GOSPODARSKA ZBORNICA SLOVENIJE

IT SOLUTIONS & SERVICES

Projekt *e*-SLOG

Elektronsko poslovanje slovenskega gospodarstva

A2 – Priporočila za izdelavo varnostne politike e-podpisa

Verzija 1.0
junij 2004

STANJE DOKUMENTA

Namen dokumenta:	Dokument vsebuje opis in priporočila vsebine *Politike e-podpisa*
Kratek naziv projekta:	e-SLOG – e-podpis
Vsebina:	*Glej "Vsebina"*
Status:	Objavljena verzija
Verzija:	1.0
Datum verzije:	junij 2004
Avtorji:	S&T Hermes Pus d.d.
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@gov.si Dr. Alenka Žužek (CVI), alenka.zuzek@gov.si Rudi Ponikvar (S&T Hermes Plus), rudi.ponikvar@hermes-plus.si Tine Prislan (S&T Hermes Plus), tine.prislan@hermes-plus.si Roman Puhek (Crea), roman.puhek@crea.si Matej Trampuš (Crea), matej.trampus@crea.si Igor Lesjak (Crea), igor.lesjak@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 Vesna Ilič (IBM), vesna.Ilic@si.ibm.com Milan Spalevič (IBM), milan.spalevic @si.ibm.com
Zgodovina verzij:	*Glej "Verzija"*

Verzija	Datum spremembe	Opombe
1.0	10. junij 2004	

VSEBINA

1. UVOD

Zagotavljanje varnosti elektronskega poslovanja izpostavlja potrebo po razširitvi nabora podatkov, ki služijo kot osnova za oceno veljavnosti digitalnega podpisa. Elektronsko poslovanje omogoča določitev pogojev pod katerimi je digitalni podpis veljaven in postane zavezujoč v določenem poslovnem kontekstu. Pravila, kot so namen uporabe e-podpisa, tehnične zahteve, proceduralna pravila, odgovornosti, morebitne omejitve, itd., se zapišejo v poseben dokument – Politika e-podpisa.

1.1. Področje, namen in organizacija poglavja

V dokumentu navajamo:

- priporočila, ki opisujejo vsebino politike e-podpisa v tekstovni obliki.

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 praktična priporočila na podlagi mednarodnih standardov in priporočil, ki bodo ciljni publiki olajšala izdelavo politike e-podpisa.

Poglavje je organizirano na naslednji način**:**

- v nadaljevanju uvodnega dela navajamo priporočila in standarde, priporočila, ki urejajo področje politike e-podpisa;
- v poglavju 2 podajamo pravno analizo vloge politike e-podpisa v elektronskem podpisovanju;
- v poglavju 3 je podan povzetek vsebine in opis točk politike e-podpisa v okviru praktičnega kontrolnega seznama;
- terminološki slovar pojasnjuje pojme, ki se v poglavju uporabljajo.

1.2. Mednarodni standardi in priporočila

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 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 ETSI sodelujejo predstavniki uprave, operaterji, podjetja, ponudniki storitev, raziskovalne ustanove in uporabniki. ETSI igra tudi pomembno vlogo pri razvoju širokega spektra standardov in tehnične dokumentacije, ki predstavlja evropski prispevek k svetovni standardizaciji na področju telekomunikacijske in informacijske tehnologije. ETSI je uradno priznan s strani Evropske komisije in sekretariata EFTA. V nadaljevanju je naštetih nekaj ETSI priporočil 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.*

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.

2. PRAVNA ANALIZA

V predpisih na območju Republike Slovenije (Zakon o elektronskem poslovanju in elektronskem podpisu (Ur.l. RS, št. 57/2000, 30/2001), Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Ur.l. RS, št. 77/2000, 2/2001)), področje *Politike e-podpisa* ni posebej urejeno, zato se pričujoči dokument v skladu z Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Ur.l. RS, št. 77/2000, 2/2001), 2. člen, naslanja na standarde in priporočila, ki so splošno priznani v Evropski uniji.

> **2. člen**
> Ne glede na določbe drugih členov te uredbe, strojna in programska oprema ter postopki izpolnjujejo merila in pogoje po tej uredbi, če so v skladu s standardi, merili ali pogoji, ki so splošno priznani v Evropski uniji in objavljeni v Uradnem listu Evropskih skupnosti.

