Overitelj na Ministrstvu za javno upravo SI-TSA

AMANDMA k POLITIKI SI-TSA

za izdajo varnih časovnih žigov

Javni del notranjih pravil overitelja na Ministrstvu za javno upravo

veljavnost: od 27. septembra 2006
št.: 1 / 3.0

Podatki o politiki:

CP_{Name}: SI-TSA-1
CP_{OID}: 1.3.6.1.4.1.6105.3.1.3
veljavnost: od 28. februarja 2006
verzija: 3.0

Izdaje politik delovanja SI-TSA	
amandma k politiki verzije 3.0, veljavnost: od 27. septembra 2006	
Amandma k Politiki SI-TSA za izdajo varnih časovnih žigov št. 1 / 3.0	*Sprememba z amandmajem št. 1 / 3.0:* • *sprememba podatkov o digitalnih potrdilih izdajatelja varnih časovnih žigov SI-TSA (SI-TSA-1 in SI-TSA-2)*
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	/

1. UVOD

(1) Amandma št. 1 / 3.0 k politiki delovanja izdajatelja SI-TSA dopolnjuje obstoječo verzijo Politike SI-TSA za izdajo varnih časovnih žigov (CP_{OID}: 1.3.6.1.4.1.6105.3.1.3). Vse storitve in novo izdani varni časovni žigi izdajatelja SI-TSA se obravnavajo po politiki, dopolnjeni s tem amandmajem.

(2) Amandma k obstoječi politiki določa podatke o novoizdanih digitalnih potrdilih izdajatelja varnih časovnih žigov SI-TSA (SI-TSA-1 in SI-TSA-2). Menjava digitalnih potrdil izdajatelja je potrebna zaradi poteka veljavnosti zasebnega ključa za podpisovanje zahtevkov za varno časovno žigosanje in ne vpliva na veljavnost pred tem izdanih varnih časovnih žigov.

(3) 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.

2. PODATKI O DIGITALNIH POTRDILIH IZDAJATELJA VARNIH ČASOVNIH ŽIGOV SI-TSA

V Politiki SI-TSA za izdajo varnih časovnih žigov (CP_{OID}: 1.3.6.1.4.1.6105.3.1.3) se v razdelku 1.3.2 »Identiteta izdajatelja SI-TSA« 4. člen nadomesti z naslednjimi podatki:

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*	979184814
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*	27 Sep 2006 07:43:51 GMT
Konec veljavnosti, angl. *Validity: Not After*	27 Sep 2011 08:13:51 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: 1.3.6.1.4.1.6105.1.5.2 [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. SHA1): angl. *Subject Key Identifier*	43BB884C177BB5EDD06DB0011B1A406F91ED20A8
Odtis potrdila	
Odtis potrdila MD-5, angl. *Certificate Fingerprint – MD5*	8b6edc2c5b4ca558fc7bc6fb66699a2a
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA1*	df428e102636edddebc751f0c191f31219f1ea0e
Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA256*	88d962795f0fba28001471db1380734a1769706e9b98dce2089a57c754be228e
Odtis potrdila *base64 (v žigu)*	dBoyH9yC5AMtQlCSyGMXD4Y+6cU=

Digitalno potrdilo drugega strežnika izdajatelja SI-TSA, t.j. potrdilo SI-TSA-2, vsebuje podatke po spodnji tabeli:

Naziv polja	Vrednost za potrdilo SI-TSA-2
Verzija, angl. *Version*	3 (*kar pomeni verzijo 3*)
Identifikacijska oznaka, angl. *Serial Number*	979184821
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*	27 Sep 2006 09:32:07 GMT
Konec veljavnosti angl. *Validity: Not After*	27 Sep 2011 10:02:07 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: 1.3.6.1.4.1.6105.1.5.2 [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. SHA1): angl. *Subject Key Identifier*	F791CE3D31299335221450915125732700555ADF
Odtis potrdila	
Odtis potrdila MD5, angl. *Certificate Fingerprint – MD5*	b48e5399685e369ef061b9b2885a4444
Odtis potrdila SHA-1, angl. *Certificate Fingerprint – SHA*1	f2cfb634bb1947e2d21fdb638c6fede692469ed7
Odtis potrdila SHA-256, angl. *Certificate Fingerprint – SHA*256	90d20a0e9937f3f1729a6e4f52b3833ee0b1d65229cea8cb070c0b612ed23c05
Odtis potrdila *base64 (v žigu)*	xra7Cw7ROemA7yb1r6HBPoCOmjM=

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

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