CENTER VLADE REPUBLIKE SLOVENIJE
ZA INFORMATIKO

POLITIKA SI-TSA

za izdajo varnih časovnih žigov

Javni del notranjih pravil overitelja na
Centru Vlade Republike Slovenije za informatiko

veljavnost: od 10. septembra 2004
verzija: 2.0

CP_{Name}: SI-TSA-1
CP_{OID}: 1.3.6.1.4.1.6105.3.1.2

Izdaje politik delovanja SI-TSA
Verzija 2.0
Politika SI-TSA za izdajo varnih časovnih žigov CP_{OID}: 1.3.6.1.4.1.6105.3.1.2 CP_{Name}: SI-TSA-1 pričetek veljavnosti: 10. september 2004
Verzija 1.0
Politika SI-TSA za izdajo varnih časovnih žigov CP_{OID}: 1.3.6.1.4.1.6105.3.1.1 CP_{Name}: SI-TSA-1 pričetek veljavnosti: 10. november 2003

VSEBINA

1. UVOD 5

1.1. Pregled 5

1.2. Pomen izrazov 6

1.3. Razpoznavni podatki izdajatelja SI-TSA 6
1.3.1 Identiteta overitelja na CVI 6
1.3.2 Identiteta izdajatelja SI-TSA 7

1.4. Subjekti in namen uporabe 8
1.4.1 Overitelj na CVI in izdajatelj SI-TSA 8
1.4.2 Uporabniki varnih časovnih žigov 9
1.4.3 Tretje osebe 9
1.4.4 Namen uporabe 9

1.5. Skladnost z veljavno zakonodajo in drugimi predpisi 9

(3) SI-TSA zagotavlja skladnost svojih storitev s pričujočo politiko, ki se dodeli vsakemu časovnemu žigu. 9

2. OBVEZNOSTI IN ODGOVORNOST 9

2.1. Obveznost SI-TSA 9
2.1.1 Splošno 9
2.1.2 Obveznost SI-TSA do uporabnikov 10

2.2. Obveznosti uporabnikov 10

2.3. Obveznosti tretjih oseb 10

2.4. Omejitve glede uporabe 10

3. VARNOST DELOVANJA SI-TSA 10

3.1. Postopki in izjava o politiki delovanja SI-TSA 11
3.1.1 Izjava o postopkih SI-TSA 11
3.1.2 Izjava o politiki SI-TSA 11

3.2. Upravljanje s ključi SI-TSA 11
3.2.1 Generiranje ključev SI-TSA 11
3.2.2 Zaščita zasebnega ključa SI-TSA 12
3.2.3 Dostava digitalnega potrdila SI-TSA 12
3.2.4 Obnova javnega ključa SI-TSA 12
3.2.5 Konec veljavnosti ključev SI-TSA 12
3.2.6 Upravljanje s kriptografskimi moduli za časovne žige 12

3.3. Časovno žigosanje 12
3.3.1 Časovni žig 12
3.3.2 Sinhronizacije ure 13

3.4. Upravljanje in izvedba operacij SI-TSA 13

4. UPRAVLJANJE Z DOKUMENTACIJO 13

5. TERMINOLOŠKI SLOVAR IN OZNAKE 13

POVZETEK

Politike overitelja na Centru Vlade Republike Slovenije za informatiko (overitelj na CVI) predstavljajo celoten javni del notranjih pravil overitelja na CVI in določajo namen, delovanje in metodologijo upravljanja s kvalificiranimi digitalnimi potrdili, dodeljevanje časovnih žigov, odgovornost overitelja na CVI ter zahteve, ki jih morajo izpolnjevati imetniki, naročniki in tretje osebe, ki se zanašajo na kvalificirana digitalna potrdila in na varne časovne žige, in drugi overitelji, ki želijo uporabljati storitve overitelja na CVI.

Overitelj na CVI izdaja kvalificirana digitalna potrdila in varne časovne žige, za katera velja najvišja stopnja varovanja in načela t.i. močne enkripcije ter deluje v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 57/2000) 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.

