Državni center za storitve zaupanja
Izdajatelj varnih časovnih žigov SI-TSA

SI-TSA

POLITIKA SI-TSA

za izdajo varnih časovnih žigov

Javni del notranjih pravil Državnega centra za storitve zaupanja

veljavnost: od 7. novembra 2015
verzija: 5.0

CP_{Name}: SI-TSA-1
CP_{OID}: 1.3.6.1.4.1.6105.3.1.5

Izdaje politik delovanja SI-TSA	
verzija: 5.0, veljavnost: od 7. novembra 2015	
Politika SI-TSA za izdajo varnih časovnih žigov CP_{OID}: 1.3.6.1.4.1.6105.3.1.5 CP_{Name}: SI-TSA-1	*Spremembi z verzijo 5.0:* • *uporaba novega naziva za overitelja na Ministrstvu za notranje zadeve, po novem je to »Državni center za storitve zaupanja«,* • *novi kontaktni podatki izdajatelja SI-TSA.*
amandma k politiki verzije 4.0, veljavnost: od 21. marca 2014	
Amandma k Politiki SI-TSA za izdajo varnih časovnih žigov št. 2 / 4.0	*Sprememba z amandmajem št. 2 / 4.0:* • *uporaba novega naziva za overitelja na Ministrstvu za pravosodje in javno upravo, po novem je to »Overitelj na Ministrstvu za notranje zadeve«.*
amandma k politiki verzije 4.0, veljavnost: od 23. julija 2012	
Amandma k Politiki SI-TSA za izdajo varnih časovnih žigov št. 1 / 4.0	*Sprememba z amandmajem št. 1 / 4.0:* • *uporaba novega naziva za overitelja na Ministrstvu za javno upravo, po novem je to »Overitelj na Ministrstvu za pravosodje in javno upravo«;* • *spremeni se jamstvo za vrednost posameznega pravnega posla.*
verzija: 4.0, veljavnost: od 18. maja 2007	
Politika SI-TSA za izdajo varnih časovnih žigov CP_{OID}: 1.3.6.1.4.1.6105.3.1.4 CP_{Name}: SI-TSA-1	*Spremembi z verzijo 4.0:* • *pri identiteti izdajatelja SI-TSA niso več navedeni tisti podatki o digitalnih potrdilih strežnikov, ki se spreminjajo ob vsaki redni menjavi digitalnih potrdil;* • *imetniki posebnih digitalnih potrdil izdajatelja SIGOV-CA ne morejo več uporabljati storitev SI-TSA.*
verzija: 3.0, veljavnost: od 28. februarja 2006	
Politika SI-TSA za izdajo varnih časovnih žigov CP_{OID}: 1.3.6.1.4.1.6105.3.1.3 CP_{Name}: SI-TSA-1	*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«;* • *upoštevanje novega naziva za osebna kvalificirana digitalna potrdila, po novem so to »posebna kvalificirana digitalna potrdila«;* • *imetniki posebnih digitalnih potrdil poslovnih subjektov ne morejo več uporabljati storitev SI-TSA.*
verzija: 2.0, veljavnost: od 10. septembra 2004	
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	*Spremembi z verzijo 2.0:* • *uporaba storitev SI-TSA je razširjena tudi za potrebe aplikacij poslovnih subjektov;* • *imetnikom osebnih kvalificiranih digitalnih potrdil SIGEN-CA je omogočena uporaba storitev SI-TSA.*
Verzija: 1.0, veljavnost: od 10. novembra 2003	
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	/

VSEBINA

POVZETEK

Politike za kvalificirana digitalna potrdila in varne časovne žige predstavljajo celoten javni del notranjih pravil Državnega centra za storitve zaupanja, ki deluje v okviru Ministrstva za javno upravo (v nadaljevanju *overitelj na MJU oz. overitelj*) 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. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14) in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06), evropskimi direktivami ter drugimi veljavnimi predpisi in priporočili.

Izdajatelj varnih časovnih žigov SI-TSA (angl. *Slovenian Time Stamping Authority)*, http://www.si-tsa.si, deluje v okviru overitelja na Ministrstvu za javno upravo, http://www.ca.gov.si, in je registriran v skladu z veljavno zakonodajo.

