Pravila delovanja izdajatelja varnih časovnih žigov SIMoD-TSA-Restricted, javni del

(Javna pravila SIMoD-TSA-Restricted)

Verzija 1.0

Izdaja	
Pravila delovanja izdajatelja varnih časovnih žigov SIMoD-TSA-Restricted, javni del, verzija 1.0	

KAZALO

Na podlagi 102. člena Zakona o obrambi (Uradni list RS, št. 103/04 – uradno prečiščeno besedilo) v zvezi z 28. in 29. členom Uredbe o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06) ter v skladu z 9. odstavkom poglavja 1.1. Pregled Pravil delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije, Verzija 2.0, št. 382-5/2006-109 z dne 24.08.2010 izdajam

PRAVILA DELOVANJA IZDAJATELJA VARNIH ČASOVNIH ŽIGOV SIMOD-TSA-Restricted, JAVNI DEL

(JAVNA PRAVILA SIMOD-TSA-Restricted)

Verzija 1.0

1. PREGLED

Ministrstvo za obrambo Republike Slovenije (v nadaljnjem besedilu: MO) upravlja z infrastrukturo javnih ključev (ang. **S**lovenian **M**inistry **o**f **D**efence **P**ublic **K**ey **I**nfrastructure - SIMoD-PKI) za potrebe obrambe države.

V okviru SIMoD-PKI deluje korenski overitelj digitalnih potrdil SIMoD-CA-Root, podrejeni overitelji digitalnih potrdil in izdajatelji varnih časovnih žigov.

Izdajatelj varnih časovnih žigov SIMoD-TSA-Restricted (ang. **S**lovenian **M**inistry **o**f **D**efence **T**ime **S**tamping **A**uthority **Restricted**) nudi storitve časovnega žigosanja v internem omrežju MO, v katerem se obravnavajo podatki do vključno stopnje tajnosti INTERNO.

Izdajatelj varnih časovnih žigov SIMoD-TSA-Restricted (v nadaljevanju: izdajatelj SIMoD-TSA-Restricted) uporablja za izdajanje varnih časovnih žigov digitalna potrdila za izdajatelje časovnih žigov overitelja SIMoD-CA-Restricted.

Izdajatelj SIMoD-TSA-Restricted izdaja varne časovne žige, za katere veljajo določbe 2. člena [7] ZEPEP in v skladu s 25. členom [7] ZEPEP izpolnjuje določbe za varen časovni žig in storitve, povezane z njim.

Varni časovni žigi izdajatelja SIMoD-TSA-Restricted ustrezajo določilom [2] ETSI TS 101 861 in [13] RFC 3161.

Izdajatelj SIMoD-TSA-Restricted izdaja varne časovne žige za potrebe uporabnikov in aplikacij, kjer je potrebno dokazati časovne lastnosti transakcij in drugih storitev. Storitve varnega časovnega žigosanja se uporablja pri hranjenju in prenosu podatkov z ali brez stopnje tajnosti; za varno časovno žigosanje datotek, sporočil in elektronskih form.

Pravila delovanja izdajatelja varnih časovnih žigov SIMoD-TSA-Restricted (v nadaljevanju Pravila SIMoD-TSA-Restricted) opisujejo tehnične lastnosti, nivo varnosti in postopke za upravljanje infrastrukture ter opravljanje storitev izdajatelja SIMoD-TSA-Restricted ter določajo obveznosti in odgovornosti izdajatelja, uporabnikov in tretjih oseb, ki se zanašajo na varen časovni žig.

Pravila SIMoD-TSA-Restricted, javni del (v nadaljevanju Javna pravila SIMoD-TSA-Restricted) predstavljajo celoten javni del notranjih pravil izdajatelja SIMoD-TSA-Restricted.

Oblika in vsebina Javnih pravil SIMoD-TSA-Restricted je usklajena z [1] ETSI TS 102 023.

Zainteresirane strani, ki potrebujejo informacije za oceno zaupanja v SIMoD-PKI kot celoto, v overitelja SIMoD-CA-Restricted in v digitalna potrdila izdajatelja SIMoD-TSA-Restricted, morajo poleg tega dokumenta upoštevati še določila [5] Politika SIMoD-PKI in [6] Pravila SIMoD-CA-Restricted.

2. REFERENCE

[1]	ETSI TS 102 023	Policy requirements for time-stamping authorities
[2]	ETSI TS 101 861	Time-stamping Profile
[3]	RFC 3628	Policy Requirements for Time-Stamping Authorities
[4]	FIPS 140-2	Federal Information Processing Standards 140-2; Security Requirements for Cryptographic Modules
[5]	Politika SIMoD-PKI	Pravila delovanja infrastrukture javnih ključev na Ministrstvu za obrambo Republike Slovenije
[6]	Pravila SIMoD-CA-Restricted	Pravila delovanja overitelja SIMoD-CA-Restricted
[7]	ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 98/04 – UPB1, 61/06)
[8]	ZObr	Zakon o obrambi (Uradni list RS, št. 103/04 – UPB1)
[9]	ZTP	Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – UPB2, 9/10)
[10]		Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01 in 86/06)
[11]	ITU-R Recommendation TF.460-5	Time scale notations
[12]	RFC 1305	Network Time Protocol
[13]	RFC 3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