Overitelja na CVI (http://www.gov.si/ca*)* predstavljata dva izdajatelja kvalificiranih digitalnih potrdil:

- SIGEN-CA (angl. *Slovenian General Certification Authority*) za državljane in pravne osebe, http://www.sigen-ca.si,
- SIGOV-CA (angl. *Slovenian Governmental Certification Authority*) za institucije javne uprave Republike Slovenije, ki so v informacijsko-telekomunikacijskem omrežju državnih organov, http://www.sigov-ca.gov.si,

ter izdajatelj varnih časovnih žigov:

- SI-TSA (angl. *Slovenian Time Stamping Authority)*, http://www.si-tsa.si.

Pričujoči dokument določa delovanje izdajatelja za varno časovno žigosanje SI-TSA, ki je del infrastrukture javnih ključev (PKI, angl. Public Key Infrastructure) overitelja na CVI. Ko želimo v neki aplikaciji časovno žigosati nek elektronski dokument oziroma podatke, pošljemo izdajatelju SI-TSA z zgostitveno funkcijo narejen "povzetek" (angl. *hash*) dokumenta oziroma podatkov. To je niz bitov določene dolžine (običajno 160 bitov), ki enolično določa dokument. Izdajatelj temu povzetku dopiše čas in vse skupaj podpiše s svojim zasebnim ključem - to je varen časovni žig. S tem je dokazano, da je elektronski dokument obstajal pred časom, navedenim v časovnem žigu, poleg tega pa se da preveriti, da se od časa žigosanja ni spremenil.

Pričujoči dokument določa pričetek delovanja izdajatelja SI-TSA po politiki CP_{OID}: 1.3.6.1.4.1.6105.3.1.2. Po tej politiki se lahko storitve SI-TSA uporabljajo za aplikacije, katerih upravljanje je v pristojnosti institucij javne uprave in za aplikacije, katerih upravljanje je v pristojnosti pravnih in fizičnih oseb, registriranih za opravljanje dejavnosti. Uporabniki storitev SI-TSA so po tej politiki tudi vsi imetniki osebnih kvalificiranih digitalnih potrdil SIGOV-CA in SIGEN-CA. Navodila za uporabo storitev so objavljena na spletnih straneh SI-TSA, http://www.si-tsa.si oz. http://www.si-tsa.gov.si.

1. UVOD

1.1. Pregled

(1) Politike overitelja na Centru Vlade Republike Slovenije za informatiko (overitelj na CVI) predstavljajo celoten javni del notranjih pravil overitelja na CVI in določajo namen, delovanje in metodologijo upravljanja s kvalificiranimi digitalnimi potrdili, dodeljevanje časovnih žigov, odgovornost overitelja na CVI ter zahteve, ki jih morajo izpolnjevati imetniki, naročniki in tretje osebe, ki se zanašajo na kvalificirana digitalna potrdila in na varne časovne žige, in drugi overitelji, ki želijo uporabljati storitve overitelja na CVI.

(2) Overitelj na CVI izdaja kvalificirana digitalna potrdila in varne časovne žige, za katera velja najvišja stopnja varovanja in načela t.i. močne enkripcije ter deluje v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 57/2000) in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/2000 in 2/2001), direktivami EU 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) Varni časovni žigi overitelja na CVI so namenjeni:
- zagotavljanju, da je bil dokument podpisan z veljavnim digitalnim potrdilom v določenem časovnem trenutku in sicer na način, da povezuje datum in čas podpisa ter podatke v elektronski obliki na kriptografsko varen način,
- za druge potrebe, kjer je potrebno dokazati časovne lastnosti transakcij in drugih storitev.

(5) Overitelja na CVI predstavljata dva izdajatelja kvalificiranih digitalnih potrdil:
- SIGOV-CA (angl. *Slovenian Governmental Certification Authority*) je izdajatelj kvalificiranih digitalnih potrdil overitelja na CVI za institucije javne uprave, ki so v informacijsko-telekomunikacijskem omrežju državnih organov,
- SIGEN-CA (angl. *Slovenian General Certification Authority*) je izdajatelj kvalificiranih digitalnih potrdil overitelja na CVI za pravne in fizične osebe

ter izdajatelj varnih časovnih žigov:
- SI-TSA (angl. *Slovenian Time Stamping Authority)*.

(6) Izdajatelja SIGOV-CA in SIGEN-CA sta mednarodno registrirana, medsebojno priznana, ter tehnološko in zakonsko enakovredna in enako veljavna.

