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

SI-TRUST
SI-TSA

POLITIKA SI-TSA

za izdajo kvalificiranih časovnih žigov

Javni del notranjih pravil Državnega centra za storitve zaupanja

veljavnost: od 23. avgusta 2018
verzija: 7.0

CP_{Name}: SI-TSA-1
CP_{OID}: 1.3.6.1.4.1.6105.3.1.7

Zgodovina politik

Izdaje politik delovanja SI-TSA	
verzija: 7.0, veljavnost: od 23. avgusta 2018	
Politika SI-TSA za izdajo kvalificiranih časovnih žigov CP_{OID}: 1.3.6.1.4.1.6105.3.1.7 CP_{Name}: SI-TSA-1	*Spremembe z verzijo 7.0:* • *spremenijo se podatki o potrdilih SI-TSA-1 in SI-TSA2,* • *algoritem za povzetek SHA-1 se nadomesti z algoritmom SHA-256,* • *spremenijo se podatki o strežniku za sinhronizacijo časa.*
verzija: 6.0, veljavnost: od 28. maja 2018	
Politika SI-TSA za izdajo kvalificiranih časovnih žigov CP_{OID}: 1.3.6.1.4.1.6105.3.1.6 CP_{Name}: SI-TSA-1	*Spremembe z verzijo 6.0:* • *izraz »varni časovni žig« se nadomesti z izrazom »kvalificirani časovni žig«,* • *uvedena je Krovna politika SI-TRUST za izdajatelje, ki delujejo v okviru ponudnika storitev zaupanja SI-TRUST, zato se pričujoča politika v določenih točkah sklicuje nanjo,* • *izrazi in okrajšave so usklajeni z veljavno zakonodajo.*
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 digitalna potrdila in elektronske časovne žige predstavljajo celoten javni del notranjih pravil Državnega centra za storitve zaupanja, ki deluje v okviru Ministrstva za javno upravo (v nadaljevanju *SI-TRUST*) in določajo namen, delovanje in metodologijo upravljanja s kvalificiranimi in normaliziranimi digitalnimi potrdili, dodeljevanje kvalificiranih elektronskih časovnih žigov, odgovornost SI-TRUST ter zahteve, ki jih morajo izpolnjevati uporabniki in tretje osebe, ki uporabljajo in se zanašajo na kvalificirana digitalna potrdila in na kvalificirane elektronske časovne žige, in drugi ponudniki storitev zaupanja, ki želijo uporabljati storitve SI-TRUST.

SI-TRUST izdaja kvalificirana digitalna potrdila ter kvalificirane elektronske časovne žige, za katera velja najvišja stopnja varovanja ter deluje v skladu z Uredbo (EU) št. 910/2014 Evropskega parlamenta in Sveta o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in razveljavitvi Direktive 1999/93/ES (eIDAS; Uradni list EU, št. L 257/73), standardi ETSI ter drugimi veljavnimi predpisi in priporočili.

SI-TRUST izdaja tudi normalizirana digitalna potrdila ter digitalna potrdila za posebne namene oz. zaprte sisteme. Pravila delovanja izdajateljev takih potrdil se določijo s politiko delovanja takega izdajatelja.

Normalizirana digitalna potrdila, ki jih izdaja SI-TRUST, so namenjena:
- izdajateljem potrdil, izdajateljem časovnih žigov, sistemom OCSP, informacijskim sistemom, podpisovanju programske kode in registra preklicanih potrdil ter v ostalih primerih, kjer ni možna uporaba kvalificiranih potrdil,
- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba teh potrdil in
- za storitve oz. aplikacije, za katere se zahteva uporaba teh potrdil.

Kvalificirana digitalna potrdila, ki jih izdaja SI-TRUST, so namenjena:
- ustvarjanju elektronskih podpisov in elektronskih žig ter avtentikaciji spletišč,
- za upravljanje, dostop in izmenjavo podatkov, kjer se predvideva uporaba teh potrdil,
- za varno elektronsko komuniciranje med imetniki potrdil in
- za storitve oz. aplikacije, za katere se zahteva uporaba teh potrdil.