3. POJMI IN KRATICE

3.1. Pojmi

Izraz	Definicija
Časovni žig	Je elektronsko podpisano potrdilo izdajatelja časovnih žigov, ki potrjuje obstoj in celovitost podatkov v elektronski obliki v določenem časovnem trenutku.
Digitalno potrdilo	Je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z imetnikom potrdila ter potrjuje njeno identiteto.
Digitalno potrdilo izdajatelja časovnih žigov	Je digitalno potrdilo, s katerim izdajatelj časovnih žigov elektronsko podpisuje časovne žige.
Elektronski podpis	Je niz podatkov v elektronski obliki, ki je vsebovan, dodan ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika.
Izdajatelj časovnega žiga (ang. time-stamping authority)	Je fizična ali pravna oseba, ki opravlja storitev izdajanja časovnih žigov.
Koordiniran univerzalni čas (ang. Coordinated Universal Time)	Je čas določen v mednarodnem standardu za meritve časa, ITU-R Recommendation TF.460-5.
Kvalificirano digitalno potrdilo	Je digitalno potrdilo, ki izpolnjuje zahteve iz 28. člena ZEPEP. Izda ga overitelj, ki deluje v skladu z zahtevami iz 28. do 36. člena ZEPEP.
Pravila izdajatelja časovnih žigov, javni del	So del pravil izdajatelja časovnih žigov, ki vsebujejo bistvene določbe, ki vplivajo na odnos med izdajateljem in uporabniki od njega izdanih časovnih žigov ter tretjimi osebami, ki se zanašajo na te časovne žige.
Pravila izdajatelja časovnih žigov, zaupni del	So del pravil izdajatelja časovnih žigov, ki vsebujejo določila glede prostorov, osebja, fizičnega, elektronskega in programskega varovanja infrastrukture izdajatelja, notranjega nadzora, ukrepanja ob nepredvidenih dogodkih in določila glede vodenja zapisov in sestave dnevnikov.
Tretja oseba	Je subjekt, ki ni aktivno udeležen v storitev časovnega žigosanja, vendar zaupa izvajalcu in rezultatu storitve.
Uporabnik storitve časovnega žiga	Je imetnik digitalnega potrdila, ki aktivno uporablja storitev časovnega žigosanja.
Varen časovni žig	Je elektronsko podpisano potrdilo izdajatelja, ki potrjuje obstoj podatkov, na katere se nanaša, v navedenem času. Varen časovni žig mora vsebovati nedvoumne in pravilne podatke o datumu, točnem času najmanj na sekundo natančno in 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 digitalnim potrdilom.

Varen elektronski podpis	Je elektronski podpis, ki izpolnjuje naslednje zahteve: • povezan je izključno s podpisnikom; • iz njega je mogoče zanesljivo ugotoviti podpisnika; • ustvarjen je s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom; • povezan je s podatki, na katere se nanaša, tako, da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi.

3.2. Kratice

Kratica	Opis
ASN.1	Priporočila organizacije ITU-T, ki definirajo različne strukturirane podatke (ang. Abstract Syntax Notation One).
ETSI	Evropski inštitut za standardizacijo na področju telekomunikacij (ang. European Telecommunications Standards Institute).
FIPS	Standardi za informacijske tehnologije, ki so v uporabi v ameriških zveznih institucijah. Izdaja jih ameriški nacionalni inštitut za standarde in tehnologijo (ang. Federal Information Processing Standards).
IETF	Združenje strokovnjakov s področja Internetnih tehnologij. Izdelujejo serije priporočil (ang. Internet Engineering Task Force).
INTRANET MO	Notranje omrežje MO; del KIS MO.
ISO	Mednarodna organizacija za standardizacijo (ang. International Standardization Organization).
ITU-T	Mednarodna organizacija za standardizacijo na področju telekomunikacij (ang. International Telecommunications Union - Telecommunication Standardization Sector).
KIS MO	Komunikacijsko informacijski sistem MO.
LDAP	Protokol, ki določa dostop do imenika in je specificiran po IETF priporočilu RFC 1777 (ang. Leightweight Directory Access Protocol).
MO	Ministrstvo za obrambo
NTP	Protokol za sinhronizacijo časa, specificiran v priporočilu RFC 1305 (ang. Network Time Protocol).
PKI	Infrastruktura javnih ključev; strojna in programska oprema ter varnostni mehanizmi za zaupanja vredno implementacijo varnostnih storitev, ki temeljijo na nesimetrični kriptografiji (ang. Public Key Infrastructure).
RFC	Priporočila, ki jih izdaja IETF (ang. Reguest for Comment).
SV	Slovenska vojska
UTC	Univerzalni koordinirani čas, specificiran v priporočilu ITU-R Recommendation TF.460-5 Time scale notations (ang. Universal Time Coordinated).
XML	Računalniški jezik in priporočila za opisovanje strukturiranih podatkov (ang. Extensible Markup Language), ki nastaja v okviru spletnega konzorcija (ang. World Wide Web Consortium).

4. OSNOVNI KONCEPTI

4.1. Storitev časovnega žigosanja

Storitev časovnega žigosanja je razdeljena na dve komponenti:

- izdajanje varnih časovnih žigov in
- upravljanje časovnega žigosanja, ki zagotavlja, da se storitev izdajanja varnih časovnih žigov izvaja samo ob izpolnjenih predpisanih zahtevah. Na primer, izdajanje varnih časovnih žigov se izvaja samo, ko je razpoložljiv vir točnega časa.

Zgoraj navedena razdelitev storitve na dve komponenti ne predpisuje načina implementacije storitve časovnega žigosanja.

4.2. Izdajatelj SIMoD-TSA-Restricted

Izdajatelja SIMoD-TSA-Restricted zastopa Svet za upravljanje z infrastrukturo javnih ključev na MO.