(7) Javni del notranjih pravil overitelja na CVI je določen z naslednjimi politikami:
- SIGOV-CA za kvalificirana digitalna potrdila za institucije javne uprave,
- SIGEN-CA za kvalificirana digitalna potrdila za pravne in fizične osebe, registrirane za opravljanje dejavnosti,
- SIGEN-CA za spletna kvalificirana digitalna potrdila za fizične osebe,
- SI-TSA za izdajo varnih časovnih žigov.

(8) Pričujoča politika določa delovanje izdajatelja SI-TSA za izdajo varnih časovnih žigov za potrebe varnih storitev, s katerimi upravljajo institucije v javni upravi in za potrebe varnih storitev v pristojnosti pravnih in fizičnih oseb, registriranih za opravljanje dejavnosti.

(9) Po tej politiki SI-TSA izdaja varne časovne žige s točnostjo ene (1) sekunde ali boljše.

1.2. Pomen izrazov

aplikacija	računalniški program, s katerim upravlja organizacija in ki za svoje delovanje potrebuje storitve izdajatelja varnih časovnih žigov
varen časovni žig	varni časovni žig je elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času (2. člen ZEPEP). Varen časovni žig mora v skladu s 34. členom Uredbe vsebovati nedvoumne in pravilne podatke o datumu, točnemu času najmanj na sekundo natančno in overitelju, ki je varni časovni žig ustvaril. Varni časovni žig je lahko dokumentu dodan ali priložen in z njim povezan, vendar morajo biti pri tem vedno izpolnjene enake zahteve kot za varen elektronski podpis s kvalificiranim potrdilom
organizacija	Organizacija je bodisi institucija javne uprave, ki je v informacijsko-telekomunikacijskem omrežju državnih organov, bodisi pravna ali fizična oseba, ki je registrirana za opravljanje dejavnosti v skladu z veljavnimi predpisi v Republiki Sloveniji ali pa tuja oseba, ki opravlja dejavnost in lahko svojo istovetnost dokaže v skladu z veljavnimi predpisi. Naročnik storitev SI-TSA je odgovorna oseba t.j. fizična oseba, ki je pooblaščena za zastopanje organizacije v pravnem prometu.
kvalificirano digitalno potrdilo	Je 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
objava SIGOV-CA	javna objava na spletnih straneh SI-TSA oz. na straneh overitelja na CVI
obvestila SI-TSA	vsa navodila, pojasnila, seznami, pogoji, posamezna obvestila, priporočila, standardi in drugi dokumenti, ki jih določi ali priporoči SI-TSA oz. overitelj na CVI in jih objavi ali kako drugače posreduje uporabnikom varnih časovnih žigov, organizacijam ali tretjim osebam
osebno potrdilo	osebno kvalificirano digitalno potrdilo v elektronski obliki (osebno potrdilo sestavlja potrdilo za podpis/overjanje podpisa in potrdilo za dešifriranje/šifriranje), ki povezuje podatke iz potrdila z imetnikovima zasebnima ključema ter potrjuje imetnikovo istovetnost (angl. *enterprise certificate*)
SI-TSA	*izdajatelj varnih časovnih žigov overitelja na CVI,* angl. *Slovenian Time Stamping Authority*
varen digitalni podpis	elektronski podpis, ki izpolnjuje zahteve 2. člena ZEPEP
Uredba	Uredba o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 77/2000 in 2/2001)
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 57/2000)

1.3. Razpoznavni podatki izdajatelja SI-TSA

1.3.1 Identiteta overitelja na CVI

Naslov:	Center Vlade Republike Slovenije za informatiko Langusova 4 1000 Ljubljana Slovenija
Telefon:	(+386) 01 4788 600
Fax:	(+386) 01 4788 649
URL:	http://www.gov.si/ca

1.3.2 Identiteta izdajatelja SI-TSA

(1) Oznaka pričujoče politike delovanja SI-TSA je: CP_{OID}: 1.3.6.1.4.1.6105.3.1.2.

(2) Kontaktni podatki SI-TSA so:

Naslov:	SI-TSA Center Vlade Republike Slovenije za informatiko Langusova 4 1000 Ljubljana Slovenija
E-pošta:	si-tsa@gov.si
Telefon:	01 4788 600
Fax:	01 4788 649
URL:	http://www.si-tsa.si, http://www.si-tsa.gov.si

(3) Izdajatelj SIGOV-CA je izdal izdajatelju SI-TSA ustrezna digitalna potrdila za izdajatelja varnih časovnih žigov v skladu z veljavno politiko SIGOV-CA. Podatki obeh potrdilih so podani spodaj.