Kvalificirani elektronski časovni žigi SI-TRUST so namenjeni:
- zagotavljanju obstoja dokumenta v določenem časovnem trenutku in sicer tako, da se poveže datum in čas žigosanja z vsebino dokumenta na kriptografsko varen način,
- povsod, kjer je potrebno na varen način dokazati časovne lastnosti transakcij in drugih storitev,
- za druge potrebe, kjer se potrebuje kvalificirani elektronski časovni žig.

Znotraj SI-TRUST deluje izdajatelj kvalificiranih časovnih žigov SI-TSA (angl. *Slovenian Time Stamping Authority)*, http://www.si-tsa.si, ki izdaja kvalificirane časovne za državne organe in poslovne subjekte.

Izdajatelj SI-TSA je registriran v skladu z veljavno zakonodajo.

Politika delovanja SI-TSA določa notranja pravila delovanja izdajatelja, ki definirajo namen, delovanje in metodologijo izdajanja časovnih žigov, odgovornosti in zahteve, ki jih morajo izpolnjevati vsi subjekti.

Pričujoči dokument določa delovanje izdajatelja SI-TSA po politiki CP_{OID}: 1.3.6.1.4.1.6105.3.1.7 in nadomešča prejšnje verzije politik. Vse storitve in novo izdani kvalificirani časovni žigi izdajatelja SI-TSA se obravnavajo po novi politiki. Za kvalificirane 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 kvalificiran časovni žig izdan.

Spremembe pričujočega dokumenta so sledeče:

- spremenijo se podatki o potrdilih SI-TSA-1 in SI-TSA2,
- algoritem za povzetek SHA-1 se nadomesti z algoritmom SHA-256,
- spremenijo se podatki o strežniku za sinhronizacijo časa.

Kvalificirani 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 kvalificirani 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. 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.

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.

1. UVOD

1.1. Pregled

(1) Skupne določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 1.1).

(2) Znotraj SI-TRUST deluje izdajatelj kvalificiranih časovnih žigov SI-TSA (angl. *Slovenian Time Stamping Authority)*, http://www.si-tsa.si, ki izdaja kvalificirane časovne za državne organe in poslovne subjekte.

(3) Izdajatelj SI-TSA je registriran v skladu z veljavno zakonodajo.

(4) Po pričujoči politiki CP_{OID}:1.3.6.1.4.1.6105.3.1.6 SI-TSA izdaja kvalificirane elektronske časovne žige 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 SI-TRUST ali na drug varen način, ki ga določi izdajatelj SI-TSA. Izdajatelj SI-TSA vsakemu izdanemu časovnemu žigu dodeli identifikator CPOID pričujoče politike.

(5) Pričujoča politika je pripravljena skladno 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)" ter določa notranja pravila delovanja izdajatelja, ki definirajo namen, delovanje in metodologijo izdajanje časovnih žigov, odgovornosti in zahteve, ki jih morajo izpolnjevati vsi subjekti.

(6) Medsebojna razmerja se lahko izvajajo tudi na podlagi pisnega dogovora med organizacijami in SI-TRUST, ali med tretjimi osebami, ki se zanašajo na potrdila izdajatelja SIGOV-CA in SI-TRUST.

(7) SI-TRUST se preko korenskega izdajatelja SI-TRUST Root lahko povezuje z drugimi ponudniki storitev zaupanja, kar se ureja z medsebojnim dogovorom oz. pogodbo.

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

1.2. Izrazi in okrajšave[1]

1.2.1 Izrazi

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 1.6.1).

1.2.2 Okrajšave

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 1.6.2).

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

1.3. Razpoznavni podatki izdajatelja časovnih žigov

1.3.1 Ponudnik storitev zaupanja

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 1.3.1).

1.3.2 Izdajatelj časovnih žigov

(1) Oznaka pričujoče politike delovanja SI-TSA je: CP_{OID}: 1.3.6.1.4.1.6105.3.1.6.

