnem strežniku CVI z naslovom:

http://www.sigen-ca.si

SIGEN-CA je ob začetku svojega delovanja generirala svoje lastno potrdilo (potrdilo SIGEN-CA, serijska številka 3B3CF9C9), ki je namenjeno podpisovanju potrdil za druge uporabnike ter preverjanju podpisa SIGEN-CA oz. veljavnosti podatkov v potrdilih imetnikov.

Potrdilo SIGEN-CA vsebuje naslednje podatke:

Serijska številka	3B3CF9C9
Overitelj potrdila	SIGEN-CA
Imetnik potrdila	SIGEN-CA
Veljavnost potrdila	od 29.junija 2001 do 29.junija 2021
Dolžina ključa	2048 bitov
MD5	49EF A6A1 F0DE 8EA7 6AEE 5B7D 1E5F C446
SHA-1	3E42 A187 06BD 0C9C CF59 4750 D2E4 D6AB 0048 FDC4

3.2. Identiteta imetnikov potrdil

Potrdila so shranjena v strukturi javnega imenika po standardu X.509 ver. 3. na strežniku Centra Vlade za informatiko z imenom *x500.gov.si*, ki je javno dostopen.

Potrdila se nahajajo v podstrukturi:

ou=SIGEN-CA, o=state-institutions, c=si

3.3. Identiteta registra preklicanih potrdil

Register preklicanih potrdil je objavljen v javnem imeniku in se nahaja v veji:

cn=CRL*n*[1], ou=SIGEN-CA, o=state-institutions, c=si

4. INFRASTRUKTURA OVERITELJA NA CVI

4.1. Osnovne lastnosti overitelja na CVI

4.1.1. Varnost in zanesljivost infrastrukture overitelja na CVI

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

(1) Oprema overitelja na CVI je postavljena v posebnih, ločenih prostorih v okviru infrastrukture CVI, deloma pa tudi izven le-te. Zavarovana je z večnivojskim sistemom fizičnega in elektronskega varovanja. Stopnja varovanja infrastrukture overitelja na CVI ustreza nivoju varovanja po standardu *FIPS 140-1 level 3*.

(2) Varnostne kopije programske opreme in šifriranih baz overitelja na CVI se redno obnavljajo in shranjujejo v dveh ločenih in fizično varovanih prostorih. Redno se preverjajo računalniški dnevniki na vseh računalniško-komunikacijskih napravah s strani članov skupine overitelja na CVI, izvajanje postopkov pa s strani nadzorne skupine overitelja na CVI.

(3) Opis infrastrukture overitelja na CVI, operativno delovanje in postopki upravljanja z infrastrukturo ter naloge nadzorne skupine overitelja na CVI so določeni z Interno politiko overitelja na CVI, ki predstavlja zaupni del notranjih pravil overitelja na CVI.

4.1.2. Šifrirni algoritmi, formati podatkov in protokoli infrastrukture overitelja na CVI

(1) Overitelj na CVI uporablja:

- za podpisovanje potrdil algoritem SHA-1 z RSA s parom ključev dolžine 2048 bitov,
- za šifriranje podatkov algoritme Triple DES, CAST-128 in RC2, (standardi FIPS PUB 81, ANSI X3.106 in ISO/IEC 10116),
- zgostitveni algoritem SHA-1 (FIPS PUB 180-1 in ANSI X9.30(2)) in MD5 (RFC 1321),
- način uporabe algoritma RSA za upravljanje s ključi RSA (RFC 1421 in RFC 1423(PEM) in PKCS#1),
- format potrdil ustreza priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:1997 ter X.509 ver. 3 (v3),
- registri preklicanih potrdil ustrezajo priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:1997, vključno z verzijo 2 (v2),
- oblika RSA enoličnih razločevalnih imen ter format javnega ključa ustrezajo priporočilu RFC 1422 in 1423 in PKCS#1,
- protokol LDAP ustreza priporočilu RFC 1777,
- hranjenje zasebnega ključa ustreza priporočiloma PKCS#5 in PKCS#8,
- komunikacija med programsko opremo na strani imetnika in infrastrukturo SIGEN-CA poteka po protokolu SEP (angl.: Secure Exchange Protocol), ki temelji na standardu GULS (angl.: Generic Upper Layers Security), ki ustreza priporočilom ITU-T za X.830, X.831, X.832 in ISO/IEC 11586-1, 11586-2 in 11586-3.

(2) Celoten nabor algoritmov, formatov podatkov in protokolov je na razpolago pri overitelju na CVI.