4.2.1. Svet za upravljanje z infrastrukturo javnih ključev na MO

V zvezi z izdajateljem SIMoD-TSA-Restricted ima Svet za upravljanje z infrastrukturo javnih ključev na MO naslednje obveznosti:

- nadzira izdelavo in vodi postopek potrditve Pravil SIMoD-TSA-Restricted,
- ocenjuje predlagane spremembe, predlaga uveljavitve sprememb in vodi postopek uveljavitve sprememb Pravil SIMoD-TSA-Restricted,
- ocenjuje in potrjuje skladnost Pravil SIMoD-TSA-Restricted s [5] Politika SIMoD-PKI,
- sprejema Pravila SIMoD-TSA-Restricted,
- imenuje operativno osebje izdajatelja SIMoD-TSA-Restricted in
- operativnemu osebju izdajatelja SIMoD-TSA-Restricted daje usmeritve in navodila za odpravljanje pomanjkljivosti, ugotovljene v nadzoru skladnosti delovanja s [5] Politika SIMoD-PKI in [6] Pravila SIMoD-CA-Restricted oziroma uveljavlja druge ustrezne ukrepe.

4.2.2. Operativno osebje izdajatelja SIMoD-TSA-Restricted

Naloge upravljanja ter zagotavljanja varnega in zanesljivega delovanja izdajatelja SIMoD-TSA-Restricted opravlja operativno osebje izdajatelja SIMoD-TSA-Restricted.

4.3. Uporabniki

Uporabniki varnih časovnih žigov so imetniki digitalnih potrdil overiteljev SIMoD-PKI in tretje osebe, ki priznavajo varne časovne žige na osnovi podpisane pogodbe ali sklenjenega dogovora o priznavanju varnih časovnih žigov izdajatelja SIMoD-TSA-Restricted.

4.4. Politika izdajanja varnih časovnih žigov in postopki izdajatelja

Pričujoči dokument vsebuje politiko izdajanja varnih časovnih žigov (poglavje 5. POLITIKA IZDAJATELJA SIMoD-TSA-Restricted), ter postopke izdajatelja varnih časovnih žigov (poglavje 7 POSTOPKI IZDAJATELJA SIMoD-TSA-Restricted).

Politika izdajanja varnih časovnih žigov predpisuje minimalne zahteve, ki jih mora izdajatelj izpolnjevati ob izvajanju storitve časovnega žigosanja.

Postopki izdajatelja varnih časovnih žigov predpisujejo postopke, ki jih izdajatelj izvaja pri izvajanju storitve časovnega žigosanja, da izpolni zahteve iz politike.

5. POLITIKA IZDAJATELJA SIMoD-TSA-Restricted

5.1. Pregled

Politika izdajatelja SIMoD-TSA-Restricted predpisuje zahteve, ki jih mora izpolnjevati izdajatelj SIMoD-TSA ob izdajanju varnih časovnih žigov.

5.2. Identifikacijska oznaka politike

Identifikacijska oznaka politike (ang. Policy Object Identifier, Policy OID) izdajanja varnih časovnih žigov izdajatelja SIMoD-TSA-Restricted je:

1.3.6.1.4.1.22295.10.1.3.1.1

5.3. Uporabniki in namen uporabe

Varni časovni žigi, izdani v skladu s Pravili SIMoD-TSA-Restricted, so namenjeni izključno službeni uporabi v MO. V drugih institucijah pa je namen omejen na opravljanje nalog povezanih z obrambo države.

Varni časovni žigi izdajatelja SIMoD-TSA-Restricted se uporabljajo za implementacijo storitev časovnega žigosanja povsod tam, kjer je dovoljena uporaba digitalnih potrdil overiteljev SIMoD-PKI.

5.4. Skladnost

Storitve izdajatelja SIMoD-TSA-Restricted, njegovo delovanje in infrastruktura, so v skladu z zahtevami in jamstvi Pravil SIMoD-TSA-Restricted.

Izdajatelj SIMoD-TSA-Restricted vključi v vse izdane varne časovne žige identifikacijsko oznako politike iz poglavja 5.2 Identifikacijska oznaka politike in s tem jamči skladnost s to politiko.

Skladnost delovanja izdajatelja SIMoD-TSA-Restricted z [7] ZEPEP, [5] Politika SIMoD-PKI in [6] Pravila SIMoD-CA-Restricted preverja inšpekcijski nadzor v okviru SIMoD-PKI.

6. OBVEZNOSTI IN ODGOVORNOSTI

6.1. OBVEZNOSTI IZDAJATELJA SIMoD-TSA-Restricted

6.1.1. Splošne obveznosti izdajatelja SIMoD-TSA-Restricted

Izdajatelj SIMoD-TSA-Restricted jamči, da izvaja vse postopke in izdaja varne časovne žige v skladu s Pravili SIMoD-TSA-Restricted, veljavno zakonodajo ter ostalimi predpisi in priporočili.

6.1.2. Obveznosti izdajatelja SIMoD-TSA-Restricted do uporabnikov

Izdajatelj SIMoD-TSA-Restricted jamči, da:

- čas, ki je vsebovan v vsakem izdanem varnem časovnem žigu, ne odstopa več kot +/- 1sekundo od univerzalnega koordiniranega časa (ang. Universal Time Coordinated, UTC, po priporočilu [11] ITU-R Recommendation TF.460-5) in
- izdani varni časovni žigi ne vsebujejo napačnih podatkov ali napak.

Izdajatelj SIMoD-TSA-Restricted deluje 24 ur na dan vse dni v letu, vendar si pridržuje pravico za zaustavitev delovanja v primeru nepravilnega delovanja, ogrožanja svoje infrastrukture in tehničnih vzrokov. Vzdrževalna dela ali nadgradnje infrastrukture bo izdajatelj SIMoD-TSA-Restricted najavil vsaj 3 dni pred pričetkom del.