Varni časovni žigi so namenjeni zagotavljanju obstoja dokumenta v določenem časovnem trenutku, povsod, kjer je potrebno na varen način dokazati časovne lastnosti transakcij in drugih storitev, za druge potrebe, kjer se potrebuje varni časovni žig. 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, ki enolično določa dokument. Izdajatelj temu povzetku dopiše čas in vse skupaj podpiše s svojim zasebnim ključem - to imenujemo 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 delovanje izdajatelja SI-TSA po politiki CP_{OID}: 1.3.6.1.4.1.6105.3.1.5 in nadomešča prejšnje verzije politik. Vse storitve in novo izdani varni časovni žigi izdajatelja SI-TSA se obravnavajo po novi politiki. Za varne časovne žige, izdane po prejšnjih politikah, velja, da se obravnavajo po novi politiki glede tistih določil, ki lahko smiselno nadomestijo oz. dopolnijo določila iz politike, po kateri je bil varen časovni žig izdan.

Nova politika vsebuje naslednji spremembi:
- *uporaba novega naziva za overitelja na Ministrstvu za notranje zadeve, po novem je to »Državni center za storitve zaupanja«,*
- *novi kontaktni podatki izdajatelja SI-TSA.*

Obvestila, navodila, politike in drugi pomembni dokumenti za uporabo storitev izdajatelja SI-TSA so objavljeni na spletnih straneh izdajatelja SI-TSA, http://www.si-tsa.si.

Politika je izdelana v skladu z mednarodnimi priporočili ETSI TS 102 023 (v.1.2.1) »Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities« in RFC 3628 "Policy requirements for Time-Stamping Authorities (TSAs)".

Ta stran je prazna.

1. UVOD

1.1. Pregled

(1) V okviru Ministrstva za javno upravo (v nadaljevanju *MJU*) deluje Državni center za storitve zaupanja (v nadaljevanju *overitelj na MJU oz. overitelj*).

(2) Politike overitelja kvalificiranih digitalnih potrdil in varnih časovnih žigov 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. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14) in Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06), 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 in
- za storitve oz. aplikacije, za katere se zahteva uporaba potrdil.

(5) Varni časovni žigi overitelja (v nadaljevanju *časovni žig*) na MJU so namenjeni:
- zagotavljanju obstoja dokumenta v določenem časovnem trenutku in sicer tako, da se datum in čas žigosanja poveže 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 varnih časovnih žigov SI-TSA (angl. *Slovenian Time Stamping Authority)*, http://www.si-tsa.si, deluje v okviru overitelja na Ministrstvu za javno upravo, http://www.ca.gov.si. Izdajatelj SI-TSA je registriran v skladu z veljavno zakonodajo.

(7) Javni del notranjih pravil overitelja na MJU je določen s politikami izdajateljev kvalificiranih digitalnih potrdil in varnih časovnih žigov.

(8) Pričujoča politika določa delovanje izdajatelja SI-TSA za izdajo varnih časovnih žigov za potrebe varnih storitev, s katerimi upravljajo državni in drugi organi, ki po veljavni zakonodaji veljajo za neposredne uporabnike državnega proračuna, in za potrebe varnih storitev v pristojnosti poslovnih subjektov, ki se lahko izkažejo z digitalnim potrdilom overitelja na MJU ali na drug varen način, ki ga določi izdajatelj SI-TSA.

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

1.2. Pomen izrazov[1]

1.2.1 Okrajšave

CA	Fizična ali pravna oseba, ki izdaja digitalna 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.*
DCF77	Dolgovalovni radijski oddajnik, ki stoji v Mainflingenu pri Frankfurtu in oddaja uradno časovno referenco 77.5 kHz.
ETSI	Mednarodna priporočila za področje telekomunikacij, angl. *European Telecommunications Standards Institut,* http://www.etsi.org.
GPS	Satelitski sistem za določanje položaja, angl. *Global Positioning System.*
MJU	Ministrstvo za javno upravo, Tržaška cesta 21, 1000 Ljubljana.
NTP	Protokol za sinhronizacijo časa, angl. *Network Time Protocol*, http://www.ntp.org.
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.
SI-TSA	Izdajatelj varnih časovnih žigov overitelja na MJU, angl. *Slovenian Time Stamping Authority.*
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.
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14).