Digitalno potrdilo izdajatelja SI-TSA, t.j. potrdilo SI-TSA-1 je:

Polje	Podatki potrdila SI-TSA-1
Verzija, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Number*	979152364
Algoritem za javni ključ, angl. *Signature Algorithm*	sha1WithRSAEncryption
Izdajatelj potrdila, angl. *Issuer*	c=si, o=state-institutions, ou=sigov-ca
Imetnik potrdila, angl. *Subject*	c=si, o=state-institutions, ou=TSA-certificates, cn=SI-TSA-1 + serialNumber=1234773726013
Pričetek veljavnosti, angl. *Validity: Not Before*	6. november 2003, 15:28:51 GMT
Konec veljavnosti, angl. *Validity: Not After*	6. november 2008, 15:58:51 GMT
Algoritem za javni ključ, angl. *Public Key Algorithm*	rsaEncryption
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA, angl. *RSA Public Key*	ključ dolžine 2048 bitov
Politika izdajatelja, angl. *Certificate Policy*	PolicyIdentifie = Policy: 1.3.6.1.4.1.6105.1.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.gov.si/ca/cps/
Uporaba ključa, angl. *Key Usage*	Digital Signature
Dodatno določilo uporabe, angl. *Extended Key Usage*	Time Stamping
Odtis potrdila	

Odtis potrdila (MD5), angl. *Certificate Fingerprint – MD5*	b0948ee7d55ea4f15cdf5ebecfa65124
Odtis potrdila (SHA-1), angl. *Certificate Fingerprint – SHA*1	db14fba285cb145cd31fb904c056d28c8cb41f5c

Digitalno potrdilo izdajatelja SI-TSA, t.j. potrdilo SI-TSA-2 je:

Polje	Podatki potrdila SI-TSA-2
Verzija, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Number*	979152366
Algoritem za javni ključ, angl. *Signature Algorithm*	sha1WithRSAEncryption
Izdajatelj potrdila, angl. *Issuer*	c=si, o=state-institutions, ou=sigov-ca
Imetnik potrdila, angl. *Subject*	c=si, o=state-institutions, ou=TSA-certificates, cn=SI-TSA-2 + serialNumber=1234773826018
Pričetek veljavnosti angl. *Validity: Not Before*	6. november 2003, 15:40:00 GMT
Konec veljavnosti angl. *Validity: Not After*	6. november 2008, 16:10:00 GMT
Algoritem za javni ključ, angl. *Public Key Algorithm*	rsaEncryption
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z alg. RSA, angl. *RSA Public Key*	ključ dolžine 2048 bitov
Politika izdajatelja, angl. *Certificate Policy*	PolicyIdentifie = Policy: 1.3.6.1.4.1.6105.1.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.gov.si/ca/cps/
Uporaba ključa, angl. *Key Usage*	Digital Signature
Dodatno določilo uporabe, angl. *Extended Key Usage*	Time Stamping
Odtis potrdila	
Odtis potrdila (MD5), angl. *Certificate Fingerprint – MD5*	29a03b4c834ab546a692043a352521b1
Odtis potrdila (SHA-1), angl. *Certificate Fingerprint – SHA*1	9e910fcb664cad6e1006f7f18256c1b04fb459f8

1.4. Subjekti in namen uporabe

1.4.1 Overitelj na CVI in izdajatelj SI-TSA

(1) Overitelj na CVI izdaja kvalificirana digitalna potrdila in varne časovne žige, za katera velja najvišja stopnja varovanja in načela t.i. močne enkripcije ter deluje v skladu z veljavnimi predpisi.

(2) Overitelja na CVI predstavljata dva izdajatelja kvalificiranih digitalnih potrdil:
- SIGOV-CA je izdajatelj kvalificiranih digitalnih potrdil overitelja na CVI za institucije javne uprave, ki delujejo v omrežju državnih organov.
- SIGEN-CA je izdajatelj kvalificiranih digitalnih potrdil overitelja na CVI za pravne in fizične osebe.

ter izdajatelj varnih časovnih žigov:

- SI-TSA (angl. *Slovenian Time Stamping Authority)*.