6.2. Obveznosti uporabnikov

Uporabniki storitve varnega časovnega žiga morajo:

- seznaniti se z Javnimi pravili SIMoD-TSA-Restricted in upoštevati vsa določila glede obveznosti, odgovornosti ter omejitev odgovornosti pri uporabi varnega časovnega žiga,
- spremljati obvestila in objave izdajatelja SIMoD-TSA-Restricted in ravnati v skladu z njimi,
- ob prevzemu varnega časovnega žiga preveriti njegovo veljavnost in preveriti, da digitalno potrdilo za preverjanje podpisa varnega časovnega žiga ni bilo preklicano,
- skrbeti za arhiv časovno žigosanih dokumentov ter podatkov potrebnih za preverjanje časovno žigosanih dokumentov,
- upoštevati tehnične pogoje za uporabo storitve varnega časovnega žiga in
- upoštevati morebitne obveznosti, določila ali omejitve, objavljene drugje.

6.3. Obveznosti tretjih oseb

Tretje osebe, ki se zanašajo na varne časovne žige izdajatelja SIMoD-TSA-Restricted, morajo:

- omejiti zaupanje v varen časovni žig le na namene, določene v Javnih pravilih SIMoD-TSA-Restricted,
- seznaniti se z Javnimi pravili SIMoD-TSA-Restricted in upoštevati vsa določila glede obveznosti, odgovornosti in omejitev odgovornosti pri uporabi varnega časovnega žiga,
- preveriti veljavnost varnega časovnega žiga oziroma preveriti, da digitalno potrdilo za preverjanje podpisa varnega časovnega žiga ni bilo preklicano in
- upoštevati morebitne obveznosti, določila ali omejitve objavljene drugje.

6.4. Omejitve odgovornosti

Izdajatelj SIMoD-TSA-Restricted ni odgovoren za direktno ali posredno škodo, izgube, stroške ter terjatve, ki izhajajo iz ali so nastale zaradi uporabe varnega časovnega žiga, če:

- je bil varni časovni žig uporabljen v drugačne namene, kot je dovoljeno s Javnimi pravili SIMoD-TSA-Restricted ali v nasprotju z relevantnimi zakoni,
- uporabnik storitve varnega časovnega žiga ali tretja stran ni postopal v skladu s predpisanimi postopki v Javnih pravilih SIMoD-TSA-Restricted ali

- je nastala škoda zaradi napake v delovanju strojne ali programske opreme uporabnika storitve varnega časovnega žiga ali tretje strani.

7. POSTOPKI IZDAJATELJA SIMoD-TSA-Restricted

Izdajatelj SIMoD-TSA-Restricted za zagotavljanje zaupanja v varne časovne žige izvaja v tem poglavju opisane postopke in varnostne kontrole ter uporablja navedene tehnične rešitve.

7.1. Izjava o postopkih izdajatelja in obvestilo uporabnikom in tretjim osebam

7.1.1. Izjava o postopkih izdajatelja SIMoD-TSA-Restricted

Vsi postopki, ki jih izvaja izdajatelj SIMoD-TSA-Restricted, so opisani Javnih pravilih SIMoD-TSA-Restricted, v Pravilih delovanja izdajatelja varnih časovnih žigov SIMoD-TSA-Restricted, zaupni del (v nadaljevanju Zaupna pravila SIMoD-TSA-Restricted) in v dopolnjujočih navodilih.

Postopki, ki jih izvaja izdajatelj SIMoD-TSA-Restricted kot sestavni del komunikacijsko informacijskega sistema MO (v nadaljevanju KIS MO), se izvajajo v okviru predpisanih postopkov za KIS MO.

7.1.2. Obvestilo uporabnikom in tretjim osebam

Izdajatelj SIMoD-TSA-Restricted objavi na spletni strani www.simod-pki.mors.si obvestilo uporabnikom in tretjim osebam o pogojih uporabe varnih časovnih žigov, ki vsebuje naslednja določila:

Določilo obvestila uporabnikom	Vsebina določila oziroma referenca na vsebino, zahtevano v določilu
Naslov izdajatelja časovnih žigov	Naslov Sveta za upravljanje z infrastrukturo javnih ključev na MO, ki je naveden v poglavju 1.5.2. Kontaktna oseba v [5] Politika SIMoD-PKI.
Oznaka politike časovnih žigov	Določena v poglavju 5.2 Identifikacijska oznaka politike.
Kriptografski algoritmi: zgoščevali algoritem algoritem digitalnega podpisa dolžina ključa	 SHA-1 ali SHA-256 sha1WithRSAEncryption ali sha256WithRSAEncryption 2048 bitov
Veljavnost časovnega žiga	Določena z veljavnostjo digitalnega potrdila SIMoD-TSA-Restricted, ki je določena v poglavju 6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil v [6] Pravila SIMoD-CA-Restricted.
Točnost časa v časovnem žigu	Določena v poglavju 6.1.2 Obveznosti izdajatelja SIMoD-TSA-Restricted do uporabnikov.
Omejitve uporabe storitve časovnega žigosanja	Storitve časovnega žigosanja so omejene na namene določene v poglavju 5.3 Uporabniki in namen uporabe.
Obveznosti uporabnikov	Določene v poglavju 6.2 Obveznosti uporabnikov.
Obveznosti tretjih oseb	Določene v poglavju 6.3 Obveznosti tretjih oseb.
Navodilo in obveza tretji osebi, da preveri veljavnost časovnega žiga	Določena v poglavju 6.3 Obveznosti tretjih oseb.

Obdobje hranjenja zapisov beleženih dogodkov	Določeno v poglavju 7.4.11 Beleženje dogodkov povezanih s storitvijo časovnega žig.
Veljavna zakonodaja	Navedena v poglavju 7.4.10 Skladnost z zakonodajo.
Omejitve odgovornosti	Navedene v poglavju 6.4 Omejitve odgovornosti.
Reševanje sporov	V skladu s poglavjem 9.13 reševanje sporov [6] Pravila SIMoD-CA-Restricted
Jamstva o skladnosti s politiko izdajanja časovnih žigov	Navedena v poglavju 5.4 Skladnost.