4.1.3. Osebje overitelja na CVI

(1) Operativno, organizacijsko in strokovno pravilno delovanje overitelja na CVI vodi vodja Sektorja za upravljanje digitalnih potrdil na CVI in je organizacijsko direktno podrejen direktorju CVI.

Med stalno pooblaščene osebe overitelja na CVI spadajo člani skupine overitelja na CVI in nadzorne skupine, ki jo vodi vodja Služba za varovanje in zaščito na CVI. Zunanje sodelavce, ki opravljajo dela za overitelja na CVI po potrebi, predlaga vodja overitelja na CVI in odobri direktor CVI.

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

(3) Vse organizacijske skupine overitelja na CVI so med seboj nezdružljive. Navedeno število oseb predstavlja minimalno število, ki pa se lahko povečuje. Ob pomanjkanju ustrezno usposobljenega kadra pa se lahko zaradi podobne vrste opravil združi osebje določenih skupin z enakimi oz. podobnimi privilegiji delovanja. Vloge posameznih organizacijskih skupin so določene z Interno politiko overitelja na CVI.

4.1.4. Zavarovanje odgovornosti overitelja na CVI

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

4.1.5. Zahteve za podrejene overitelje

Medsebojna razmerja med overiteljem na CVI in podrejenim overiteljem se izvaja na podlagi podpisane pisne pogodbe. Overitelj na CVI zagotavlja, da podrejeni overitelji izpolnjujejo ustrezno raven varnostnih zahtev. Overitelj na CVI redno pregleduje izpolnjevanje varnostnih zahtev in postopkov pri upravljanju s potrdili podrejenih overiteljev.

4.1.6. Lastnosti medsebojnega priznavanja

(1) Overitelj na CVI se lahko povezuje in priznava z domačimi in tujimi overitelji, vendar ni dolžna priznati drugih overiteljev tudi, če ima drugi overitelj status akreditiranega overitelja. Medsebojno priznavanje se izvaja na podlagi podpisane pisne pogodbe.

(2) Overitelj na CVI zagotavlja, da bo izvajala medsebojno priznavanje izključno po podpisu pisne pogodbe z drugimi overitelji, ki pa morajo izpolnjevati vsaj najmanjšo raven varnostnih zahtev, ki veljajo za podrejene overitelje overitelja na CVI. Pooblaščene osebe overitelja na CVI pregledujejo javni in zaupni del notranjih pravil drugega overitelja.

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

(4) Bistvene dele pogodb o medsebojnem priznavanju, ki se nanašajo na lastnosti potrdil enega ali obeh overiteljev ali na pravice in obveznosti imetnikov teh potrdil ali tretjih oseb, ki se zanašajo na ta potrdila, objavi overitelj na CVI.

4.1.7. Vloga in pomen prijavnih služb SIGEN-CA

(1) Naloge prijavne službe so:
- preverjajo istovetnost bodočih imetnikov,
- sprejemajo in preverjajo podatke v vlogi za pridobitev potrdil,
- sprejemajo vloge za preklic potrdil,
- izdajajo potrebno dokumentacijo imetnikom oz. bodočim imetnikom,
- vloge na varen način posredujejo na SIGEN-CA.

(2) Institucije, ki opravljajo naloge prijavne službe, pooblasti overitelj na CVI. Izpolnjevati morajo pogoje za opravljanje nalog prijavnih služb, ki jih določi in objavi overitelj na CVI.

(3) Bodoči imetnik potrdila izpolni vlogo za pridobitev potrdila in jo odda osebno na pristojni prijavni službi. Na prijavni službi se na podlagi ustrezne dokumentacije preveri podatke o bodočem imetniku in se odobri izdaja potrdila.

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

4.1.8. Javni imenik potrdil

(1) Vsa potrdila so objavljena v imeniku, ki je v skrbništvu overitelja na CVI.

(2) Stalen dostop do imenika je možen po protokolu LDAP. Potrdila so shranjena v polju "userCertificate".

(3) V imeniku je tudi register preklicanih potrdil.

(4) Register preklicanih potrdil se osvežuje:
- po vsakem preklicu potrdila,
- enkrat dnevno, če ni novih zapisov oz. sprememb v registru preklicanih potrdil (24 ur po zadnjem osveževanju).

(5) Register preklicanih potrdil vsebuje:
- identifikacijsko oznako preklicanega potrdila in
- čas in datum preklica.