1.4.2 Uporabniki varnih časovnih žigov

(1) Uporabniki varnih časovnih žigov so:
- aplikacije v skrbništvu organizacij (glej razd. 1.2 za podroben opis organizacije),
- imetniki osebnih potrdil SIGOV-CA ali SIGEN-CA oz. organizacija, kjer so imetniki zaposleni oz. za katero opravljajo delo

(2) Organizacija je naročnik storitev SI-TSA.

(3) Medsebojna razmerja med organizacijo in SI-TSA ureja ta politika in medsebojni dogovor.

1.4.3 Tretje osebe

Tretje osebe so subjekti, ki se zanašajo na izdane varne časovne žige izdajatelja SI-TSA.

1.4.4 Namen uporabe

Storitve SI-TSA so namenjene:
- zagotavljanju, da je bil dokument podpisan z veljavnim digitalnim potrdilom v določenem časovnem trenutku in sicer na način, da povezuje datum in čas podpisa ter podatke v elektronski obliki na kriptografsko varen način,
- za druge potrebe, kjer je potrebno dokazati časovne lastnosti transakcij in drugih storitev.

1.5. Skladnost z veljavno zakonodajo in drugimi predpisi

(1) Overitelj na CVI in izdajatelj SI-TSA delujeta v skladu z:
- Zakonom o elektronskem poslovanju in elektronskem podpisu (Ur.l. RS, št. 57/2000 in 30/2001),
- Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Ur.l. RS, št. 77/2000, 2/2001),
- priporočili RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP),
- in drugimi veljavnimi predpisi.

(2) Oblika in vsebina javnega dela notranjih pravil izdajatelja SI-TSA je usklajena s priporočili ETSI TS 102 023 (v.1.2.1) »Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities«.

(3) SI-TSA zagotavlja skladnost svojih storitev s pričujočo politiko, ki se dodeli vsakemu časovnemu žigu.

2. OBVEZNOSTI IN ODGOVORNOST

2.1. Obveznost SI-TSA

2.1.1 Splošno

SI-TSA oz. overitelj na CVI je dolžan:
- delovati v skladu s svojimi notranjimi pravili in ostalimi veljavnimi predpisi, na katere se politika nanaša,
- izdajati varne časovne žige v skladu s to politiko.

2.1.2 Obveznost SI-TSA do uporabnikov

SI-TSA oz. overitelj na CVI je dolžan izpolnjevati vse obveznosti do svojih naročnikov oz. uporabnikov, vključno z objavljeno razpoložljivostjo in varnostjo svojih storitev.

2.2. Obveznosti uporabnikov

Uporabniki oz. naročniki morajo:
- izpolnjevati zahteve v skladu s to politiko,
- upoštevati priporočila SI-TSA glede zanesljive uporabe varnih časovnih žigov.

2.3. Obveznosti tretjih oseb

Tretje osebe morajo:
- preveriti pravilnost zapisa varnega časovnega žiga,
- preveriti verodostojnost časovnega žiga, t.j. preveriti digitalni podpis izdajatelja SI-TSA,
- preveriti potrdilo izdajatelja SIGOV-CA, ki je podpisal potrdilo SI-TSA,
- upoštevati morebitne omejitve uporabe storitev SI-TSA, kot to določa pričujoča politika,
- upoštevati morebitne druge obveznosti do uporabnikov SI-TSA.

2.4. Omejitve glede uporabe

(1) Omejitev uporabe, razen tistih, ki so določene v tej politiki oziroma v medsebojnem dogovoru, ni.

(2) Uporaba mora biti v skladu z veljavno zakonodajo.

3. VARNOST DELOVANJA SI-TSA

(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) Podrobnejše določbe fizičnega varovanja so skladno z Uredbo določene v Interni politiki overitelja na CVI.

3.1. Postopki in izjava o politiki delovanja SI-TSA

3.1.1 Izjava o postopkih SI-TSA

Vsa določila tega razdelka[1] so, če ni podrobno podano v drugih razdelkih te politike, določena z Interno politiko overitelja na CVI.

3.1.2 Izjava o politiki SI-TSA

Vsa določila izjave o politiki delovanja SI-TSA[2] so, če ni podrobno podano v nadaljevanju tega razdelka, podana v drugih razdelkih te politike.

