ARHIVIRANJE DIGITALNO PODPISANIH ELEKTRONSKIH DOKUMENTOV

Alenka Žužek [*], *Aleš Dobnikar* [**]

UDK: 930.253:004.3

***Alenka Žužek, Aleš Dobnikar: Arhiviranje digitalno podpisanih elektronskih dokumentov**. Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja. Zbornik referatov z dopolnilnega izobraževanja, Maribor 1/2002, št. 1, str. 269 – 277.*

Izvirnik v slovenščini, izvleček v slovenščini in angleščini, povzetek v angleščini.

Elektronski način izmenjave dokumentov postaja prevladujoči način poslovanja oz. komuniciranja, tako za poslovne kot tudi za zasebne namene. Elektronsko poslovanje in komuniciranje prinaša veliko prednosti, vse večja pa postaja potreba po zagotavljanju varnosti podatkov in resnične identitete oseb v medsebojnem komuniciranju. V prispevku si bomo podrobneje ogledali problematiko in predstavili smernice za rešitev.

UDC: 930.253:004.3

***Alenka Žužek, Aleš Dobnikar: Long-term Management of Electronically-signed Documents**. Technical and Field Related Problems of Traditional and Electronic Archiving. Conference Proceedings, Maribor 1/2002, No. 1, pp. 269 – 277.*

Original in Slovenian, abstract in Slovenian and English, summary in English.

The rapid development of information technologies has dramatically changed the way how government authorities, corporations and individuals communicate and carry out their daily activities. The paper summerizes the most promising recommendations to ensure that electronically-signed records are accessible as long as they are needed.

1. UVOD

Zagotavljanje ustrezne varnosti podatkov in resnične identitete oseb v medsebojnem komuniciranju na elektronski način v Republiki Sloveniji urejata predvsem Zakon o elektronskem poslovanju in elektronskem podpisu (Ur.l. RS, št. 57/2000) in Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Ur. l. RS, št. 77/2000 in 2/2001). Bistveni pomen zakona je, da pod posebnimi pogoji elektronskemu podpisu priznava enako veljavo, kot jo ima v papirnatem svetu lastnoročni podpis. Varno elektronsko poslovanje, tako interno v državni oz. javni upravi, kot širše, na nivoju storitev, ki jih javna uprava nudi državljanom in pravnim osebam, omogoča vzpostavitev infrastrukture digitalnih potrdil (angl. *digital certificate*) javnih ključev, s katerimi upravlja overitelj na Centru Vlade Republike Slovenije za informatiko (CVI).

[*] ***Dr. Alenka Žužek, Center Vlade Republike Slovenije za informatiko, Langusova 4, 1000 Ljubljana, Slovenija.***

[**] ***Aleš Dobnikar, Center Vlade Republike Slovenije za informatiko, Langusova 4, 1000 Ljubljana, Slovenija.***

Digitalna potrdila predstavljajo sodobno obliko osebnih identifikatorjev v elektronskem okolju. Nudijo dve osnovni možnosti za zasebnost v elektronskem poslovanju oz. komuniciranju:

- šifriranje podatkov zagotavlja zaupnost in nadzor nad dostopom do podatkov,
- digitalni podpis predstavlja digitalno alternativo klasičnemu podpisu.

Digitalna potrdila overitelja na CVI seveda predstavljajo šele tehnološki pogoj za legitimnost e-poslovanja oz. e-komuniciranja. Šele zavedanje prednosti, ki jih nudi e-komuniciranje v najširšem pomenu besede, bo porok k globalnemu pristopu po formalizaciji in posodabljanju notranjih in zunanjih postopkov in čim hitrejšemu in uspešnejšemu prehodu iz klasičnega v e-poslovanje.

Tehnologija digitalnih potrdil in elektronskega poslovanja pa prinaša tudi določene slabosti. Digitalna potrdila in posledično tudi ključi, ki so v njih vsebovani, imajo omejeno življenjsko dobo. Stopnja varnosti ključa se s starostjo zmanjšuje. Iz tega razloga imajo digitalna potrdila omejeno obdobje veljavnosti, znotraj katerega je možnost zlorabe minimalna. Časovna omejenost uporabe digitalnih potrdil pa vpliva na varnost elektronskih dokumentov, ki jih je potrebno hraniti dlje, kot je obdobje veljavnosti digitalnih potrdil.

