GOSPODARSKA ZBORNICA SLOVENIJE

IT SOLUTIONS & SERVICES

POSLOVANJE

Projekt *e*-SLOG

Elektronsko poslovanje slovenskega gospodarstva

A1 – Priporočila za format dokumenta (XML) za varen e-podpis

(S&T Hermes Plus, SETCCE, Crea)

A8 - Priporočila uporabe kriptografskih algoritmov

(S&T Hermes Plus)

v. 1.0
junij 2004

STANJE DOKUMENTA

Namen dokumenta:	delo skupine za e-podpis
Kratek naziv projekta:	e-SLOG – e-podpis
Vsebina:	*Glej "Vsebina"*
Status:	Objavljena verzija
Verzija:	1.0
Datum verzije:	junij 2004
Avtorji:	Rudi Ponikvar, CVI, e-SLOG
Naslovniki:	Dušan Zupančič (GZS), dusan.zupancic@gzs.si Ariana Grobelnik (GZS), ariana.grobelnik@gzs.si Samo Grčman (GZS), samo.grcman@gzs.si Dr. Aleš Dobnikar (CVI, ales.dobnikar@gzs.si Dr. Alenka Žužek (CVI), alenka.zuzek@gov.si Rudi Ponikvar (Hermes Plus), rudi.ponikvar@hermes-plus.si Tine Prislan (Hermes Plus), tine.prislan@hermes-plus.si Roman Puhek (Crea), roman.puhek@crea.si Matej Trampuš (Crea), matej.trampus@crea.si Aljoša Blažič (SETCCE), aljosa@setcce.org Gašper Lavrenčič (SETCCE), gasper@setcce.org Dr. Tomaž Klobučar (SETCCE), tomaz@setcce.org Boštjan Berčič (Institut za pravno informatiko), bostjan.bercic@ipri-zavod.si
Zgodovina verzij:	*Glej "Verzija"*

Verzija	Datum spremembe	Opombe
1.0	junij 2004	

VSEBINA

1. UVOD

Internet, kot odprto omrežje, postaja nepogrešljiv pri vsakodnevnem poslovanju večine podjetij in posameznikov, ter s tem glavni komunikacijski medij. Internet je v svojih prvih letih s stališča varnosti veljal za rizično okolje in ta sloves se ga drži še danes. Pri elektronskem načinu opravljanja storitev, pa je velik poudarek ravno na zagotavljanju ustrezne varnosti pri dostopu do posameznih aplikacij oziroma uporabi takšne infrastrukture, ki omogoča varno elektronsko poslovanje. Za uspešno vpeljavo elektronskega načina poslovanja je tudi pomembno, da storitve, ki se vršijo na elektronski način, zagotovijo enak ali celo višji nivo varnosti in zaupanja kot storitve, ki se opravljajo na klasičen način. Omogočiti je potrebno mehanizme za nedvoumno ugotavljanje identitete, zaupnost pri izmenjavi občutljivih podatkov, avtenticiran dostop do podatkov, ter celovitost podatkov. Za varno elektronskega poslovanje moramo tako zagotoviti:

- **avtentikacijo:** zagotoviti nedvoumno identifikacijo uporabnika kot tudi strežnika oz. aplikacije, do katere uporabnik dostopa,
- **nezatajljivost:** z digitalnim podpisom z podporo za nezatajljivost zagotoviti nezmožnost zanikanja izvora podatkov ter vključenost v opravljanje storitev, preprečiti možnost ponarejanja opravljenih storitev,
- **celovitosti podatkov:** z digitalnim podpisom podatkov zagotoviti celovitost izmenjanih podatkov, kar pomeni, da se zagotovi, da podatki niso bili kakorkoli spremenjeni od svojega nastanka in da o tem ciljni uporabnik ne bi bil obveščen,
- **zaupnost:** z ustreznimi postopki šifriranja zagotoviti zaupnost povezave med uporabnikom in strežnikom, prav tako pa mora biti zagotovljena zaščita podatkov, ki se ob tem izmenjajo.