1.2.2 Izrazi

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

Časovni žig	Varen časovni žig predstavlja elektronsko podpisano potrdilo izdajatelja, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času (2. člen ZEPEP). Varen časovni žig mora vsebovati podatke v skladu s 34. členom Uredbe (nedvoumne in pravilne podatke o datumu, točnemu času najmanj na sekundo natančno in overitelju oz. izdajatelju, 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 (primerjaj okrajšavo *ZEPEP* in izraz *Uredba*).
Digitalni podpis	Varen elektronski podpis, ki izpolnjuje zahteve 2. člena ZEPEP in 25. člena Uredbe.
Državni organ	Ministrstva, organi v sestavi ministrstev, vladne službe in upravne enote, Državni zbor,

[1] To podpoglavje v priporočilu ETSI TS 102 023 v1.2.1 ni predvideno.

	Državni svet, Ustavno sodišče, Računsko sodišče, Varuh človekovih pravic, pravosodni organi in druge osebe javnega prava, ki so neposredni uporabniki državnega proračuna v skladu z Zakonom o javnih financah (Uradni list RS, št. 11/11 – uradno prečiščeno besedilo, 14/13 – popr., 101/13 in 55/15 – ZFisP).
Izdajatelj	V okviru overitelja na MJU deluje več izdajateljev. Le-ti izdajajo bodisi kvalificirana digitalna potrdila bodisi varne časovne žige (primerjaj izraz *Overitelj na MJU*).
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 okrajšavo *ZEPEP* in izraz *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 definicijo *Potrdila*).

(2) Drugi izrazi pričujočega dokumenta so podani v spodnji tabeli.

Aplikacija	Računalniški program, s katerim upravlja organizacija in ki za svoje delovanje potrebuje storitve izdajatelja varnih časovnih žigov in ki se lahko izkaže z digitalnim potrdilom overitelja na MJU ali na drug varen način, ki ga določi izdajatelj SI-TSA.
Državni center za storitve zaupanja	Državni center za storitve zaupanja, ki deluje v okviru Ministrstva za javno upravo.
Imetniki potrdil	Zaposleni, ki so pooblaščeni za uporabo potrdila, za potrdila za splošne nazive, za strežnike, za podpis kode ali izdajatelja varnih časovnih žigov (angl. *subject*).
Infrastruktura overitelja na MJU	Vsi prostori overitelja, njegova strojna in programska oprema ter varnostni mehanizmi, ki so potrebni za varno delovanje njegovih izdajateljev.
Izdajatelj SIGOV-CA	Izdajatelj kvalificiranih digitalnih potrdil za državne organe overitelja na MJU, angl. *Slovenian Governmental Certification Authority*, http://www.sigov-ca.gov.si (primerjaj definicijo *Državni organ* in *Overitelj*).
Izdajatelj SI-TSA	Izdajatelj varnih časovnih žigov, ki deluje v okviru overitelja na MJU, angl. *Slovenian Time Stamping Authority,* http://www.si-tsa.si.
Organizacija	Bodisi državni organ, bodisi poslovni subjekt 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 (primerjaj definicijo *Državni organ*).
Overitelj na MJU	Glej izraz Državni center za storitve zaupanja.
Uporabnik	Bodisi aplikacija, s katero upravlja organizacija, bodisi imetnik posebnega potrdila SIGOV-CA.
Objava SI-TSA	Javna objava na spletnih straneh SI-TSA oz. na straneh overitelja na MJU, http://www.si-tsa.si in http://www.ca.gov.si.
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 MJU in jih objavi ali kako drugače posreduje uporabnikom varnih časovnih žigov, organizacijam ali tretjim osebam.
Posebno potrdilo *ali* Potrdilo	Posebno kvalificirano digitalno potrdilo v elektronski obliki (posebno potrdilo sestavlja potrdilo za overjanje podpisa in potrdilo za šifriranje), ki povezuje podatke iz potrdila z imetnikovima zasebnima ključema ter potrjuje imetnikovo identiteto (angl. *enterprise certificate*). Prejšnje poimenovanje za to potrdilo je »osebno kvalificirano digitalno potrdilo«.

Uredba	Uredba o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 – uradno prečiščeno besedilo, 61/06 – ZEPT in 46/14).