3. PRIPOROČILA ZA IZDELAVO POLITIKE ELEKTRONSKEGA PODPISA (E-PODPISA)

Politika e-podpisa je nabor pravil za ustvarjanje in preverjanje e-podpisa. Politika e-podpisa je lahko zapisana v formalni obliki, kot je ASN.1, ali pa v neformalni tekstovni (berljivi) obliki. Z njo morajo biti seznanjeni vsi udeleženci procesa (podpisnik-stranka, tretje osebe itd.) in jo morajo upoštevati tako v fazi ustvarjanja e-podpisa, kot tudi v fazi preverjanja. S tem zagotovimo, da lahko v slučaju spora, razsodnik preveri veljavnost e-podpisa in če je bil uporabljen skladno z dogovorjeno politiko.

Uporabniki morajo izkazati svojo soglasnost s pogoji politike e-podpisa. Soglasnost je lahko podana skozi sporazum med izdajateljem politike in uporabnikom ki priznava obveze, ki izhajajo iz politike e-podpisa. Politika e-podpisa je lahko vključena v podpisani dokument:

- eksplicitno, če obstaja politika v obliki dokumenta in je objavljena na način, ki omogoča eksplicitno sklicevanje nanjo;
- implicitno, če strani v poslovnem procesu vedno uporabljajo isto politiko in je privzeto oziroma dogovorjeno, da je podpis veljaven če je v skladu s to politiko, razen če je navedeno drugače. Implicitna referenca na določeno politiko e-podpisa se tako privzame če v e-podpisu, oziroma dokumentu, ni navedeno nasprotno, oziroma ni navedena referenca na drugo politiko e-podpisa. Politika e-podpisa je lahko implicitna tudi če je vgrajena v tehnična sredstva za ustvarjanje podpisa in tako transparenta za uporabnika.

Oseba, ki preverja e-podpis, mora pred preverjanjem poznati določila politike e-podpisa. Le-ta mora biti dostopna v tekstovni obliki ali predstavljena na način, ustrezen za avtomatsko procesiranje s strani sistema (npr. ASN.1, XML).

Iz *Politike e-podpisa* morajo biti razvidni pogoji pod katerih mora biti podpis ustvarjen in pod katerimi se preverja, da se

lahko sprejme kot veljaven.

V nadaljevanju je kot kontrolni seznam podan pregled vsebina *Politike e-podpisa* v tekstovni (berljivi) obliki.

3.1. Politika e-podpisa – kontrolna lista

☐ **Oblika politike e-podpisa.**

Politika e-podpisa je uporabljena v različnih fazah procesa. Z njo se mora seznaniti podpisnik, da se prepriča da je prava za namen in kontekst podpisa. V tej fazi mora biti politika na razpolago v berljivi obliki, tako da je lahko na razumljiv način prikazana podpisniku. Ko uporabnik izbere določeno politiko, mora biti v skladu z njo izveden elektronski podpis, kar pomeni, da mora biti politika na razpolago tudi v obliki, ki jo lahko uporabi aplikacija za ustvarjanje elektronskega podpisa.

Ko elektronsko podpisan dokument prejme stran kateri je bil namenjen, oziroma stran, ki preverja veljavnost podpisa, mora biti možno direktno, ali indirektno prepoznati katera politika je bila uporabljena v fazi ustvarjanja podpisa, tako da je lahko v skladu z njo izveden postopek preverjanja veljavnosti podpisa. Politika mora biti zopet na voljo v berljivi obliki, da jo lahko v razumljivi obliki prikazana osebi, ki preverja podpis in v obliki, ki jo lahko uporabi aplikacija s katero se podpis preverja.

To pomeni, da mora bit *Politika e-podpisa* na razpolago v sledečih oblikah:
- v obliki razumljivi ljudem, oziroma berljivi obliki
- v obliki, primerni za procesiranje s strani aplikacij. V ta namen, je politika lahko vgrajena v samo aplikacijo, ali pa na voljo v primerni obliki (na primer RFC3125 ASN.1 obliki).