(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*	sha256WithRSAEncryption
Izdajatelj potrdila, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGOV-CA
Imetnik potrdila, angl. *Subject*	c=SI, o=state authorities, ou=TSA-certificates, cn=SI-TSA-1, serialnumber=1234773726021
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*	sha256WithRSAEncryption
Izdajatelj potrdila, angl. *Issuer*	c=SI, o=Republika Slovenija, oi=VATSI-17659957, cn=SIGOV-CA
Imetnik potrdila, angl. *Subject*	c=SI, o=state authorities, ou=TSA-certificates, cn=SI-TSA-2, serialnumber=1234773826026
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 Ponudnik storitev zaupanja in izdajatelj časovnih žigov

(1) SI-TRUST deluje v skladu z veljavnimi predpisi ter izdaja kvalificirana digitalna potrdila in kvalificirane časovne žige, za katera velja najvišja stopnja varovanja.

(2) Izdajatelj kvalificiranih časovnih žigov SI-TSA (angl. Slovenian Time Stamping Authority) deluje v okviru SI-TRUST (http://www.si-trust.gov.si).

1.4.2 Uporabniki kvalificiranih časovnih žigov

(1) Uporabniki kvalificiranih časovnih žigov so aplikacije oz. organizacije, ki so skrbniki le-teh. Izdajatelj SI-TSA izdaja kvalificirane časovne žige za državne organe in poslovne subjekte.

(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 kvalificirani časovni žig.

1.5. Skladnost z veljavno zakonodajo in drugimi predpisi

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 9.14 in 9.15).

2. OBVEZNOSTI IN ODGOVORNOSTI

2.1. Obveznosti izdajatelja časovnih žigov

2.1.1 Splošno

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 9.6.1).

2.1.2 Obveznosti do uporabnikov

(1) Izdajatelj SI-TSA oz. SI-TRUST je dolžan:
- izdajati časovne žige v skladu s to politiko in ostalimi predpisi ter priporočili,
- zagotoviti pravilnost podatkov kvalificiranega časovnega žiga.

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 kvalificiranih časovnih žigov,
- redno spremljati vsa obvestila in objave SI-TSA in ravnati v skladu z njimi,
- v skladu s priporočili izdajatelja skrbeti za arhiv elektronskih dokumentov ter potrebnih podatkov za preverjanje časovno žigosanih dokumentov,
- ravnati v skladu s to politiko in določili iz morebitne pogodbe oz. dogovora in ostalimi veljavnimi predpisi 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 časovnih žigov

(1) Izdajatelj SI-TSA oz. SI-TRUST 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. SI-TRUST 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 SI-TRUST, 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) Ministrstvo za javno upravo ima glede delovanja SI-TRUST ustrezno zavarovano svojo odgovornost v skladu z veljavno zakonodajo.

(4) Izdajatelj SI-TSA oz. SI-TRUST jamči za vrednost posameznega pravnega posla, opremljenega s kvalificiranim časovnim žigom, 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

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 9.6.4).

2.7. Omejitve glede uporabe

(1) Omejitev 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 IZDAJATELJA ČASOVNIH ŽIGOV

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.1).

3.1. Postopki in izjava o politiki delovanja izdajatelja časovnih žigov

3.1.1 Izjava o postopkih izdajatelja časovnih žigov

Vsa določila tega razdelka[2] so, če ni podrobno podano v drugih razdelkih te politike, določena z Interno politiko SI-TRUST.

3.1.2 Izjava o politiki izdajatelja časovnih žigov

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 kvalificiranih časovnih žigov

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

3.1.2.2 Postopek v primeru sporov

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 9.13).

3.1.2.3 Inšpekcijski nadzor

Določbe so opredeljene v Krovni politiki SI-TRUST (celotno pogl. 8.).

3.2. Upravljanje s ključi izdajatelja časovnih žigov

3.2.1 Generiranje ključev izdajatelja časovnih žigov

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

(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 veljavno zakonodajo v Interni politiki SI-TRUST.

3.2.2 Zaščita zasebnega ključa izdajatelja časovnih žigov

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 6.2.1).

3.2.3 Dostava digitalnega potrdila izdajatelja časovnih žigov

(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 na spletnih straneh SI-TSA.