1.3. Razpoznavni podatki izdajatelja SI-TSA

1.3.1 Identiteta Državnega centra za storitve zaupanja

Naslov:	Državni center za storitve zaupanja Ministrstvo za javno upravo Tržaška cesta 21 1000 Ljubljana
Telefon:	01 4788 330
URL:	http://www.ca.gov.si
Oznaka:	State-institutions
Oznaka:	Republika Slovenija

1.3.2 Identiteta izdajatelja SI-TSA

(1) Oznaka pričujoče politike delovanja SI-TSA je: CP_{OID}: 1.3.6.1.4.1.6105.3.1.5.

(2) Kontaktni podatki SI-TSA so podani spodaj::

Naslov:	SI-TSA Državni center za storitve zaupanja Ministrstvo za javno upravo Tržaška cesta 21 1000 Ljubljana
E-pošta:	si-tsa@gov.si
Telefon:	01 4788 330
Enotni kontaktni center:	080 2002, 01 4788 590 ekc@gov.si
URL:	http://www.si-tsa.si

(3) Izdajatelj SIGOV-CA je izdal izdajatelju SI-TSA ustrezna digitalna potrdila za dva (2) strežnika izdajatelja v skladu z veljavno politiko SIGOV-CA. Podatki obeh potrdil so podani spodaj.

(4) Digitalno potrdilo prvega strežnika izdajatelja SI-TSA, t.j. potrdilo SI-TSA-1, vsebuje podatke po spodnji tabeli:

Naziv polja	Vrednost za potrdilo SI-TSA-1
Verzija, angl. *Version*	3 (*kar pomeni verzijo 3*)
Identifikacijska oznaka, angl. Serial Number	*enolična interna številka potrdila-celo število*
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	*pričetek veljavnosti po GMT*
Konec veljavnosti, angl. Validity: Not After	*konec veljavnosti po GMT*
Algoritem za javni ključ, angl. *Public Key Algorithm*	rsaEncryption
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritem RSA, angl. *RSA Public Key*	*ključ dolžine 2048 bitov*
Politika izdajatelja, angl. Certificate Policy	*PolicyIdentifier = Policy: določilo politike* *[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
Identiteta ključa (po alg. SHA-1): angl. Subject Key Identifier	*identifikator ključa*
Odtis potrdila (ni del potrdila)	
Odtis potrdila MD-5, angl. Certificate Fingerprint – MD5	*razpoznavni odtis potrdila po MD5*
Odtis potrdila SHA-1, angl. Certificate Fingerprint – SHA-1	*razpoznavni odtis potrdila po SHA-1*
Odtis potrdila SHA-256, angl. Certificate Fingerprint – SHA-256	*razpoznavni odtis potrdila po SHA-256*
Odtis potrdila base64 (v žigu)	*razpoznavni odtis potrdila v žigu*

Digitalno potrdilo drugega strežnika izdajatelja SI-TSA, t.j. potrdilo SI-TSA-2, je podan v tabeli spodaj:

Naziv polja	Vrednost za potrdilo SI-TSA-2
Verzija, angl. *Version*	3 (*kar pomeni verzijo 3*)
Identifikacijska oznaka, angl. Serial Number	*enolična interna številka potrdila-celo število*
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	*pričetek veljavnosti po GMT*
Konec veljavnosti, angl. Validity: Not After	*konec veljavnosti po GMT*

Algoritem za javni ključ, angl. *Public Key Algorithm*	rsaEncryption
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, šifriran z algoritem RSA, angl. *RSA Public Key*	*ključ dolžine 2048 bitov*
Politika izdajatelja, angl. Certificate Policy	*PolicyIdentifier = Policy: določilo politike* *[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
Identiteta ključa (po alg. SHA-1): angl. Subject Key Identifier	*identifikator ključa*
Odtis potrdila (ni del potrdila)	
Odtis potrdila MD-5, angl. Certificate Fingerprint – MD5	*razpoznavni odtis potrdila po MD5*
Odtis potrdila SHA-1, angl. Certificate Fingerprint – SHA-1	*razpoznavni odtis potrdila po SHA-1*
Odtis potrdila SHA-256, angl. Certificate Fingerprint – SHA-256	*razpoznavni odtis potrdila po SHA-256*
Odtis potrdila base64 (v žigu)	*razpoznavni odtis potrdila v žigu*

Polji, označeni kot kritični (angl. *critical*), sta sledeči:

- *namen uporabe* (angl. *Key Usage*),
- *razširjen namen uporabe* (angl. *Extended Key Usage)*.