7.2. Upravljanje s ključi izdajatelja SIMoD-TSA-Restricted

7.2.1. Generiranje para ključev

Generiranje para ključev v povezavi z digitalnimi potrdili izdajatelja SIMoD-TSA-Restricted in izdajanje varnih časovnih žigov se izvaja v strojnem varnostnem kriptografskem modulu, ki ima potrdilo o skladnosti s [4] FIPS 140-2 Level 3.

Generiranje para ključev izvede operativno osebje izdajatelja SIMoD-TSA-Restricted ob prisotnosti prič, ki nadzorujejo izvajanje postopka. Izvedba postopka se dokumentira v zapisniku.

7.2.2. Zaščita zasebnega ključa

Zasebni ključ izdajatelja SIMoD-TSA-Restricted se generira in uporablja izključno v varnostnem kriptografskem modulu. Zasebni ključ se izven varnostnega kriptografskega modula nikdar ne pojavi v nešifrirani obliki.

Za operacije, kjer se upravlja z varnostnim kriptografskim modulom izdajatelja SIMoD-TSA-Restricted, je vedno potrebna prisotnost vsaj dveh oseb z ustreznimi pooblastili, ki izkažeta svojo istovetnost s pametno kartico s porazdeljenim ključem kriptografskega modula in skrivnim geslom kartice.

Varnostna kopija zasebnega ključa izdajatelja SIMoD-TSA-Restricted se zagotavlja z varnostnimi mehanizmi varnostnega kriptografskega modula. Varnostna kopija je pred izvozom iz varnostnega kriptografskega modula šifrirana. Dešifrirni ključ je porazdeljen na N[1] od M[2] operaterskih pametnih karticah varnostnega kriptografskega modula.

Zasebni ključi izdajatelja SIMoD-TSA-Restricted se ne arhivirajo.

7.2.3. Dostava javnega ključa

Javni ključ je objavljen v digitalnem potrdilu izdajatelja SIMoD-TSA-Restricted. Uporabniki lahko digitalno potrdilo pridobijo kadarkoli iz imenika ali na spletnih straneh http://www.simod-pki.mors.si, vendar je njihova obveznost, da preverijo istovetnost izdajatelja SIMoD-TSA-Restricted in celovitost digitalnega potrdila.

7.2.4. Obnova ključev

Veljavnost ključev in digitalnih potrdil izdajatelja SIMoD-TSA-Restricted je določena v poglavju 6.3.2. Obdobje veljavnosti ključev in digitalnih potrdil v [6] Pravila SIMoD-CA-Restricted.

[1] N mora biti enako ali večje od 2.
[2] M mora biti eneko ali večje od 3.

Obnova ključev izdajatelja SIMoD-TSA-Restricted se izvede pred iztekom obdobja veljavnosti zasebnega ključa. V postopku obnove se tvori nov par ključev v skladu z določili poglavja 7.2.1 Generiranje para ključev.

7.2.5. Prenehanje veljavnosti ključev

Izdajatelj SIMoD-TSA-Restricted zagotavlja, da ne uporablja zasebnih ključev po prenehanju njihove veljavnosti.

Zasebni ključi se uničijo tako, da jih ni več mogoče povrniti. Mediji, na katerih se je nahajal zasebni ključ, so varno izbrisani. V postopku uničenja zasebnih ključev je uničena tudi varnostna kopija zasebnih ključev.

7.2.6. Upravljanje z varnostnim kriptografskim modulom

Varnostni kriptografski modul je poslan s strani dobavitelja na naslov izdajatelja SIMoD-TSA-Restricted v zaprti pošiljki. Operativno osebje izdajatelja SIMoD-TSA-Restricted ob prejemu pošiljke preveri, da ni poškodovana in ni bila odprta. Po odprtju pošiljke operativno osebje izdajatelja SIMoD-TSA-Restricted preveri neoporečnost varnostnega kriptografskega modula.

Varnostni kriptografski modul se hrani v varovanih prostorih izdajatelja SIMoD-TSA-Restricted.

Instalacija in aktiviranje varnostnega kriptografskega modula izvede operativno osebje izdajatelja SIMoD-TSA-Restricted v varovanih prostorih. V postopku aktiviranja in tvorjenja ključev so uporabljeni mehanizmi večkratne avtorizacije.

7.3. Časovno žigosanje

7.3.1. Varen časovni žig

Vsak varni časovni žig izdajatelja SIMoD-TSA-Restricted je izdan varno in vsebuje točen čas. Bistvene lastnosti vsakega izdanega varnega časovnega žiga so:

- vsebuje identifikacijsko oznako politike, kot je določena v poglavju 5.2 Identifikacijska oznaka politike,
- vsebuje edinstveno identifikacijsko oznako varnega časovnega žiga,
- vsebuje čas, ko je bil varni časovni žig ustvarjen,
- čas, vsebovan v varnem časovnem žigu, je v okviru odstopanj določenih v poglavju 6.1.2 Obveznosti izdajatelja SIMoD-TSA-Restricted do uporabnikov,
- v primeru nerazpoložljivosti časovnega vira ali če je odstopanje časa večje od zajamčenega, se varnega časovnega žiga ne izda,
- varni časovni žig je ustvarjen z zasebnim ključem, ki se uporablja le v ta namen in
- oblika zahtevka za pridobitev varnega časovnega žiga ter varni časovni žig mora biti v skladu s priporočilom [13] RFC 3161 ali z Entrust Timestamp XML shemo.

7.3.2. Sinhronizacija ure z univerzalnim koordiniranim časom

Ura izdajatelja SIMoD-TSA-Restricted je usklajena s satelitskim sprejemnikom univerzalnega koordiniranega časa.

Izdajatelj SIMoD-TSA-Restricted usklajuje svojo uro s sprejemnikom univerzalnega koordiniranega časa po protokolu za sinhronizacijo časa (ang. Network Time Protocol, NTP, po priporočilu [12] RFC 1305).