4.2. Osnovne lastnosti potrdila

(1) Na podlagi pričujoče politike SIGEN-CA izdaja:
- potrdila za fizične osebe ter
- potrdila za druge overitelje na osnovi pisne pogodbe.

(2) Potrdilo se izda na osnovi pravilno izpolnjene in podpisane vloge na ustreznem obrazcu.

(3) Vsak imetnik spletnega potrdila ima en par ključev, ki ga sestavlja zasebni in javni ključ. Par ključev se tvori z imetnikovo programsko opremo. Zasebni ključ ima samo imetnik. Javni ključ imetnika pa se pošlje SIGEN-CA v postopku tvorbe potrdila. Javni ključ je objavljen kot sestavni del potrdila.

Ključi so 1024-bitni RSA.

(4) SIGEN-CA hrani nujno potrebne podatke o imetniku spletnega potrdila, ki so vključeni v to potrdilo. SIGEN-CA nikoli ne hrani in tudi nima dostopa do zasebnega ključa imetnika spletnega potrdila.

(5) Veljavnost spletnih potrdil je največ pet (5) let od prevzema.

(6) Podatki v spletnem potrdilu so:
- identifikacijska oznaka,
- nedvoumno razločevalno ime potrdila (DN), dodatno serijsko številko ter ime in priimek imetnika potrdila,
- elektronski naslov imetnika,
- številka politike, pod katero je bilo izdano potrdilo (CP_{OID}), in iz katere je razvidno tudi, da gre za kvalificirano potrdilo,
- začetek in konec veljavnosti potrdila,
- naziv in sedež SIGEN-CA,
- javni ključ,
- identiteta registra preklicanih potrdil,
- podatki o uporabi potrdila,
- podatki o šifrirnih algoritmih.

(7) Imetnik potrdila je nedvoumno določen z razločevalnim imenom (DN). Vsak imetnik potrdila ima lahko pod istimi naštetimi podatki eno samo potrdilo.

(8) Imetnik lahko zaprosi za največ tri (3) potrdila v obdobju dveh (2) let.

4.2.1. Zahteve za elektronski naslov

(1) Elektronski naslov mora izpolnjevati naslednje zahteve:
- mora biti enolično,
- mora biti pomensko povezano z imetnikom,
- ne sme vsebovati šumnikov,
- dovoljene so samo črke angleške abecede (A-Z), pri čemer ni razlike med velikimi in malimi črkami, cifre (0-9) ter pomišljaj (-),
- prvi ali zadnji znak ne smeta biti pomišljaj,
- dolžina niza je lahko med 3 in 24 znaki.

(2) Overitelj na CVI si pridržuje pravico za zavrnitev vloge za potrdilo, 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.

5. UPRAVLJANJE POTRDIL

5.1. Izdaja potrdila

(1) Za pridobitev potrdila mora bodoči imetnik pravilno izpolniti in podpisati vlogo za pridobitev potrdila.

(2) Vloge za pridobitev potrdila so dostopne na prijavnih službah in na spletnih straneh SIGEN-CA.

(3) Izdajo potrdila odobrijo pooblaščene osebe overitelja, ki si pridržujejo pravico za zavrnitev izdaje potrdila. O odobritvi oz. zavrnitvi je bodoči imetnik obveščen. V primeru odobritve bodoči imetnik prejme vso potrebno dokumentacijo v skladu s 36. členom ZEPEP. Dokumentacija vključuje to politiko ter potrebna navodila in pojasnila v skladu z veljavnimi predpisi in s katerimi je bil bodoči imetnik seznanjen že pred podpisom vloge za izdajo potrdila.

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

(5) SIGEN-CA na podlagi odobrene vloge opravi rezervacijo potrdila v desetih (10) dneh od odobritve vloge. Pri tem bodoči imetnik potrdila prejme referenčno številko in avtorizacijsko kodo za prevzem potrdila.

(6) SIGEN-CA preda bodočemu imetniku potrdila referenčno številko in avtorizacijsko kodo osebno ali pa ju posreduje po dveh ločenih poteh: referenčno številko po elektronski pošti, avtorizacijsko kodo pa po priporočeni pošti. Po prevzemu potrdila postaneta referenčna številka in avtorizacijska koda neuporabni.

(7) Bodoči imetnik potrdila mora po prejemu referenčne številke in avtorizacijske kode potrdilo prevzeti v šestdesetih (60) dneh od rezervacije potrdila, sicer SIGEN-CA rezervacijo potrdila prekliče.