1.4. Subjekti in namen uporabe

1.4.1 Državni center za storitve zaupanja in izdajatelj SI-TSA

(1) Državni center za storitve zaupanja izdaja kvalificirana digitalna potrdila in varne časovne žige, za katera velja najvišja stopnja varovanja ter deluje v skladu z veljavnimi predpisi.

(2) Izdajatelj varnih časovnih žigov SI-TSA (angl. *Slovenian Time Stamping Authority*) deluje v okviru Državnega centra za storitve zaupanja (http://www.ca.gov.si).

1.4.2 Uporabniki varnih časovnih žigov

(1) Uporabniki varnih časovnih žigov so aplikacije oz. organizacije, ki so skrbniki le-teh (glej podpogl. 1.2 za podroben opis organizacije).

(2) Medsebojna razmerja med organizacijo in SI-TSA ureja ta politika in morebiten medsebojni dogovor oz. pogodba o uporabi storitev časovnega žigosanja izdajatelja SI-TSA.

1.4.3 Tretje osebe

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

1.4.4 Namen uporabe

Storitve SI-TSA so namenjene:
- zagotavljanju obstoja dokumenta v določenem časovnem trenutku in sicer tako, da se datum in čas žigosanja poveže 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.

1.5. Skladnost z veljavno zakonodajo in drugimi predpisi

(1) Overitelj na MJU in izdajatelj SI-TSA delujeta v skladu z:
- ZEPEP,
- Uredbo,
- evropskimi direktivami,
- priporočili RFC za časovno žigosanje: RFC 3161 »Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)«,
- priporočili ETSI za časovne žige: ETSI TS 101 861 (v1.2.1) »Time stamping profile«,
- in drugimi veljavnimi predpisi.

(2) SI-TSA deluje v skladu s pričujočo politiko, katere identifikator CP_{OID} se dodeli vsakemu časovnemu žigu.

(3) 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« in RFC 3628 "Policy requirements for Time-Stamping Authorities (TSAs)".

2. OBVEZNOSTI IN ODGOVORNOST

2.1. Obveznost izdajatelja SI-TSA

2.1.1 Splošno

Izdajatelj SI-TSA oz. overitelj na MJU 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, obrazce, cenik, navodila za varno uporabo varnih časovnih žigov),
- izdajati časovne žige v skladu s to politiko in ostalimi predpisi ter priporočili.

2.1.2 Obveznost SI-TSA do uporabnikov

(1) Izdajatelj SI-TSA oz. overitelj na MJU je dolžan:

- zagotoviti pravilnost podatkov varnega časovnega žiga,
- 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 in tretje osebe o pomembnih zadevah ter
- izpolnjevati vse druge zahteve v skladu s to politiko.

(2) Izdajatelj SI-TSA oz. overitelj na MJU zagotavlja čim večjo dostopnost svojih storitev časovnega žigosanja, 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 časovnih žigov in
- nedostopnost storitve časovnega žigosanja kot posledica višje sile ali izrednih dogodkov.

(3) Ostale obveznosti izdajatelja SI-TSA oz. overitelja na MJU so določene z medsebojnim dogovorom ali pogodbo.

2.2. Obveznosti uporabnikov

Uporabniki morajo:
- dati izdajatelju točne in popolne podatke o identiteti oz drugih podatkov za izkaz istovetnosti,
- ob prejemu časovnega žiga preveriti le-tega v skladu z navodili izdajatelja SI-TSA,
- ob morebitnih napakah ali problemih takoj obvestiti izdajatelja SI-TSA,
- seznaniti se s to politiko in upoštevati vse določila glede njihove obveznosti, odgovornosti ter omejitve glede uporabe časovnega žiga,
- upoštevati tudi vsa druga priporočila SI-TSA glede zanesljive uporabe varnih časovnih žigov,
- redno spremljati vsa obvestila in objave SI-TSA in ravnati v skladu z le-temi,
- v skladu s priporočili izdajatelja skrbeti za arhiv elektronskih dokumentov ter potrebnih podatkov za preverjanje časovno žigosanih dokumentov,
- izpolnjevati vse druge zahteve v skladu s to politiko oz. pogodba ali dogovorom ter
- upoštevati morebitna druga pravila, ki so izven pristojnosti izdajatelja in so določena drugje.