3.1.2.1 Način uporaba varnih časovnih žigov

Način uporabe storitev varnih časovnih žigov SI-TSA objavi v svojih navodilih na svoji spletni strani.

3.1.2.2 Postopek v primeru sporov

Za reševanje morebitnih sporov je pristojno sodišče v Ljubljani po pravu Republike Slovenije.

3.1.2.3 Nadzor

(1) Izvajanje določb ZEPEP overitelja na CVI skladno z ZEPEP opravlja pristojna inšpekcijska služba.

(2) Overitelj na CVI javno objavi sklepe inšpekcijskega nadzora.

3.2. Upravljanje s ključi SI-TSA

3.2.1 Generiranje ključev SI-TSA

(1) Par ključev za podpisovanje in verifikacijo varnih časovnih žigov se generira v fizično in elektronsko varnem okolju overitelja po posebnem postopku generiranja ključev SI-TSA.

(2) Generiranje ključev se izvede v varnih strojnih kriptografskih modulih, ki so v skladu z določili NIST FIPS 140-2 level 3.

(3) Javni ključ izdajatelja SI-TSA podpiše izdajatelj SIGOV-CA in mu izda digitalno potrdilo.

(4) Digitalno potrdilo z javnim ključem in zasebni ključ SI-TSA se generirajo z algoritmi in na način v skladu z zahtevami SIGOV-CA in v skladu z mednarodno uveljavljenimi priporočili.

(5) Podrobna določila glede generiranja ključev SI-TSA so v skladu z Uredbo v Interni politiki overitelja na CVI.

[1] v skladu s priporočili ETSI TS 102 023 v.1.2.1, razd. 7.1.1
[2] v skladu s priporočili ETSI TS 102 023 v.1.2.1, razd. 7.1.2

3.2.2 Zaščita zasebnega ključa SI-TSA

Zasebni ključi izdajatelja SI-TSA za podpisovanje časovnih žigov so varovani v varnih strojnih kriptografskih modulih, ki so v skladu z določili NIST FIPS 140-2 level 3.

3.2.3 Dostava digitalnega potrdila SI-TSA

(1) Javni ključi izdajatelja SI-TSA so objavljeni in dostavljeni v skladu s politiko SIGOV-CA, vedno v obliki digitalnega potrdila izdajatelja SI-TSA.

(2) Lastnosti in podatki o javnih ključih so objavljeni tudi na spletnih straneh SI-TSA.

3.2.4 Obnova javnega ključa SI-TSA

Veljavnost javnih ključev izdajatelja SI-TSA je določena s politiko SIGOV-CA.

3.2.5 Konec veljavnosti ključev SI-TSA

(1) SI-TSA zagotavlja, da ne uporablja ključev po poteku njihove veljavnosti.

(2) SI-TSA zagotavlja, da pravočasno in na varen način nadomesti pretečene ključe z veljavnimi.

(3) Postopek za uničenje zasebnih ključev po njihovem preteku izdajatelja SI-TSA poteka na varen način skladno z določili Interne politike overitelja na CVI. Zasebni ključi se uničijo tako, da jih ni mogoče restavrirati.

3.2.6 Upravljanje s kriptografskimi moduli za časovne žige

(1) SI-TSA skrbi za varnost strojnih kriptografskih modulov v njihovem celotnem življenjskem ciklu.

(2) Podrobna določila glede ravnanja s kriptografskimi moduli SI-TSA so v skladu z Uredbo v Interni politiki overitelja na CVI.

3.3. Časovno žigosanje

3.3.1 Časovni žig

(1) SI-TSA zagotavlja, da so časovni žigi izdani na varen način s točnim časom, kot je to določeno v razd. 1.1.

(2) Profil časovnega žiga je v skladu z mednarodnimi RFC 3161 »Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)«. Podrobnejši podatki so objavljeni na spletnih straneh SI-TSA.

3.3.2 Sinhronizacije ure

(1) SI-TSA zagotavlja točnost časa v skladu z določili iz razd. 1.1.

(2) Ura SI-TSA se na varen način uskladi s časom UTC s strežnikom za sinhronizacijo časa po protokolu NTP, ki uporablja referenčno uro GPS.

3.4. Upravljanje in izvedba operacij SI-TSA

Podrobna določila glede upravljanja in izvedbe operacij so v skladu z Uredbo v Interni politiki overitelja na CVI.