Tehnologije, ki zagotavljanje servise potrebne za izpolnitev naštetih zahtev, so znane že vsaj toliko časa, ali pa dlje kot Internet, je pa uporaba Interneta v poslovne namene vzpodbudila razvoj komercialnih produktov, ki omogočajo njihovo širšo uporabo. Osnovne tehnologije so:

- šifriranje s simetričnimi ključi;
- šifriranje z asimetričnimi ključi (javni-skrivni ključ);
- digitalni podpis; in
- digitalna potrdila.

V varnostne rešitve e-storitev morajo biti poleg zgoraj naštetih osnovnih vidikov, ki jih lahko zagotovimo z uporabo digitalnih potrdil, vpeti tudi ostali splošni pogoji zagotavljanja varnosti:

- zaščita sistema s požarno pregrado,
- sistem za spremljanje vdorov,
- sistem za spremljanje alarmov,
- varnostno kopiranje dokumentov,
- protivirusna zaščita,
- zagotovitev visoke razpoložljivosti sistema,
- zagotovitev varnega ravnanja uporabnika.

Pričujoči dokument, ki je nastal v okviru delovne skupine za elektronski podpis, kot del projekta e-SLOG na Gospodarski zbornici Slovenije, v nadaljevanju podaja priporočilo za format dokumenta za elektronski podpis e-SLOG računa.

1.1. Področje, namen in organizacija poglavja

V dokumentu navajamo:

- Priporočilo XML sheme digitalnega podpisa e-SLOG računa.
- Priporočila uporabe kriptografskih algoritmov.

Ciljna publika poglavja so

- predvsem slovenska podjetja, ki želijo v svoje poslovne procese integrirati elektronski podpis, manj pa
- ponudniki programske opreme, ki vključuje elektronski podpis.

Namen poglavja je navesti priporočila na podlagi mednarodnih standardov in priporočil, ki bo omogočila združljivost rešitev med uporabniki e-SLOG Računa .

Poglavje je organizirano na naslednji način**:**

- v nadaljevanju uvodnega dela navajamo priporočila in standarde, priporočila, ki urejajo področje XML e-podpisa;
- v poglavju 2 podajamo pravno analizo vloge e-podpisa v elektronskem poslovanju;
- v poglavju **Error! Reference source not found.** je podan povzetek in opis priporočene sheme XML e-podpisa v okviru praktičnega kontrolnega seznama;
- terminološki slovar pojasnjuje pojme, ki se v dokumentu uporabljajo.

1.2. Mednarodni standardi in priporočila

World Wide Web Consortium (W3C) je mednarodna organizacija, katere poslanstvo je razvoj tehnologij, standardov in priporočil, ki omogočajo medsebojno povezljivost aplikacij v spletnem okolju. V W3C okviru deluje tudi delovna skupina za XML e-podpis, ki je pripravila priporočila za sintakso in procesiranje XML digitalnega podpisa. V nadaljevanju so našteta W3C priporočila s področja XML digitalnega podpisa.

W3C XML Signature WG priporočila:

- *RFC 2807 XML Signature Requirements,*
- *RFC 3275 XML-Signature Syntax and Processing,*
- *RFC 3076 Canonical XML,*

Signature Syntax and Processing (interop-report)
REC: http://www.w3.org/TR/xmldsig-core/
Draft Standard: http://www.ietf.org/rfc/rfc3275.txt
Canonical XML (Interop-report)
REC: http://www.w3.org/TR/xml-c14n
Informational: RFC3076
Exclusive Canonical XML (interop-report)
REC: http://www.w3.org/TR/xml-exc-c14n
XPath Filter (interop-report)
REC: http://www.w3.org/TR/xmldsig-filter2/
Additional XML Security URIs
Informational: http://www.ietf.org/internet-drafts/draft-eastlake-xmldsig-uri-03.txt
XML Signature Requirements
Note: http://www.w3.org/TR/xmldsig-requirements
Informational: http://www.ietf.org/rfc/rfc2807.txt

V Evropski uniji pripravlja standarde in priporočila s področja telekomunikacij in informacijske tehnologije European Telecommunications Standards Institute (ETSI). ETSI je neprofitna organizacija, katere poslanstvo je priprava standardov in priporočil za področje Evrope, ki bodo služili kot smernice razvoja telekomunikacijskih storitev in informacijske tehnologije v prihodnje. V nadaljevanju so našteta ETSI priporočila s področja elektronskega poslovanja.