2.3. Obveznosti tretjih oseb

Tretje osebe, ki se zanašajo na časovne žige SI-TSA, morajo:
- preveriti časovni žig v skladu z navodili izdajatelja SI-TSA,
- ob morebitnih napakah ali problemih takoj obvestiti izdajatelja SI-TSA,
- seznaniti se s to politiko in upoštevati vse določila glede njihove obveznosti, odgovornosti ter omejitve glede zaupanja in uporabe časovnega žiga,
- upoštevati tudi vsa druga priporočila SI-TSA glede zanesljive uporabe časovnih žigov,
- spremljati vsa obvestila in objave SI-TSA in ravnati v skladu z le-temi,
- upoštevati morebitna druga pravila, ki so izven pristojnosti izdajatelja in so določena drugje.

2.4. Odgovornost izdajatelja SI-TSA

(1) Izdajatelj SI-TSA oz. overitelj na MJU je odgovoren:
- da izdan časovni žig vsebuje vse predpisane podatke po tej politiki in drugih predpisih,
- za izvajanje vseh svojih obveznosti, navedenih zgoraj v podpogl. 2.1.

(2) Izdajatelj SI-TSA oz. overitelj na MJU ni odgovoren za neposredno ali posredno škodo, izgube ipd., ki bi nastala zaradi uporabe časovnih žigov izdajatelja SI-TSA, če:
- je bil časovni žig izdan kot rezultat napake, neverodostojnih podatkov ali drugih napak uporabnika ali katerekoli druge osebe javnega ali zasebnega prava,
- je bila storitev izdaje časovnega žiga zahtevana po objavi preklica digitalnih potrdil strežnikov SI-TSA ali izdajatelja SIGOV-CA,
- je bila povzročena zaradi izpada oz. nedostopnosti in nerazpoložljivosti infrastrukture, ki ni v domeni upravljanja overitelja na MJU, vključno z uporabnikovo programsko in strojno opremo,
- uporabnik ni upošteval določil pričujoče politike in medsebojnega dogovora oz. pogodbe in druga objavljena izdajateljeva priporočila glede namena in načina uporabe svojih storitev
- uporabnik ni upošteval drugih veljavnih predpisov.

(3) Glede finančne odgovornosti ima 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.

(4) Izdajatelj SI-TSA oz. overitelj na MJU jamči za varen časovni žig do višine 5.000 EUR.

2.5. Odgovornost uporabnikov

Uporabnik odgovarja za vsako škodo, ki izvira iz nespoštovanja določil te politike, navodil, obvestili SI-TSA ter druge veljavne zakonodaje.

2.6. Odgovornost tretjih oseb

Tretje osebe so odgovorne za izvajanje vseh obveznosti, določene s pričujočo politiko in navodili, obvestili SI-TSA ter druge veljavne zakonodaje.

2.7. Omejitve glede uporabe

(1) Omejitve uporabe, razen teh, ki so določene v tej politiki oziroma v medsebojnem dogovoru oz. pogodbi, ni.

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

2.8. Cenik

Cenik in način zaračunavanja časovnega žigosanja je objavljen na spletnih straneh izdajatelja SI-TSA,

http://www.si-tsa.si.

3. VARNOST DELOVANJA SI-TSA

(1) Oprema overitelja na MJU je postavljena v posebnih, ločenih prostorih v okviru infrastrukture overitelja, deloma pa tudi izven le-te. Zavarovana je z večnivojskim sistemom fizičnega in elektronskega varovanja. Varovanje infrastrukture overitelja na MJU se izvaja v skladu s priporočili stroke za najvišji nivo varovanja.

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

3.1. Postopki in izjava o politiki delovanja SI-TSA

3.1.1 Izjava o postopkih SI-TSA

Vsa določila tega razdelka[2] so, če ni podrobno podano v drugih razdelkih te politike, določena z Interno politiko overitelja na MJU.

3.1.2 Izjava o politiki SI-TSA

Vsa določila izjave o politiki delovanja SI-TSA[3] so, če ni podrobno podano v nadaljevanju tega razdelka, podana v drugih razdelkih te politike.