3.2.4 Obnova javnega ključa izdajatelja časovnih žigov

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

3.2.5 Konec veljavnosti ključev izdajatelja časovnih žigov

(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 SI-TRUST. 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 veljavno zakonodajo v Interni politiki SI-TRUST.

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 morata biti v skladu s priporočilom RFC 3161 »Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP)«, standardoma ETSI EN 319 421 in ETSI EN 319 422 ter navodili izdajatelja SI-TSA, ki so objavljena na spletnih straneh izdajatelja SI-TSA.

(3) Izdajatelj SI-TSA dodatno podpira možnost časovnega žigosanja z uporabo transportnega protokola, določenega s priporočilom RFC 3161 v poglavju »3.4. Time-Stamp Protocol via HTTP«, pri čemer sta sporočili za zahtevek in odgovor za časovno žigosanje v formatu XML v skladu s shemo »Entrust XML«, ki je objavljena na spletnih straneh izdajatelja SI-TSA.

(4) 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-256)
	Podatki o časovnem žigu: - *algoritem za povzetek (SHA-256)* - *povzetek*
	Podatki o izdajatelju SI-TSA - *algoritem za povzetek (SHA-256)* - *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

[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 srednjeevropskim časom.

3.3.2 Sinhronizacije ure

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

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

3.4. Upravljanje in organizacija

3.4.1 Varovanje infrastrukture

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.1).

3.4.2 Dostop do infrastrukture izdajatelja časovnih žigov

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.1.2).

3.4.3 Organizacijska struktura izdajatelja časovnih žigov

3.4.3.1 Organizacija ponudnika storitev zaupanja in zaupanja vredne vloge

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.2.1).

3.4.3.2 Število oseb za posamezne vloge

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.2.2).

3.4.3.3 Izkazovanje istovetnosti za opravljanje posameznih vlog

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.2.3).

3.4.3.4 Nezdružljivost vlog

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.2.4).

3.4.4 Nadzor nad osebjem

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.3).

3.4.4.1 Potrebne kvalifikacije in izkušnje osebja ter njegova primernost

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.3.1).

3.4.4.2 Preverjanje primernosti osebja

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.3.2).

3.4.4.3 Izobraževanje osebja

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.3.3).

3.4.4.4 Zahteve za redna usposabljanja

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.3.4).

3.4.4.5 Menjava nalog

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.3.5).

3.4.4.6 Sankcije

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.3.6).

3.4.4.7 Zahteve za zunanje izvajalce

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.3.7).

3.4.4.8 Dostop osebja do dokumentacije

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.3.8).

3.4.5 Fizično varovanje

3.4.5.1 Lokacija in zgradba ponudnika storitev zaupanja

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.1.1).

3.4.5.2 Fizični dostop do infrastrukture ponudnika storitev zaupanja

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.1.2).

3.4.5.3 Napajanje in prezračevanje

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.1.3).

3.4.5.4 Zaščita pred poplavo

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.1.4).

3.4.5.5 Zaščita pred požari

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.1.5).

3.4.5.6 Hramba nosilcev podatkov

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.1.6).

3.4.5.7 Odstranjevanje odpadkov

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.1.7).

3.4.5.8 Hramba na oddaljeni lokaciji

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.1.8).

3.4.6 Upravljanje infrastrukture

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.1).

3.4.7 Upravljanje dostopov do infrastrukture

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.1.2).

3.4.8 Vzpostavitev in vzdrževanje infrastrukture

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.1.1).

3.4.9 Ogrožanje varnosti infrastrukture

Določbe so opredeljene v Krovni politiki SI-TRUST (celotno podpogl. 5.7).

3.4.10 Prenehanje delovanja izdajatelja časovnih žigov

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 5.8).

3.4.11 Skladnost z veljavno zakonodajo

Določbe so opredeljene v Krovni politiki SI-TRUST (podpogl. 9.15).

3.4.12 Varnostni pregledi sistema

Določbe so opredeljene v Krovni politiki SI-TRUST (celotno podpogl. 5.4).

3.5. Upravljanje s politiko[5]

Določbe so opredeljene v Krovni politiki SI-TRUST (celotni podpogl. 1.5 in 9.12).

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