ETSI priporočila s področja upravljanja infrastrukture digitalnih potrdil:

- *Policy requirements for certification authorities issuing qualified certificates - TS 101 456 v 1.2.1 (april 2002),*
- *Qualified Certificate Profile - TS 101 862 v 1.2.1 (junij 2001),*
- *Policy requirements for certification authorities issuing public key certificates - TS 102 042 (april 2002),*
- *International Harmonization of Policy Requirements for CAs issuing Certificates - TR 102040 (marec 2002).*

ETSI priporočila glede storitve časovnega žiga:

- *Policy requirements for time-stamping authorities - TS 102 023 (april 2002),*

- *Time stamping profile - TS 101 861 v1.2.1 (marec 2002).*

ETSI priporočila glede digitalnega podpisa:

- *Signature Policies Report - TR 102 041 (februar 2002),*
- *XML Advanced Electronic Signatures (XAdES) - TS 101 903 (februar 2002),*
- *Electronic Signature Formats - TS 101 733 v 1.3.1 (februar 2002),*
- *XML format for signature policies - TR 102 038 (april 2002).*
- *Signature Policy for Extended Business Model –TR 102 045 STF 209-T1 (nov. 2002) - osnutek.*
- *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures – ETSI SR 002 176 V1.1.1 (2003-03) – posebno poročilo.*

2. PRAVNA PODLAGA

Celovitost podatkov in nezatajljivost sta kritična elementa varnega elektronskega poslovanja. To dejstvo je bilo potrjeno tudi z pravno formalno ureditvijo elektronskega poslovanja. Področje elektronskega poslovanja je pravno formalno urejeno na več nivojih. V okviru držav EU zakonodajno področje elektronskega poslovanja urejajo ustrezne direktive evropskega parlamenta in komisije združenih narodov. Poleg teh pa ima večinoma vsaka članica EU tudi svojo nacionalno zakonodajo.

V Sloveniji ureja področje elektronskega podpisa Zakon o elektronskem poslovanju in elektronskem podpisu (Ur.l. RS, št. 57/2000, 30/2001), s pripadajočo Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Ur.l. RS, št. 77/2000, 2/2001), ki usklajen z Direktivo 1999/93/EC in z določili Modelnega zakona Komisije OZN za mednarodno gospodarsko pravo (UNCITRAL) o elektronskem poslovanju in enotnimi pravili za elektronske podpise ter z določili primarne evropske zakonodaje.

V predpisih na območju Republike Slovenije, področje sintakse in procesiranja XML digitalnega podpisa ni posebej urejeno, zato se pričujoči dokument naslanja na mednarodne standarde, priporočila in prakso.

3. PRAKTIČNA PRIPOROČILA S KONTROLNO LISTO

3.1. Priporočilo XML sheme digitalnega podpisa e-SLOG računa.

3.1.1 XML digitalni podpis (XML-Signature [XMLDSIG])

W3C XML-Signature priporočilo (RFC3275) za digitalni podpis, je razvito za uporabo pri izmenjavi XML dokumentov. Priporočilo določa sintakso in pravila procesiranja digitalnega podpisa v XML dokumentih. Podobno kot ostali standardi za shranjevanje podpisanih podatkov (npr. PKCS #/7), zagotavlja avtentifikacijo podpisnika, integriteto podatkov in podporo nezanikanju. Za razliko od ostalih standardov, pa XML-Signature upošteva lastnosti in prednosti Interneta in XML-a. XML-Signature lahko uporabimo za podpis podatkov XML obliki, podatkov v tekstovni obliki (npr. HTML), podatkov v binarni obliki (npr. JPG), ali pa le del podatkov v XML obliki. Podpisani podatki so lahko vključeni v XML-Signature strukturo preko sklica na URI, so del istega dokumenta kot XML-Signature, so vsebovani v XML-Signature strukturi, ali pa je XML-Signature del podatkovne strukture.

XML-Signature sestavljajo komponente prikazane na Sliki 1.