3.1.2.1 Način uporabe 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 MJU skladno z ZEPEP opravlja pristojna inšpekcijska služba.

(2) Overitelj na MJU javno objavi povzetek sklepov inšpekcijskega nadzora.

3.2. Upravljanje s ključi SI-TSA

3.2.1 Generiranje ključev SI-TSA

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

(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 nivo 3.

(3) Javni ključ izdajatelja SI-TSA je podpisal izdajatelj SIGOV-CA in mu izdal 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 MJU.

3.2.2 Zaščita zasebnega ključa SI-TSA

Zasebni ključ izdajatelja SI-TSA za podpisovanje časovnih žigov je varovan v varnih strojnih kriptografskih modulih, ki so v skladu z določili NIST FIPS 140-2 nivo 3.

3.2.3 Dostava digitalnega potrdila SI-TSA

(1) Javni ključ izdajatelja SI-TSA je objavljen in dostavljen v skladu s politiko SIGOV-CA, vedno v obliki digitalnega potrdila izdajatelja SI-TSA.

(2) Lastnosti in podatki o potrdilih oz. javnih ključih izdajatelja SI-TSA 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 MJU. 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 MJU.

3.3. Časovno žigosanje

3.3.1 Časovni žig

(1) SI-TSA zagotavlja, da so časovni žigi izdani na varen način s točnim časom s točnostjo ene (1) sekunde ali boljše.

(2) Oblika zahtevka za pridobitev časovnega žiga ter sam časovni žig mora biti v skladu s priporočilom RFC 3161 »Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)« ali shemo »Entrust XML« in v skladu z navodili izdajatelja SI-TSA, ki so objavljena na spletnih straneh izdajatelja SI-TSA.

(3) Profil časovnega žiga vsebuje štiri (4) sklope podatkov, podanih v tabeli spodaj, podrobnejši opis pa je podan na spletnih straneh izdajatelja SI-TSA:

Podatki o časovno žigosanih podatkih, angl. *SignedInfo*	*Kanonikalizacijska metoda*
	Algoritem za podpis (RSA, s katerim je šifriran povzetek, narejen z algoritmom SHA-1)
	Podatki o časovnem žigu: - *algoritem za povzetek (SHA-1)* - *povzetek*
	Podatki o izdajatelju SI-TSA - *algoritem za povzetek (SHA-1)* - *povzetek, ki enolično označuje izdajatelja SI-TSA*
Podpis, angl. *SignatureValue*	*Podpis*
Digitalno potrdilo SI-TSA angl. *KeyInfo of TimeStampAuthority*	*Odtis potrdila po base64*
Podatki o časovnem žigu, angl. *TimeStampInfo*	*Oznaka politike, pod katero je časovni žig izdan*
	Povzetek sporočila, ki se časovno žigosa
	Serijska številka, ki je enolična za vsak časovni žig, ki ga je izdal SI-TSA
	Čas, ko je bil časovni žig izdan in sicer kot univerzalni čas[4]
	Naključno generirano število, ki je vključeno v časovni žig opcijsko, ko uporabnik to zahteva
	Drugi neobvezni podatki

3.3.2 Sinhronizacije ure

(1) Ura strežnikov SI-TSA se na varen način uskladi s časom UTC s strežnikom za sinhronizacijo časa po

[4] Univerzalni čas, angl. *Universal Time*, kar označuje "Z" na koncu podatka, npr.: 2004-02-16T07:06:11.703Z. Univerzalni čas je v zimskem času eno(1) uro, v letnem času pa dve (2) uri za našim.

protokolu NTP, ki uporablja referenčno uro GPS ali DCF77 ali referenčni oscilator.

(2) Usklajenost ure strežnikov SI-TSA z referenčnim časom se stalno preverja in v primerih morebitnih odstopanj SI-TSA ustrezno ukrepa.

3.4. Upravljanje in organizacija

3.4.1 Varovanje infrastrukture

(1) Varovanje infrastrukture izdajatelja SI-TSA se izvaja v skladu s priporočili stroke za najvišji nivo varovanja.

(2) Celotna infrastrukture overitelja na MJU je varovana z večnivojskim sistemom fizičnega in elektronskega varovanja.