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

5.2. Preklic potrdila

(1) Overitelj na CVI prekliče potrdilo tudi na zahtevo imetnika, na zahtevo pristojnega sodišča, sodnika za prekrške ali upravnega organa.

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

(3) 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 ključni podatki, ki so navedeni v potrdilu.

(4) Če potrdilo vsebuje podatke o tretji osebi, je ta dolžna zahtevati preklic potrdila, če izve, da je bil zasebni ključ imetnika potrdila ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

(5) Overitelj na CVI prekliče potrdilo tudi brez zahteve imetnika, takoj ko izve:
- da so se spremenile okoliščine, ki vplivajo na veljavnost potrdila,
- 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 je bila infrastruktura overitelja na CVI 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 prenehala z izdajanjem potrdil ali da je bilo overitelju na CVI prepovedano upravljanje s potrdili in njegove dejavnosti ni prevzel drug overitelj,
- da je preklic odredilo pristojno sodišče, sodnik za prekrške ali upravni organ.

(6) Overitelj na CVI v primerih iz prejšnjega odstavka prekliče potrdilo brez predhodnega obvestila imetniku potrdila.

(7) Preklic lahko imetnik zahteva osebno v rednem delovnem času, elektronsko in telefonsko pa 24 ur na dan vse dni v letu.

(8) Če se preklic opravi osebno, je potrebno ustrezno vlogo za preklic potrdila izročiti na prijavno službo.

(9) Če se preklic opravi elektronsko, mora imetnik na SIGEN-CA poslati vlogo za preklic, ki mora biti digitalno podpisana z zaupanja vrednim potrdilom. Ob poslanem zahtevku za preklic mora izdajatelj zahtevka za preklic hkrati tudi telefonsko obvestiti SIGEN-CA na dežurno telefonsko številko za preklice.

(10) Če se preklic zahteva s strani imetnika digitalnega potrdila samo telefonsko na dežurno telefonsko številko za preklice, mora imetnik ob tem navesti geslo, ki ga je v ustrezni vlogi za izdajo potrdila imetnik podal kot geslo za preklic potrdila. Če le-tega v vlogi za pridobitev potrdila ni navedel, telefonsko ne more preklicati potrdila.

(11) Overitelj na CVI bo po prejemu veljavne zahteve za preklic najkasneje v štirih (4) urah preklicala potrdilo. V tem času bo preklicano potrdilo v imeniku dodano v register preklicanih potrdil.

5.3. Morebitno prenehanje delovanja overitelja na CVI oz. SIGEN-CA

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

6. ODGOVORNOST

6.1. Odgovornost imetnika potrdila

Imetnik oziroma bodoči imetnik potrdila je dolžan:
- skrbno prebrati to politiko pred podpisom vloge za potrdilo,
- spremljati vsa obvestila SIGEN-CA in ravnati v skladu z njimi,
- uporabljati potrdilo v skladu s to politiko,
- osebno prevzeti potrdilo,

- ob prevzemu potrdila preveriti podatke v potrdilu in ob morebitnih napakah ali problemih takoj obvestiti SIGEN-CA oziroma zahtevati preklic,
- spremljati razvoj tehnologije oziroma obvestila SIGEN-CA in ustrezno posodabljati potrebno strojno in programsko opremo za varno delo s potrdili,
- uporabljati tako programsko opremo, ki je v skladu z obvestili SIGEN-CA (z dovolj močnimi kriptografskimi moduli),
- zasebni ključ in vse druge zaupne podatke ščititi s primernim geslom ali na drug način tako, da ima dostop do njih samo imetnik,
- poskrbeti za varnostno kopijo svojega zasebnega ključa, če programska in strojna oprema to omogoča, in jo shraniti na varnem mestu,
- po preteku veljavnosti potrdila uničiti vse podatke za uporabo potrdila,
- skrbeti za originalno podpisane dokumente in arhiv teh dokumentov,
- uporabljati potrdilo v času njegove veljavnosti,
- vse spremembe, ki so povezane s potrdilom, nemudoma sporočiti SIGEN-CA,
- zahtevati preklic potrdila, če je bil zasebni ključ ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu,
- nositi odgovornost za vsako škodo, ki je bodisi posredno ali neposredno povzročena zato, ker je bila omogočena uporaba oz. zloraba imetnikovega potrdila s strani nepooblaščenih oseb,
- nositi odgovornost za škodo v vsakem primeru zlorabe potrdila od prijave preklica do preklica.