<Signature>	
<SignedInfo>	Znotraj <SignedInfo> se nahajajo podpisani podatki.
(CanonicalizationMethod)	Algoritem uporabljen za preoblikovanje <SignedInfo> zapisa v točno določeno obliko.
(SignatureMethod)	Algoritem uporabljen za ustvarjanje digitalnega podpisa.
(<Reference (URI=)? >	Nabor sklicev (referenc) in pripadajočih zgoščenih vrednosti vključenih v <SignedInfo> element.
(Transforms)?	Seznam operacij, izvedenih na podatkih, preden je izveden izračun zgoščene vrednosti.
(DigestMethod)	Algoritem uporabljen za izračun zgoščene vrednosti podatkov.
(DigestValue)	Zgoščena vrednost podatkov.
</Reference>)+	
</SignedInfo>	
(SignatureValue)	Vsebuje digitalni podpis (šifrirano zgoščeno vrednost <SignedInfo> elementa).
(KeyInfo)?	Element vsebuje seznam podatkov (na primer digitalnih potrdil, algoritmov) potrebnih za preverjanje podpisa.
(Object)*	Podatki o objektu (delu XML dokumenta, če je le ta del podpisa.
</Signature>	

Slika 1: Struktura XML Signature dokumenta

3.1.2 Varen XML digitalni podpis

V EU je European Telecommunications Standards Institute (ETSI) pripravil priporočilo za *XML Advanced Electronic Signatures (XAdES) - TS 101 903 (februar 2002)*, ki osnovni XML-Signature (W3C XMLDSIG) specifikaciji XML digitalnega podpisa, dodaja elemente za varen digitalni podpis, ter elemente za dolgotrajno in legitimno hranjenje digitalno podpisanih dokumentov.

XAdES priporočilo temelji na ETSI *Electronic Signature Formats - TS 101 733 v 1.3.1 (februar 2002)* priporočilu, ki podaja splošne pogoje za ustvarjanje varnega e-podpisa, zagotavljanje nezataljivosti, ter dolgotrajno in legitimno hranjenje digitalno podpisanih dokumentov. ETSI za format e-podpisa s podano realizacijo e-podpisa z različnimi zahtevami po času ohranjanja v formatu XML. ETSI *Electronic Signature Formats - TS 101 733 v 1.3.1 (februar 2002)* priporočilo za realizacijo e-podpisa uporablja ASN.1 (Abstract Syntax Notation 1) notacijo in sledi RFC 2630 priporočilu.

ETSI *Electronic Signature Formats - TS 101 733 v 1.3.1 (februar 2002)* priporočilo določa sledeče oblike e-podpisa:

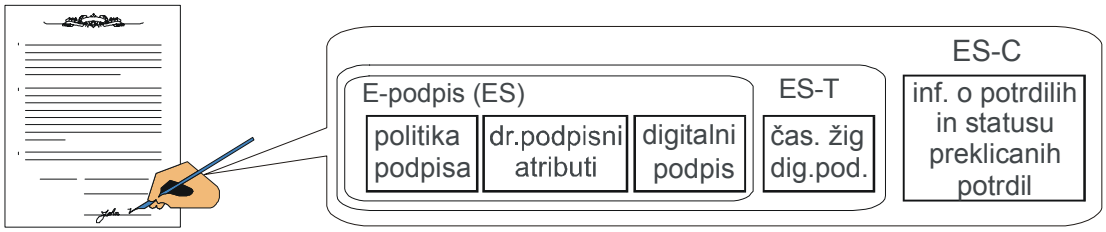
1. **Osnovni elektronski podpis, ES** (angl. *electronic signature*): vključuje elektronski podpis in ostale osnovne informacije, priložene s strani podpisnika; za pravno veljavnost pa vključuje še druge potrebne atribute podpisa:
   - referenca na politiko elektronskega podpisa, ki določa tehnične zahteve in pravna razmerja med podpisom in tretjo osebe, ter ostale potrebne atribute digitalnega podpisa,
   - podpisani podatki;
   - digitalni podpis (ustvarjen s podpisnikovim zasebnim ključem);
   - drugi podpisani atributi (definirani v politiki uporabe elektronskega podpisa in so lahko obvezni ali neobvezni):
     - oznaka namena podpisa (angl. *commitment type*);
     - enolična razločevalna oznaka digitalnega potrdila podpisnika;
     - vloga podpisnika (angl. *role attribute*);
     - lokacija podpisnika;
     - datum in ura podpisa;
     - format podpisanih podatkov

   Ta oblika nudi osnovno identifikacijo podpisnika in zaščito celovitosti. Ustvarimo ga lahko brez dostopa do »on-line« storitev (časovnega žiga), zaradi česar ta oblika ne nudi možnosti za določitev časovnega okvirja (kdaj je bil elektronski podpis ustvarjen), kakor tudi ne zaščite proti kasnejšemu zanikanju podpisnika, da je bil elektronski podpis ustvarjen v času veljavnosti pripadajočega potrdila.