☐ **Splošne informacije.**

Sekcija vsebuje sledeča polja:
- identifikacijska oznaka (Signature Policy Indentifier), ki vsebuje edinstveno oznako politike e-podpisa;
- datum izdaje;
- ime izdajatelja;
- področje uporabe politike, ki vsebuje splošne zakonske in pogodbene pogoje, ter kontekst in namen uporabe e-podpisa po pričujoči politiki;
- dodatna razširitvena polja (če je potrebno), ki vsebujejo ostale informacije v zvezi z uporabo e-podpisa v kontekstu pričujoče politike.

☐ **Preverjanje e-podpisa.**

Prejemnik elektronsko podpisanega dokumenta je obvezen preveriti veljavnost e-podpisa preden uporabi dokument, ali informacije iz dokumenta. Stran ki preverja veljavnost e-podpisa (npr. prejemnik) zbere podatke potrebne za preverjanje veljavnosti digitalnih potrdil in e-podpisa.

Preverjanje podpisa je lahko izvedeno interaktivno (aktivno sodelovanje prejemnika), ali pa avtomatizirano (vgrajeno v informacijski sistem). Politika e-podpisa mora vsebovati sekcijo *Politika preverjanja e-podpisa* z opisom predpisanega postopka preverjanja veljavnosti e-podpisa.

☐ **Politika preverjanja e-podpisa.**

Politika preverjanja e-podpisa določa pravila, ki jih je potrebno upoštevati za preverjanje veljavnosti e-podpisa. Določa katere podatke mora podpisnik vključiti v e-podpis in katere podatke mora stran ki preverja e-podpis preveriti, da se lahko privzame da je e-podpis potencialno veljaven.

V politiko se lahko vključi pravila za nabor dokumentov. V tem primeru se poda skupna pravila za vse dokumente, ter pravila specifična za določen dokument, ali določen namen (prevzeto obvezo) e-podpisa.

*Politika preverjanja e-podpis*a lahko vsebuje:
- nabor pravil, ki so skupna za vse dokumente in namene; in
- nabor pravil, ki so specifična za določen dokument, ali namen.

Vsebina *Politike preverjanja e-podpisa* je napisana kot:
- nabor pravil, ki so skupna za vse dokumente in namene. Ta pravila določajo pogoje zaupanja v digitalna potrdila, časovni žig in atribute, skupaj z morebitnimi omejitvami glede atributov, ki smejo biti vključeni v e-podpis.
- nabor pravil za določen dokument in namen, ki določajo pogoje zaupanja v digitalna potrdila, časovni žig in atribute, skupaj z morebitnimi omejitvami glede atributov, ki smejo biti vključeni v e-podpis.

☐ Podatki za preverjanje e-podpisa.

Izdajatelj politike e-podpisa določi kateri podatki morajo biti, oziroma so lahko vključeni v e-podpisa in katera pravila morajo biti upoštevana. Med podatke za preverjanje e-podpisa sodijo:
- pravila za uporabo oziroma priznavanje overiteljev;
- pravila ki se tičejo uporabniških digitalnih potrdil (npr. veljavni OID-ji politik overiteljev pod katerimi so bili izdani);
- pravila za ugotavljanje ali je bil e-podpis ustvarjen v času, ko je bilo digitalno potrdilo veljavno (npr. z uporabo časovnega žiga ali oznake);
- obdobje opreznosti (npr. politika lahko določi, da je podpis veljavne šele po preteku določenega časa, po katerem se lahko z visoko verjetnostjo trdi, da je bilo digitalno potrdilo v času podpisa veljavno);
- pravila za preverjanje statusa digitalnih potrdil (npr. uporaba CRL);
- pravila za zaščito e-podpisa v primeru razkritja overiteljevega ključa, ali slabosti uporabljenih algoritmov;
- pravila za okolje, ki ga mora uporabljati podpisnik (npr. obvezna uporaba pametne kartice, protivirusna zaščita, ...);
- podatki, ki jih mora pridobiti stran, ki preverja veljavnost podpisa;
- morebitne omejitve uporabe algoritmov in dolžine ključev;
- pravila za vloge (funkcije) podpisnikov;
- zahteve za preverjanje verige zaupanja med digitalnimi potrdili (certificate chain).