6.2. Odgovornost za tretje osebe

(1) Tretja oseba mora:

- skrbno prebrati to politiko in vsa obvestila overitelja na CVI,
- ravnati in uporabljati potrdila v skladu s to politiko in obvestili,
- skrbeti za originalno podpisane dokumente,
- v času uporabe potrdila natančno preveriti, če potrdilo ni v registru preklicanih potrdil,
- v času uporabe potrdila preveriti podpis SIGEN-CA, ki je objavljen v tej politiki in tudi na spletnih straneh SIGEN-CA oz. drugih izdajateljev potrdil overitelja na CVI.

(2) Če potrdilo vsebuje podatke o tretji osebi, je ta dolžna zahtevati preklic potrdila, če izve, da je bil zasebni ključ ogrožen na način, ki vpliva na zanesljivost uporabe, ali če obstaja nevarnost zlorabe, ali če so se spremenili podatki, ki so navedeni v potrdilu.

6.3. Odgovornost overitelja na CVI

(1) Overitelj na CVI je pooblaščen:

- za izdajanje potrdil in upravljanje z njimi v skladu s svojimi notranjimi pravili in veljavnimi predpisi,
- za varno hranjenje vseh osebnih in zaupnih podatkov o SIGEN-CA in imetnikih potrdil,
- za točnost podatkov v potrdilu od trenutka izdaje do preklica ali prenehanja veljavnosti potrdila,
- da potrdilo vsebuje vse predpisane podatke za potrdilo po tej politiki in veljavnih predpisih,
- da je imel imetnik potrdila v času izdaje le-tega zasebni ključ ustrezen v potrdilu navedenemu javnemu ključu,

- za takojšen preklic potrdila in objavo preklica v registru preklicanih potrdil, če za preklic obstajajo razlogi po tej politiki ali veljavnih predpisih,
- za izpolnjevanje drugih zahtev te politike, svoje interne politike in veljavnih predpisov.

(2) Overitelj na CVI je dolžan:
- sprejemati podatke o imetnikih samo na način, določen s pravili delovanja prijavnih služb,
- upoštevati odločitve Komisije za pritožbe SIGEN-CA,
- objavljati na svojih spletnih straneh vse informacije o tistih spremembah glede dejavnosti SIGEN-CA, ki kakorkoli vplivajo na imetnike potrdil in tretje osebe.

(3) Overitelj na CVI ni odgovoren za posledice, do katerih bi prišlo zaradi:
- uporabe potrdil za namene, ki niso izrecno predvideni v tej politiki,
- nepravilnega ali pomanjkljivega varovanja gesel ali zasebnih ključev, izdajanje zaupnih podatkov ali ključev tretjim osebam in neodgovornega ravnanja imetnikov,
- kakršnekoli zlorabe oziroma vdora v informacijski sistem imetnika potrdila in s tem do podatkov s strani nepooblaščene osebe,
- nedelovanja ali slabega delovanja informacijske infrastrukture imetnika potrdila ali tretjih oseb,
- nepreverjanja podatkov in veljavnosti potrdil v registru preklicanih potrdil,
- uporabe potrdil na nestandardni način ali na opremi z okrnjenimi kriptografskimi moduli,
- drugega ravnanja imetnika potrdila ali tretje osebe v nasprotju z obvestili SIGEN-CA, to politiko in veljavnimi predpisi.
- škode, ki je bodisi posredno ali neposredno povzročena zato, ker je bila omogočena uporaba oz. zloraba imetnikovega potrdila nepooblaščenim osebam s strani ali zaradi nepazljivega ravnanja imetnika,

(4) Overitelj na CVI ni odgovoren:
- za uporabo in zanesljivost delovanja strojne in programske opreme, ki jo priporoča,
- za uporabo potrdil ter veljavnost potrdil ob spremembah elektronskih naslovov ali spremembah imen imetnikov.

(5) Overitelj na CVI ni v nobenem primeru pooblaščen za vsebino podatkov, ki se šifrirajo ali podpisujejo z uporabo njenih potrdil, ali za ravnanje 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.

(6) Po preklicu oz. preteku veljavnosti potrdila overitelj na CVI ni več odgovoren za posledice v zvezi z uporabo tega potrdila, razen za objavo v registru preklicanih potrdil.

(7) Infrastruktura overitelja na CVI ustreza najvišjim stopnjam varovanja in zaščite potrdil in ključev, vendar je varnost potrdil zagotovljena samo, če imetniki in tretje osebe, ki se zanašajo na potrdila, upoštevajo in ravnajo v skladu z obvestili SIGEN-CA.