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

3.4.2 Dostop do infrastrukture izdajatelja SI-TSA

(1) Dostop do infrastrukture overitelja na MJU oz. izdajatelja je omogočen samo pooblaščenim osebam overitelja na MJU skladno z njihovimi nalogami in pooblastili, določenimi v Interni politiki overitelja na MJU.

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

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

3.4.3 Nadzor nad osebjem

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

3.4.3.1 Potrebne kvalifikacije in izkušnje osebja

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

3.4.3.2 Primernost osebja

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

3.4.3.3 Dodatno izobraževanje osebja

Osebju izdajatelja SI-TSA se zagotavlja vsa potrebna izobraževanja.

3.4.3.4 Zahteve za redna usposabljanja

Osebje overitelja na MJU se usposablja glede na potrebe oz. novosti v zvezi z delovanjem izdajatelja SI-TSA.

3.4.3.5 Menjava nalog

Ni predpisana.

3.4.3.6 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.

3.4.3.7 Zahteve za zunanje izvajalce

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

3.4.3.8 Dostop osebja do dokumentacije

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

3.4.4 Fizično varovanje

3.4.4.1 Lokacija in zgradba overitelja na MJU

(1) Oprema overitelja na MJU je postavljena v posebnih, varovanih, ločenih prostorih v okviru infrastrukture Ministrstva za javno upravo.

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

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

3.4.4.2 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.

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

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

3.4.4.3 Napajanje in prezračevanje

Infrastruktura overitelja na MJU ima zagotovljeno neprekinjeno napajanje in ustrezne klimatske sisteme, podrobno o tem v Interni politiki overitelja na MJU.

3.4.4.4 Zaščita pred poplavo

Infrastruktura overitelja na MJU ni izpostavljena nevarnosti poplav, razen v primeru višje sile, podrobno o tem v Interni politiki overitelja na MJU.

3.4.4.5 Zaščita pred požari

Prostori overitelja na MJU so varovani pred morebitnim izbruhom požara, podrobno o tem v Interni politiki overitelja na MJU.

3.4.4.6 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.

3.4.4.7 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.

3.4.4.8 Hramba na oddaljeni lokaciji

Glej razd. 3.4.4.1.

3.4.5 Upravljanje infrastrukture

Podrobnosti upravljanja infrastrukture so v skladu z Uredbo določene v Interni politiki overitelja na MJU.

3.4.6 Upravljanje dostopov do infrastrukture

Glej razd. 3.4.2.

3.4.7 Vzpostavitev in vzdrževanje infrastrukture

(1) Izdajatelj SI-TSA izvaja svoje storitve na zaupanja vredni infrastrukture, ki je certificirana v skladu z najvišjimi zahtevami za varovanje.

(2) Podrobnosti o tem so skladno z Uredbo opisane v Interni politiki overitelja na MJU.

3.4.8 Ogrožanje varnosti infrastrukture

V primeru ogrožanja varnosti infrastrukture overitelja na MJU glede izdaje časovnih žigov bo izdajatelj SI-TSA

ukrepal, kot je to določeno v Interni politiki overitelja na MJU.

3.4.9 Prenehanje delovanja SI-TSA

Če bo overitelj na MJU prenehal z opravljanjem svoje dejavnosti ali izdajatelj SI-TSA prenehal z izdajanjem časovnih žigov, bo overitelj na MJU ukrepal v skladu z ZEPEP.

3.4.10 Skladnost z veljavno zakonodajo

Glej podpogl. 1.5.

3.4.11 Varnostni dnevniki

(1) Izdajatelj SI-TSA 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.

3.5. Upravljanje z dokumentacijo[5]

(1) Overitelj na MJU si pridržuje pravico do spremembe tega dokumenta brez predhodnega obveščanja uporabnikov, v kolikor spremembe ne vplivajo na namen uporabe in postopkov 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 oz. izdajatelja SI-TSA pod novo identifikacijsko številko (CP_{OID}) in označenim datumom začetka njene veljavnosti. V tem času lahko uporabniki na elektronski naslov izdajatelja SI-TSA podajo svoje pripombe, ki jih obravnavajo pooblaščene osebe overitelja na MJU.

(3) Overitelj lahko izda tudi amandmaje k politiki.

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

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

[5] To podpoglavje ni v skladu s priporočilom ETSI TS 102 023 v1.2.1.