☐ Identifikacijska oznaka politike e-podpisa

Edinstvena identifikacijska oznaka je potrebna za razločevanje med politikami v določenem poslovnem kontekstu. Izdajatelj lahko da podpisniku le identifikacijsko oznako politike, ali pa oznako in politiko. Ker v določenih primerih ni praktično dajati celega dokumenta, se lahko navede le kazalec na dokument, oziroma lokacijo kjer se politika nahaja. V tem primeru ni dovolj, da damo uporabniku le identifikacijsko oznako (OID). Za nedvoumno identifikacijo politike, je potrebno podati zgoščeno vrednost (hash) politike e-podpisa in oznako uporabljenega algoritma zgoščevalne funkcije.,

Informacije, ki podajajo referenco na politiko e-podpisa tako tipično vsebujejo:
- edinstven OID politike e-podpisa;
- URL kazalec na dokument, ali lokacijo kjer se nahaja kopija politike e-podpisa;
- zgoščeno vrednost (hash) politike e-podpisa;
- oznako uporabljenega algoritma zgoščevalne funkcije.

☐ Objava politike e-podpisa

Politika e-podpisa mora biti v času veljavnosti objavljena na način, ki omogoča da je dostopna vsem stranem v procesu (uporabnikom ki podpisujejo in uporabnikom ki preverjajo veljavnost podpisa). Politika e-podpisa se

običajno objavi na spretni strani in je lahko dostopna preko http, ali https protokola. Obstajati mora tudi način, na katerega lahko uporabnik ugotovi, da je politika avtentična. Nekaj najbolj pogostih oblik objave politike:

- politika je objavljena na strežniku, do katerega je možen dostop preko protokola SSL;
- besedilo politike je vgrajeno v aplikacijo, ki ji uporabnik zaupa in katere izvor pozna;
- »tradicionalna« različica politike je natisnjena na papirju in potrjena z žigom ali navadnim podpisom;

☐ **Arhiviranje politike e-podpisa**

Politika e-podpisa mora biti dostopna tudi po poteku veljavnosti. Izdajatelj mora v ta namen zagotoviti ustrezen arhiv in ga navesti v politiki. Izdajatelj mora v primeru prenehanja delovanja zagotoviti, da druga organizacija prevzame skrb za upravljanje arhiva njegovih politik.

☐ **Avtentikacija politike e-podpisa**

Podpisnik, oziroma uporabnik *Politike e-podpisa* se mora prepričati, da uporablja pravo politiko. To se lahko zagotovi tako, da jo pridobi iz zaupanja vrednega vira, ali pa iz nezaupanja vrednega vira, če je politika podpisana. Ko se prepriča v avtentičnost vira lahko preveri zgoščeno vrednost (hash) politike in jo uporabi kot verodostojen dokument. Izdajatelj mora zagotoviti dostopnost *Politike e-podpisa* v skladu z opisom v točki Objava politike e-podpisa.

4. TERMINOLOŠKI SLOVAR

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)

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)

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

izdajatelj politike e-podpisa – subjekt, ki določi tehnične in proceduralne zahteve za ustvajanje in preverjanje e-podpisa za določene poslovne potrebe

politika preverjanja e-podpisa – del politike e-podpisa, ki določa tehnične zahteve za ustvarjanje in preverjanje e-podpisa

časovni žig - podatkovni objekt, ki povezuje podatek, ki je bil preoblikovan s kriptografskimi algoritmi, s točnim časom, s čimer je vzpostavljen dokaz, da je podatek obstajal pred tem časom

5. PRILOGE

Dokument ne vsebuje prilog.

6. IZJAVA O SKLADNOSTI S TEMI PRIPOROČILI

Pričujoči dokument podaja priporočilo vsebine *Politke e-podpisa* v berljivi obliki. Dokument ne podaja strogo formalizirane oblike in strogih tehničnih zahtev, ki bi lahko bili podlaga za formalno presojo. Zaradi kompleksnosti e-poslovanja, raznolikosti okolij v katerih se uporablja in posledično širokega nabora možnosti, je najbolj smiselno, da za skladnost jamči izdajatelj *Politike e-podpisa*.

Skladnost s temi priporočili lahko izdajatelj *Politike e-podpisa* 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

[RFC3125]: RFC 3125 Electronic Signature Policies, http://www.ietf.org/rfc/rfc3125.txt

[ETSI] ETSI - Electronic Signatures and Infrastructures http://portal.etsi.org/esi/el-sign.asp
- ETSI TR 102 041 V1.1.1 (2002-02) Signature Policy Report

[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