2. **Elektronski podpis s časovnim žigom, ES-T** (angl. *electronic signature with time*): doda ES časovni žig, ali časovno oznako.

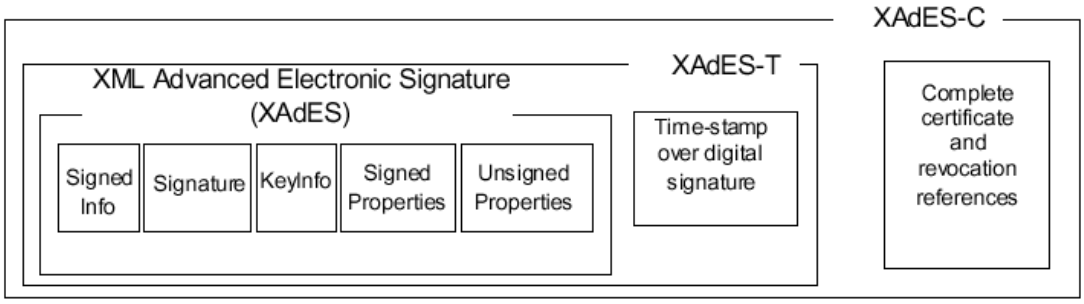
3. **Elektronski podpis z vsemi podatki za overjanje, ES-C** (angl. *electronic signature with complete validation data*): ES-T doda reference na vse podatke, ki zagotavljajo (overitveno pot, informacijo o preklicu). ES-C vsebuje tako referenco na vse podatke za vrednotenje, kot tudi njihove zgoščene vrednosti. PRI ES-C obliki se podatki za preverjanje veljavnost elektronskega podpisa ne hranijo skupaj z ES. ES-X (ES extended) predstavlja razširjeno ES-C obliko, ki se od osnovne ES-C oblike razlikuje v tem, da se podatki za preverjanje veljavnost elektronskega podpisa hranijo skupaj z ES.

Na Sliki 2. je podan prikaz elektronskega podpisa (ES) z dodanim časovnim žigom (ES-T) in vsemi podatki za overjanje (ES-C).



Slika 2. – Elektronski podpis s časovnim žigom in podatki za overjanje

XAdES prenaša opisane oblike elektronskega podpisa v XML okolje. ES, ES-T in ES-C oblike elektronskega podpisa v XML okolju prikazuje spodnja slika. ES, ES-T in ES-C XML ekvivalentne oblike se imenujejo XAdES, XAdES-T, XAdES-C, ki W3C XML-Signature elementom (Signed Info, Signature, KeyInfo) dodajo elemente za zagotavljanje varnega elektronskega podpisa oz. celotne informacije za preverjanje digitalnega podpisa v skladu z EU priporočili.



Slika 3. - *Elektronski podpis s časovnim žigom in podatki za overjanje v XML obliki*

Tehnične podrobnosti realizacije posamezne oblike elektronskega podpisa so podane v W3C in ETSI priporočilih in standardih navedenih v poglavju 1.2.

3.1.3 XML shema digitalnega podpisa e-SLOG računa

Na osnovi analize mednarodnih standardov in priporočil, ter trenutne prakse v svetu, je za XML digitalni podpis e-SLOG računa predlagana shema XML digitalnega podpisa, skladna z W3C in XAdES (XAdES-EPES (Explicit policy based Electronic Signature) profil) priporočili, ki vsebuje vse bistvene elemente digitalnega podpisa, potrebne za ugotavljanje verodostojnosti podpisa, integritete podpisanih podatkov in identitete podpisnika.

V nadaljevanju je podan splošni opis verzije 1.4 e-SLOG sheme XML digitalnega podpisa (signature_1_4.xsd) in sheme XAdES razširitev (xades_1_4.xsd). Datoteki signature_1_4.xsd in xades_1_4.xsd z definicijami shem sta objavljeni na GZS spletnih straneh (http://www.gzs.si).