(8) Infrastruktura overitelja na CVI deluje 24 ur na dan vse dni v letu, vendar si overitelj na CVI pridržuje pravico za ustavitev delovanja v primeru nepravilnega delovanja, možnosti zlorabe, tehničnih vzrokov. V primeru vzdrževanja ali nadgradnje overitelja na CVI se vzdrževalna dela sedem (7) dni predhodno objavi.

(9) Overitelj na CVI 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 to na vlogi za izdajo potrdila ali kasneje v pisni obliki odobril imetnik potrdila, ali na zahtevo pristojnega sodišča, sodnika za prekrške ali upravnega organa. Podatki se posredujejo tudi brez pisne privolitve, če to določa zakonodaja oz. veljavni predpisi.

7. KONČNE DOLOČBE

(1) Ob morebitnem sporu med overiteljem na CVI na eni strani in imetnikom potrdila ali tretjo osebo na drugi strani, se bo druga stran najprej pritožila Komisiji za pritožbe SIGEN-CA.

(2) Če postopek pred Komisijo za pritožbe SIGEN-CA ne reši spora, je zanj pristojno sodišče v Ljubljani po pravu Republike Slovenije.

(3) Določbe glede avtorskih, sorodnih in drugih pravic intelektualne lastnine:

- na pričujoči politiki pripadajo vse pravice overitelju na CVI,
- na javnih ključih pripadajo vse pravice overitelju na CVI,
- na zasebnem ključu pripadajo vse pravice imetniku potrdila,
- na vseh ostalih podatkih v potrdilu vse pravice pripadajo overitelju na CVI.

8. TERMINOLOŠKI SLOVAR IN OZNAKE

CP_{Name}	Ime politike delovanja overitelja (*Angl.: Certification Policy Name*), enolično povezano z mednarodno številko politike delovanja $CP_{OID.}$ (*Angl.: Certification Policy Object Identifier*).
CP_{OID}	Mednarodna številka, ki enolično določa politiko delovanja (*Angl.: Certification Policy Object IDentifier*).
CRL	Seznam preklicanih potrdil (prim. definicijo Register preklicanih potrdil). (*Angl.: CRL, Certification Revocation List)*.
CVI	Center Vlade Republike Slovenije za informatiko.
DN	Enolično razločevalno ime (prim. definicijo Razločevalno ime). (*Angl.: DN, Distinguished Name*).
Dodatna serijska številka	Enolično 13-mestno število, ki ga potrdilu podeli SIGEN-CA. Prvih 8 mest številke je enolično število uporabnika, 9. in 10. mesto določata vrsto potrdila, naslednji dve mesti predstavljata zaporedno številko potrdila, zadnje mesto je kontrola zapisa po mod. 11.
Imetnik potrdila	Imetnik potrdila je oseba, ki je navedena v potrdilu in ki razpolaga s svojim zasebnim ključem.
Infrastruktura overitelja na CVI	Infrastruktura overitelja na CVI so vsi prostori overitelja, njegova strojna in programska oprema ter varnostni mehanizmi, ki so potrebni za varno delovanje.
Javni imenik potrdil	Javni imenik na CVI po standardu X.500, kjer so shranjena potrdila po standardu X.509 ver. 3.
LDAP	LDAP (*Angl.: Leightweight Directory Access Protocol*) je protokol, ki določa dostop do imenika in je specificiran po IETF (*Angl.: Internet Engineering Task Force*) priporočilu RFC 1777.
Overitelj	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi. (*Angl.: CA, Certification Authority*).
Potrdilo	Potrdilo v elektronski obliki, ki povezuje podatke iz potrdila z zasebnim ključem določene osebe ter potrjuje njeno identiteto. (*Angl.: Digital certificate)*.
Prijavna služba	Služba ali oseba za sprejem vlog za potrdila in preverjanje istovetnosti bodočih imetnikov. (*Angl.: RA, Registration Authority*).
Razločevalno ime	Enolično ime (prim. definicijo DN) v potrdilu, ki nedvoumno in enolično definira imetnika v strukturi javnega imenika.
Register preklicanih potrdil	Seznam preklicanih potrdil. (*Angl.: CRL, Certification Revocation List*.) Osvežuje se enkrat dnevno oz. z vsakim preklicem potrdila.

SIGEN-CA	Izdajatelj potrdil za pravne in fizične osebe overitelja potrdil na Centru Vlade za informatiko (CVI). (*Angl.: SI, Slovenian*, GEN, General, CA, Overitelj) (prim. definicijo Overitelj).
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 57/2000)