Satelitski sprejemnik koordiniranega univerzalnega časa je zavarovan pred nepooblaščenim dostopom.

7.4. Organizacija in upravljanje izdajatelja SIMoD-TSA-Restricted

7.4.1. Upravljanje varnosti

Upravljanje varnosti izdajatelja SIMoD-TSA-Restricted kot sestavnega dela KIS MO, se izvaja v okviru predpisanih postopkov za KIS MO.

Izdajatelj SIMoD-TSA-Restricted evidentira postopke inštalacije, sprememb konfiguracije in nadgradnje za vse svoje komponente.

Posebne zahteve glede upravljanja varnosti izdajatelja SIMoD-TSA-Restricted so opisane v Zaupnih pravilih SIMoD-TSA-Restricted in izvedbenih navodilih.

7.4.2. Označevanje gradnikov izdajatelja SIMoD-TSA-Restricted

Označevanje in upravljanje z gradniki izdajatelja SIMoD-TSA-Restricted kot sestavnega dela KIS MO se izvaja skladno z s predpisi, ki urejajo področje tajnih podatkov in označevanje gradnikov KIS MO.

7.4.3. Zahteve za osebje izdajatelja SIMoD-TSA-Restricted

7.4.3.1. Operativno osebje izdajatelja SIMoD-TSA-Restricted

Z izdajateljem SIMoD-TSA-Restricted upravlja operativno osebje izdajatelja SIMoD-TSA-Restricted.

Operativno osebje izdajatelja SIMoD-TSA-Restricted mora biti usposobljeno za delo s strojno in programsko opremo izdajatelja varnih časovnih žigov, za ukrepanje ob izrednih dogodkih in za zagotavljanje neprekinjenega delovanja.

Razdelitev nalog je podrobneje določena v Zaupnih pravilih SIMoD-TSA-Restricted.

7.4.3.2. Druge funkcije

Pristojne organizacijske enote v MO skrbijo za:

- fizično varovanje in nadzor prostorov izdajatelja SIMoD-TSA-Restricted ter
- pravne zadeve.

Pomoč uporabnikom opravlja skupina zaposlenih v organizacijski enoti MO, pristojni za informatiko in telekomunikacije, ki skrbi za pomoč uporabnikom pri delu z informacijskimi sistemi ter pooblaščene osebe za informatiko v organizacijskih enotah MO. Zaposleni iz tega odstavka niso del operativnega osebja izdajatelja SIMoD-TSA-Restricted.

Nastavitev uporabniškega okolja uporabnikom storitev varnega časovnega žiga je naloga skupine zaposlenih v organizacijski enoti MO, pristojni za informatiko in telekomunikacije, ki skrbi za uporabniško okolje ter pooblaščenih oseb za informatiko v organizacijskih enotah MO. Zaposleni iz tega odstavka niso del operativnega osebja izdajatelja SIMoD-TSA-Restricted.

7.4.3.3. Zunanji izvajalci

Zunanji izvajalci morajo za izvajanje posegov izpolnjevati vse pogoje, določene v [9] ZTP oziroma implementacijo pravil na lokacijah izdajatelja SIMoD-TSA-Restricted.

7.4.4. Fizično varovanje

7.4.4.1. Lokacija in konstrukcija prostorov

Dejavnosti izdajatelja SIMoD-TSA-Restricted se izvajajo v ustrezno varovanih prostorih in na varni lokaciji.

Prostori izpolnjujejo pogoje za namestitev komunikacijske in informacijske opreme ter arhivskih medijev skladno s predpisi, ki urejajo področje tajnih podatkov. Komunikacijska in informacijska oprema izdajatelja SIMoD-TSA-Restricted je nameščena v prostorih varnostnega območja I. stopnje.

7.4.4.2. Fizični dostop

Nadzor fizičnega dostopa izvaja pristojna služba MO.

Nadzor nad vstopom se izvaja z uporabo tehničnih sredstev, ki preprečujejo nepooblaščen vstop. Vstop je dovoljen samo operativnemu osebju izdajatelja SIMoD-TSA-Restricted. Druge osebe, ki izkažejo upravičeni interes, smejo vstopiti v prostore samo v spremstvu operativnega osebja izdajatelja SIMoD-TSA-Restricted. O vstopih in izstopih v prostore se vodi evidenca.

Preden odhodom iz prostorov je potrebno preveriti:

- da programska in strojna oprema pravilno in varno deluje (izdajatelj SIMoD-TSA-Restricted opravlja svoje storitve, gesla za upravljanje z izdajateljem pa morajo biti deaktivirana),
- da so varnostne omare pravilno zaklenjene,
- da so morebitni zapisi podatkov (npr. izpisi iz tiskalnika) primerno hranjeni, odvečno gradivo pa uničeno in
- da so varnostni mehanizmi varovanja vklopljeni in delujejo.

7.4.4.3. Napajanje in klimatske naprave

Prostor je opremljen s:

- sistemom za brezprekinitveno napajanje naprav in
- klimatsko napravo za kontrolo temperature in vlage.

7.4.4.4. Zaščita pred poplavo

Prostori se nahajajo na lokaciji, kjer je verjetnost poplave zelo majhna.

7.4.4.5. Zaščita pred ognjem

Prostori so opremljeni z detektorji temperature in dima.

7.4.4.6. Shranjevanje medijev

Mediji z varnostnimi kopijami in arhiv podatkov so shranjeni v ustrezni protivlomni omari.

Mediji, hranjeni na oddaljeni lokaciji, so v prostorih, ki zagotavljajo enake pogoje, kot so na osnovni lokaciji.