Problem hranjenja dokumentov za več let, ali celo trajno povzroča poleg časovne omejenosti uporabe digitalnih potrdil tudi omejitve uporabe informacijskega sistema, tj. izpad medija, kjer se podatki shranjujejo, in zastarelost strojne in programske opreme. Za dolgoročno shranjevanje dokumentov na zanesljiv in varen način je potrebno zagotoviti:

- zanesljivost vsebine dokumenta,
- avtentičnost dokumenta in subjekta, ki je dokument ustvaril,
- celovitost oz. garancijo, da dokument ni bil spremenjen delno ali v celoti,
- uporabnost oz. berljivost dokumenta ter v primeru podpisanih dokumentov tudi verifikacijo podpisa v daljšem ali trajnem časovnem obdobju,
- pravno veljavnost arhiviranega dokumenta.

Za zagotavljanje teh pogojev, tako v svetu kot pri nas, še ni tehnološko dorečenih enostavnih rešitev oz. standardov, posledično pa tudi ne pravnih oz. zakonskih podlag, ki bi na splošno oz. globalno določale načine in pravno veljavo arhiviranja elektronskih dokumentov. Po drugi strani pa že izvajajo različne iniciative in priporočila, tako za tehnološki kot pravni vidik, arhiviranja elektronskih dokumentov. Mednje sodita na primer ZDA in Avstralija [1,2].

V prispevku sledi predstavitev overitelja digitalnih potrdil na CVI, ki nudi tehnološki pogoj za legitimnost e-poslovanja oz. e-komuniciranja. V 3. poglavju je podrobneje predstavljena problematika arhiviranja elektronskih dokumentov s smernicami za rešitev. Na koncu so na kratko predstavljena priporočila oz. standardi.

2. OVERITELJ DIGITALNIH POTRDIL NA CVI

Digitalno potrdilo je sodobna alternativa klasičnim osebnim identifikatorjem in bo tako v razvitih družbah, kot tudi pri nas, kmalu zamenjal klasične osebne identifikatorje. Digitalno potrdilo vključuje bistvene podatke o imetniku, njihovo verodostojnost pa zagotavlja digitalni podpis izdajatelja potrdila – to je overitelja

(angl. CA: *Certification Authority*, tudi PKI: *Public Key Infrastructure* oz. TTP: *Trusted Thirth Party*).

Overitelj digitalnih potrdil na CVI je overitelj kvalificiranih digitalnih potrdil, za katere velja najvišja stopnja varovanja in načela t.i. močne enkripcije in deluje v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP) in objavljenimi politikami delovanja. Overitelja na CVI sestavljata dva izdajatelja digitalnih potrdil [7]:

- SIGOV-CA (Slovenian GOVernmental Certification Authority) za institucije javne uprave ter
- SIGEN-CA (Slovenian GENeral Certification Authority) za pravne in fizične osebe.

Kvalificirana digitalna potrdila overitelja na CVI so namenjena:

- za upravljanje s podatki javne uprave,
- za dostop in izmenjavo podatkov, s katerimi upravlja javna uprava,
- za varno elektronsko komuniciranje med imetniki kvalificiranih digitalnih potrdil overitelja in
- za storitve oz. aplikacije, za katere se zahteva uporaba digitalnih potrdil overitelja na CVI.

Overitelj na CVI izdaja dve vrsti digitalnih potrdil, osebna in spletna, med katerima obstajajo specifične razlike, pogojene z namenom uporabe. Le-to omogoča posebna tehnologija in specifične lastnosti programske opreme ter infrastrukture. Medtem ko pripada spletnim digitalnim potrdilom en par ključev (javni in zasebni), pripadajo osebnim digitalnim potrdilom dva ločena para ključev - za digitalno podpisovanje oz. overjanje ter za šifriranje oz. dešifriranje. Vsak par sestavljata zasebni in javni ključ. Pri tem javnost ključa pomeni, da je le-ta javno dostopen oz. objavljen v t.i. javnem imeniku, zasebnost pa, da ima dostop do tega ključa samo imetnik digitalnega potrdila.

Digitalno potrdilo je računalniški zapis, ki vsebuje podatke o imetniku (ime, naslov in podobno), njegov javni ključ ter podatke o overitelju digitalnega potrdila in obdobje veljavnosti. Slika 1 prikazuje zgled digitalnega potrdila. Potrdilo je izdal SIGOV-CA, s svojim digitalnim podpisom pa jamči za istovetnost podatkov v potrdilu (na sliki označeno s CA). Potrdilo izkazuje povezavo med imetnikom in njegovim javnim in zasebnim ključem. Javni ključ je del potrdila ("67C8 783D ..."), zasebni ključ mora imetnik varno hraniti pri sebi.