3.1.3.1 Splošni opis e-SLOG XML digitalnega podpisa

Digitalni podpis je vsebovan v <Signature> bloku. Glavni elementi strukture so:

- <SignedInfo> - XML-DSIG blok ki vsebuje informacije ki bodo podpisane
- <SignatureValue> - dejanski digitalni podpis
- <KeyInfo> - digitalno potrdilo uporabljeno digitalni podpis
- <Object> + <QualifyingProperties> - blok z XAdES razširitvami. Blok vsebuje:
    - <SignedProperties> - blok z dodatnimi podpisanimi podatki
    - <SignedSignatureProperties> - dodatne informacije za opis digitalnega podpis, ki so:
        - (<SigningTime>) - čas podpisa (lokalni čas računalnika na katerem je ustvarjen podpis)
        - (<SigningCertificate>) - podatki o digitalnem potrdilu uporabljenem za podpis (zgoščena vrednost potrdila, razločevalno ime overitelja, serijska številka)
        - (<SignaturePolicyIndentifier>) - podatki o politiki digitalnega podpisa
        - (<SignerRole>) - funkcija podpisnika
    - <SignedDataObjectProperties> - dodatne informacije o podpisanih podatkih, ki so:
        - <DataObjectFormat> - oblika podatkov oziroma pravila za prikaz

V verziji 1.4 sheme e-SLOG digitalnega podpisa ni predvidena uporaba ostalih XAdES <SignedProperties> elementov, ter <UnsignedProperties> elementov.

3.1.3.2 Kontrolni seznam skladnosti z e-SLOG XML shemo digitalnega podpisa

XML digitalni podpis ustvarjen skladno z e-SLOG XML shemo mora vsebovati najmanj sledeče elemente[1]:	
<Signature Id= >	☐
<SignedInfo>	☐
<CanonicalizationMethod Algorithm= >	☐
<SignatureMethod Algorithm= >	☐
(<Reference URI= Id= Type=>	☐
(<Transforms>	☐
<Transform Algorithm= >	☐
</Transforms>)?	
<DigestMethod Algorithm= />	☐
<DigestValue />…<DigestValue>	☐
</Reference>)+	
</SignedInfo>	
<KeyInfo>	☐
<X509Data>	☐
<X509Certicate />	☐
</X509Data>	
</KeyInfo>	
<Object>	☐
<QualifyingProperties xmlns= Target= >	☐
<SignedProperties Id= >	☐
<SignedSignatureProperties>	☐
<SigningTime />	☐
<SigningCertificate>	☐
<Cert>	☐
<CertDigest>	☐
<DigestMethod Algorithm= />	☐
<DigestValue />...<DigestValue>	☐
</CertDigest>	
<IssuerSerial>	☐
<X509IssuerName xmlns= />	☐
<X509SerialNumber xmlns= />	☐
</IssuerSerial>	
</Cert>	
</SigningCertificate>	
<SignaturePolicyIdentifier>	☐
<SignaturePolicyId>	☐
<SigPolicyId>	☐
<Identifier>…</Identifier>	☐
<Description>…<:Description>	☐
</SigPolicyId>	
<SigPolicyHash	☐
<DigestMethod Algorithm= … />	☐
<DigestValue>…<DigestValue>	☐
</SigPolicyHash>	
<SigPolicyQualifiers>	☐

[1] Elementi z praznim kontrolnim poljem (»☐« v zadnjem stolpcu) so vključeni zaradi preglednosti.

<SigPolicyQualifier>	☐
<SPURI>…</SPURI>	☐
</SigPolicyQualifier>	
</SigPolicyQualifiers>	
</SignaturePolicyId>	
</SignaturePolicyIdentifier>	
</SignedSignatureProperties>	
<SignedDataObjectProperties>	☐
<DataObjectFormat ObjectReference= >	☐
<Description>...<Description>	☐
<MimeType>...</MimeType>	☐
</DataObjectFormat>	
<SignedDataObjectProperties>	☐
</SignedProperties>	
</QualifyingProperties>	
</Object>	
<Signature>	

3.2. Priporočila uporabe kriptografskih algoritmov

V tema poglavju je podan priporočen nabor kriptografskih algoritmov za e-SLOG XML digitalni podpis. Pri Priporočila je bilo izdelano na osnovi ETSI posebnega poročila (ETSI SR 002 176 V1.1.1 2003-03, Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures) in v Sloveniji in v svetu uveljavljene prakse. ETSI posebno poročilo podaja predlog liste odobrenih algoritmov in pripadajočih parametrov, ter kombinacije algoritmov za kreiranje in verifikacijo digitalnega podpisa.