7.4.4.7. Odstranjevanje odpadkov

Dokumenti v papirni obliki se uničujejo z rezalnikom v varovanih prostorih izdajatelja SIMoD-TSA-Restricted. Vsebina medijev, na katerih se hranijo tajni podatki, se pred odstranitvijo iz prostorov varno izbriše ali pa se medije fizično uniči.

V primeru, da medijev ni mogoče varno izbrisati ali uničiti v prostorih izdajatelja SIMoD-TSA-Restricted, se medij dostaviti v uničevalno mesto po postopku, predpisanem za stopnjo tajnosti podatkov, ki jih medij hrani.

7.4.4.8. Hranjenje na oddaljeni lokaciji

Izdajatelj SIMoD-TSA-Restricted uporablja oddaljeno lokacijo za varno hranjenje varnostnih kopij in arhivskih podatkov. Podatki, mediji ali naprave so na oddaljeni lokaciji shranjene v varovanih prostorih, ki zagotavljajo enako raven varnosti kot je na osnovni lokaciji.

Pametne kartice s porazdeljenim šifriranim ključem, s katerim so zaščiteni zasebni ključi izdajatelja SIMoD-TSA-Restricted, se hranijo na različnih lokacijah.

7.4.5. Zagotavljanje varnega in zanesljivega delovanja

Izdajatelj SIMoD-TSA-Restricted ima vzpostavljene mehanizme za varno in zanesljivo delovanje.

7.4.5.1. Zagotavljanje celovitosti strojne in programske opreme

Preverjanje celovitosti operacijskega sistema in aplikativne programske opreme se preverja z ustreznim programskim orodjem.

Varnostni mehanizmi na nivoju KIS MO vključujejo zaščito pred virusi in neželeno programsko opremo.

Komponente informacijskega in komunikacijskega sistema izdajatelja SIMoD-TSA-Restricted so zaščitene s senzorji za zaščito pred vdori.

7.4.5.2. Ugotavljanje in odprava incidentov

Z namenom zagotavljanja varnega delovanja izdajatelja SIMoD-TSA-Restricted se beležijo dogodki, navedeni v poglavju 7.4.11 Beleženje dogodkov povezanih s storitvijo časovnega žigosanja.

Operativno osebje izdajatelja SIMoD-TSA-Restricted pregleduje dnevnike beleženih dogodkov z namenom odkrivanja in odprave incidentov. Ob vsakem opozorilu o morebitnem incidentu, ki ga razbere iz dnevnika beleženih dogodkov ali prejme iz nadzornega sistema oceni verjetnost povzročitve škode in predvidi ukrepe za zmanjšanje grožnje.

7.4.5.3. Upravljanje z mediji

Nosilci varnostnih kopij in arhiva podatkov, pametne kartice s porazdeljenim ključem za dostop do zasebnega ključa na varnostnem kriptografskem modulu in ostali mediji se hranijo na način, da je minimizirana možnost uničenja, kraje, nepooblaščenega dostopa.

Z nosilci tajnih podatkov se upravlja v skladu s predpisi, ki urejajo področje tajnih podatkov.

7.4.6. Upravljanje dostopa do sistemov

7.4.6.1. Varnostne kontrole na ravni računalniškega omrežja

Izdajatelj SIMoD-TSA-Restricted je nameščen v izoliranem omrežju infrastrukture SIMoD-PKI, ki je v interno omrežje INTRANET MO povezano preko varnostnih pregrad. Varnostna pravila na varnostnih pregradah dovoljujejo prehod samo protokolom, potrebnim za dostop do storitev infrastrukture SIMoD-PKI.

V povezavi z izdajateljem SIMoD-TSA-Restricted so uporabnikom dovoljeni samo protokoli za dostop do storitve časovnega žigosanja.

7.4.6.2. Fizični dostop do sistemov

Upravljanje in nadzor fizičnega dostopa do sistemov je opisan v poglavju 7.4.4.2 Fizični dostop.

7.4.6.3. Preverjanje istovetnosti operativnega osebja

Operativno osebje izdajatelja SIMoD-TSA-Restricted izkaže svojo istovetnost:

- pri vstopu v varovane prostore z identifikacijsko kartico in vstopno kodo in
- za delo na izdajateljevem informacijskem sistemu s prijavnim imenom in geslom.

Vsako prijavno ime ali digitalno potrdilo za opravljanje nalog operativne osebe mora:

- pripadati eni sami fizični osebi in
- omogočati avtorizacijo za izvedbo nalog samo v obsegu predpisanih nalog.

7.4.7. Vzpostavitev infrastrukture in vzdrževanje

Strojna oprema, operacijski sistemi in programska oprema izdajatelja SIMoD-TSA-Restricted so komercialni proizvodi.

Postopki inštalacije, sprememb konfiguracije in nadgradnje za vse komponente izdajatelja SIMoD-TSA-Restricted so dokumentirani.

Operativno osebje periodično in ob vsaki namestitvi nove verzije ali popravka preverja celovitost operacijskega sistema in aplikativne programske opreme izdajatelja SIMoD-TSA-Restricted.

Zunanji izvajalec, ki je dobavil informacijsko in komunikacijsko opremo in izvedel začetno inštalacijo, jamči, da oprema:

- res izvira od proizvajalca,
- v obdobju med proizvodnjo in inštalacijo ni prišlo do spreminjanja in posegov v opremo in
- je inštaliral opremo prave verzije in s predvidenim namenom uporabe.

Programska koda programske opreme je zaščitena na način, da se da preveriti njen izvor in celovitost.

7.4.8. Ogrožanje storitve varnega časovnega žigosanja

7.4.8.1. Načrt ponovne vzpostavitve delovanja

Izdajatelj SIMoD-TSA-Restricted v primeru ogrožanja zasebnega ključa, ob izgubi sinhronizacije ure s sprejemnikom univerzalnega koordiniranega časa ali ob ogrožanju strojne ali programske opreme oziroma podatkov, izvaja postopke za povrnitev storitve varnega časovnega žigosanja.