4. UPRAVLJANJE Z DOKUMENTACIJO

(1) Overitelj na CVI si pridržuje pravico do spremembe tega dokumenta brez predhodnega obveščanja uporabnikov in tretjih oseb, če spremembe ne vplivajo na način opravljanja storitev SI-TSA.

(2) Spremembe politike SI-TSA, ki bistveno vplivajo na način storitve SI-TSA, 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. Skladno z ZEPEP se prijava novosti storitev overitelja na CVI opravi tudi na pristojno ministrstvo za register overiteljev v Republiki Sloveniji.

5. TERMINOLOŠKI SLOVAR IN OZNAKE

Izraz	Pomen
Aplikacija	Računalniški program, s katerim upravlja organizacija, in ki za svoje delovanje potrebuje storitve izdajatelja varnih časovnih žigov
CP_{Name}	Ime politike delovanja overitelja oz. izdajatelja (angl. *Certification Policy Name*), povezano z mednarodno številko politike delovanja CP_{OID} (CP_{Name}, angl. *Certification Policy Object Identifier*)
CP_{OID}	Mednarodna številka, ki enolično določa politiko delovanja (CP_{OID}, angl. *Certification Policy Object IDentifier*).
CVI	Center Vlade Republike Slovenije za Informatiko, Langusova 4, 1000 Ljubljana, Slovenija (http://www.gov.si/cvi)
ETSI	Priporočila angl. *European Telecommunications Standards Institut.*. Politika SI-TSA je uskaljena s priporočili ETSI 102 023 (v.1.2.1) »Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities«
Infrastruktura overitelja	Infrastruktura overitelja na CVI so vsi prostori overitelja, njegova strojna in programska

na CVI	oprema ter varnostni mehanizmi, ki so potrebni za varno delovanje njegovih izdajateljev
Organizacija	Organizacija je bodisi institucija javne uprave, ki je v informacijsko-telekomunikacijskem omrežju državnih organov, bodisi pravna ali fizična oseba, ki je registrirana za opravljanje dejavnosti v skladu z veljavnimi predpisi v Republiki Sloveniji ali pa tuja oseba, ki opravlja dejavnost in lahko svojo istovetnost dokaže v skladu z veljavnimi predpisi. Naročnik storitev SI-TSA je odgovorna oseba t.j. fizična oseba, ki je pooblaščena za zastopanje organizacije v pravnem prometu.
Kvalificirano digitalno potrdilo	Je 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 o elektronskem poslovanju in elektronskem podpisu.
NTP	Protokol za sinhronizacijo časa, angl. *Network Time Protocol*, http://www.ntp.org
overitelj	Fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi. (CA, angl. *Certification Authority*)
SIGEN-CA	Izdajatelj potrdil za pravne in fizične osebe overitelja na Centru Vlade RS za informatiko (CVI). (SIGEN-CA, angl. *Slovenian General Certification Authority*) (prim. definicijo Overitelj)
SIGOV-CA	Izdajatelj potrdil za institucije javne uprave overitelja na Centru Vlade RS za informatiko (CVI). (SIGOV-CA, angl. *Slovenian Governmental Certification Authority*) (prim. definicijo Overitelj), http://www.sigov-ca.gov.si
SI-TSA	Izdajatelj varnih časovnih žigov overitelja na CVI. (SI-TSA, angl. *Slovenian Time stamping Authority*) (prim. definicijo Overitelj), http://www.si-tsa.si, http://www.si-tsa.gov.si
RFC 3161	RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP) (RFC, angl. *Request for Comments*)
TSA	Overitelj oz. izdajatelj časovnih žigov, angl. *Time-Stamping Autorithy*
UTC	Koordiniran univerzalni čas, angl. *Coordinated Universal Time,* mednarodni standard za meritve časa, veljaven od. l. 1972
Varen časovni žig	Varni časovni žig je elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času (2. člen ZEPEP). Varen časovni žig mora v skladu s 34. členom Uredbe vsebovati nedvoumne in pravilne podatke o datumu, točnemu času najmanj na sekundo natančno in overitelju, ki je varni časovni žig ustvaril. Varni časovni žig je lahko dokumentu dodan ali priložen in z njim povezan, vendar morajo biti pri tem vedno izpolnjene enake zahteve kot za varen elektronski podpis s kvalificiranim potrdilom
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 57/2000)