Algoritmi - priporočilo za ustvarjanje kriptografskih ključev

	Algoritem	Priporočena dožina ključa	Priporočena doba uporabe
končni uporabniki	RSA	1024	do 5 let
overitelji	RSA	1024 2048	do 5 let do 20 let

Algoritmi - priporočilo za ustvarjanje elektronskega podpisa

	Algoritem	Opomba
zgoščevalna funkcija	SHA-1	skladnen z FIPS PUB 180-1 and ANSI X9.30
digitalni podpis	RSA	skladnen z PKCS#1

4. SLOVAR IN POJMOVNIK

digitalno potrdilo - potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto

kvalificirano digitalno potrdilo – potrdilo v elektronski obliki, ki izpolnjuje zahteve iz 28. člena ZEPEP. Izda ga overitelj, ki deluje v skladu z zahtevami iz 29. do 36. člena ZEPEP

podatki za elektronsko podpisovanje – podatki za elektronsko podpisovanje so edinstveni podatki, kot so šifre ali zasebni šifrirni ključi, ki jih podpisnik uporablja za oblikovanje elektronskega podpisa (ZEPEP, 2.člen)

podatki za preverjanje elektronskega podpisa - edinstveni podatki, kot so šifre ali javni šifrirni ključi, ki se uporabljajo za preverjanje elektronskega podpisa (ZEPEP, 2.člen)

politika e-podpisa – zbirka pravil za ustvarjanje in preverjanje elektronskega podpisa. Določa tudi pogoje, pod katerimi je elektronski podpis veljaven.

overitelj - fizična ali pravna oseba, ki izdaja potrdila ali opravlja druge storitve v zvezi z overjanjem ali elektronskimi podpisi (ZEPEP, 2. člen)

podpisnik - oseba, ki ustvari ali je v njenem imenu in v skladu z njeno voljo ustvarjen elektronski podpis

elektronski podpis - niz podatkov v elektronski obliki, ki je vsebovan v, dodan k ali logično povezan z drugimi podatki, in je namenjen preverjanju pristnosti teh podatkov in identifikaciji podpisnika

varen elektronski podpis - 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

sredstvo za preverjanje elektronskega podpisa - nastavljena programska ali strojna oprema, ki se uporablja za preverjanje elektronskega podpisa (ZEPEP, 2. člen)

sredstvo za varno elektronsko podpisovanje - nastavljena programska ali strojna oprema, ki jo podpisnik uporablja za oblikovanje varnega elektronskega podpisa (ZEPEP, 2. člen)

5. PRILOGE

Dokument ne vsebuje prilog.

6. IZJAVA O SKLADNOSTI S TEMI PRIPOROČILI

Pričujoči dokument podaja priporočilo sheme XML digitalnega podpisa e-Slog računa. Za skladnost s temi priporočili jamči proizvajalec aplikacije.

Skladnost s temi priporočili lahko proizvajalec ugotovi na podlagi presoje, ki jo izvede sam, ali pa se za presojo obrne na tretjo stranko, ki je specializirana za takšne presoje. Ne glede na to, na kakšen način je proizvajalec ugotavljal skladnost, pa lahko le on poda izjavo o skladnosti s temi priporočili in s tem prevzame tudi morebitne obveznosti.

Podoben način zagotavljanja skladnosti je uveljavljen tudi v EU (CWA 14172-4).

7. DODATNI VIRI

[W3C]: XML Signature WG, http://www.w3.org/Signature/

[ETSI] ETSI - Electronic Signatures and Infrastructures http://portal.etsi.org/esi/el-sign.asp

[ZEPEP] Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP) http://objave.uradni-list.si/bazeul/URED/2000/057/B/522615430.htm

[Uredba] Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje http://www.gov.si/cvi/slo/ep/Uredba.htm