V primeru okvare strojne ali programske opreme oziroma podatkov, pri kateri zasebni ključi izdajatelja SIMoD-TSA-Restricted niso bili uničeni, bodo storitve časovnega žigosanja vzpostavljene nazaj v najkrajšem možnem času. Skrajni rok za vzpostavitev storitve je en teden (7 dni).

V primeru okvare, kjer pride do uničenja zasebnega ključa SIMoD-TSA-Restricted in vseh njegovih kopij, se postopa, kot da je prišlo do zlorabe zasebnega ključa.

Ob nezmožnosti vzpostavitve storitve v enem tednu (7 dni) ali ob zlorabi zasebnega ključa bo izdajatelj SIMoD-TSA-Restricted izvedel naslednje postopke:

- preklical svoje digitalno potrdilo,
- objavil obvestilo o preklicu potrdila in
- tvoril nove ključe.

7.4.8.2. Obveščanje uporabnikov o ogrožanju storitve

Izdajatelj SIMoD-TSA-Restricted bo uporabnike in tretje osebe obvestil o okoliščinah ogrožanja storitve varnega časovnega žigosanja.

7.4.8.3. Prekinitev izdajanja varnih časovnih žigov

V primeru ogrožanja storitve varnega časovnega žigosanja ali izgubi sinhronizacije ure s sprejemnikom univerzalnega koordiniranega časa oziroma v obdobju, ko ni zagotovljena točnost časa, kot je predpisano v poglavju 6.1.2 Obveznosti izdajatelja SIMoD-TSA-Restricted do uporabnikov, izdajatelj SIMoD-TSA-Restricted ne izdaja varnih časovnih žigov.

7.4.8.4. Obveščanje uporabnikov o ogroženih časovnih žigih

Izdajatelj SIMoD-TSA-Restricted bo uporabnikom in tretjim osebam zagotovil informacije, ki bodo omogočale prepoznavanje ogroženih varnih časovnih žigov.

7.4.9. Prenehanje delovanja izdajatelja SIMoD-TSA-Restricted

Vzroki za prenehanje delovanja izdajatelja SIMoD-TSA-Restricted so:

- zloraba zasebnih ključev izdajatelja SIMoD-TSA-Restricted,
- nezmožnost pravočasne ponovne vzpostavitve delovanja po okvari oz. nesreči,
- odločitev inšpekcije ali pristojnega sodišča ali
- prenehanje potrebe po storitvah izdajatelja SIMoD-TSA-Restricted.

Odločitev o prenehanju delovanja izda Svet za upravljanje z infrastrukturo javnih ključev na MO.

Takoj po sprejetju odločitve o prenehanju delovanja, nikoli pa kasneje kot tri (3) dni pred predvidenim prenehanjem delovanja, bo izdajatelj SIMoD-TSA-Restricted o tem obvestil vse uporabnike oziroma javno objavil namero o prenehanju delovanja.

Ob prenehanju delovanja bo izdajatelj SIMoD-TSA-Restricted:

- preklical potrdila izdajatelja SIMoD-TSA-Restricted in uničil svoje zasebne ključe,
- zagotovil razpoložljivost in dostopnost podatkov potrebnih za preverjanje veljavnosti izdanih varnih časovnih žigov in
- zagotovil hranjenje arhiviranih podatkov za obdobje pet (5) let po prenehanju delovanja.

7.4.10. Skladnost z zakonodajo

Izdajatelj SIMoD-TSA-Restricted izdaja varne časovne žige v skladu z:

- Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP; Uradni list RS, št. 98/04 –UPB1, 61/60),
- Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00 in 2/01 in 86/06),
- Zakonom o obrambi (Uradni list RS, št. 103/04 – uradno prečiščeno besedilo),
- Zakonom o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo) in
- priporočili EU in NATO.

7.4.11. Beleženje dogodkov povezanih s storitvijo časovnega žigosanja

7.4.11.1. Vrste beleženih dogodkov

Izdajatelj SIMoD-TSA-Restricted beleži naslednje dogodke:

- v zvezi s ključi izdajatelja SIMoD-TSA-Restricted,
- izdanimi varnimi časovnimi žigi,

- na operacijskem sistemu, programski in strojni opremi izdajatelja SIMoD-TSA-Restricted,
- na operacijskem sistemu, programski in strojni opremi komunikacijskega sistema,
- v zvezi s fizičnim dostopom do izdajatelja SIMoD-TSA-Restricted in
- povezane z uničevanjem kriptografskega materiala (npr. zasebnih ključev in nosilcev ključev).

Dnevnike beleženih dogodkov se zbira in obdeluje, če je le mogoče, v elektronski obliki. Originali dnevnikov beleženih dogodkov se hranijo v varovanih prostorih izdajatelja SIMoD-TSA-Restricted. Varnostna kopija dnevnikov beleženih dogodkov se hrani na lokaciji, oddaljeni vsaj 25 km od prostorov izdajatelja SIMoD-TSA-Restricted.

Obdobje hranjenja dnevnikov beleženih dogodkov je do naslednjega rednega pregleda na sistemu in najmanj pet (5) let v arhivu.

Z namenom lažjega pregledovanja dnevnikov beleženih dogodkov in izdelave arhiva se dnevnike lahko obdeluje in izdeluje poročila.

8. KONČNE DOLOČBE

Pravila delovanja izdajatelja varnih časovnih žigov SIMoD-TSA-Restricted, javni del, začnejo veljati in se uporabljati naslednji dan po podpisu.

Številka: 382-5/2006-124

Datum: 3.12.2010

Mag. Jurij Bertok
Sekretar
Vodja Sveta za upravljanje z infrastrukturo javnih ključev na MO