Digitalna potrdila omogočajo izvedbo šifriranja in digitalnega podpisovanja dokumentov. S šifriranjem se zagotovi zaupnost in nadzor nad dostopom do podatkov, digitalni podpis pa predstavlja digitalno alternativo klasičnemu podpisu, pomeni pa nezatajljivost podpisnika, celovitost in avtentičnost. Digitalni podpis, izveden s pomočjo kvalificiranega digitalnega potrdila overitelja na CVI, ima enako veljavo, kot jo ima v papirnatem svetu lastnoročni podpis. Prav zato pa je potrebno ustvariti pravno in tehnološko okolje za zagotavljanje možnosti verifikacije podpisanih dokumentov tudi za trajno hranjene dokumente.

Slika 1 - Digitalno potrdilo

Slika 2 - Digitalno podpisan dokument

2.1 DIGITALNO PODPISANI DOKUMENTI

Ko želi imetnik digitalnega potrdila digitalno podpisati nek dokument, uporabi za to svoj zasebni ključ za podpisovanje. Digitalni podpis se izvede tako, da se najprej po posebnem postopku naredi t.i. "seštevek" sporočila - zgoščena vsebina (ki zagotavlja, da sporočila kasneje ni mogoče spremeniti, saj bi ta seštevek ne bil več isti), to število pa je potem zašifrirano z zasebnim ključem podpisnika. Ker svoj zasebni ključ pozna izključno samo imetnik, je to jamstvo, da je podpis res njegov.

Digitalno podpisan dokument predstavlja naslednji zgled. Ana Novak, imetnica digitalnega potrdila s Slike 1, želi digitalno podpisati pismo podjetju "St. Inf." in s tem zagotoviti nedvoumnost izvora dokumenta. Slika 2 prikazuje digitalno podpisano pismo. Verifikacija njenega podpisa je uspešna, če je njeno digitalno potrdilo veljavno. Veljavno mora biti njeno digitalno potrdilo, pa tudi potrdilo izdajatelja.

3. ARHIVIRANJE ELEKTRONSKIH DOKUMENTOV

Podatki v elektronski obliki, ki se izmenjujejo z elektronsko pošto, so del podatkovnih baz, spletnih strani in drugih informacijskih sistemov, niso pomembni samo trenutno, ob nastanku oz. neposredni uporabi. Predstavljajo lahko pravno, finančno, administrativno, kulturno in še kako drugače pomemben zapis oz. dokument za poslovanje neke organizacije.

Podatke je potrebno hraniti in ohranjati berljive različno dolgo. Nekatere dokumente je potrebno hraniti nekaj let, nekaj desetletij, obstajajo pa seveda tudi podatki, ki zahtevajo trajno hranjenje. Dolgotrajno ali celo trajno ohranjanje dokumentov v elektronski obliki postavlja celo vrsto vprašajev, na katera bo potrebno s pomembnostjo podatkov, ki nastajajo na elektronski način, čimprej najti odgovore. Znani so primeri izgube podatkov NASA, podatkov o toksičnih odpadkih v New Yorku [8], izguba tisočih podatkovnih baz bivših vzhodnonemških vladnih arhivov [4] itd.

Izguba hranjenih elektronskih podatkov oz. njihova nedostopnost je lahko posledica različnih faktorjev:

1. izpad oz. kvarljivost medijev, na katerih se podatki ohranjajo,
2. staranje programske in strojne opreme, na katerih so podatki nastali,
3. problem dokazovanja njihove avtentičnosti zaradi omejene življenjske dobe ključev oz. digitalnih potrdil,
4. človeške napake in napake strojne in programske opreme,

5. računalniški virusi, zunanji dogodki (potres, požar, ...).

Rešitve, ki bodo omogočale dolgoročno ohranjanje elektronskih dokumentov na zanesljiv in varen način, morajo zagotoviti, 0:

- **zanesljivost:** dokument mora ohraniti zanesljivost vsebine za verodostojno predstavitev aktivnosti, transakcije in drugih lastnosti,
- **avtentičnost:** ohraniti se mora avtentičnost zapisa, kdo ga je kreiral in posredoval. Določiti je potrebno politiko in postopke, po katerih se preverja nastanek, prenos, prevzem in upravljanje z dokumentom. Preprečiti se mora možnost spreminjanja dokumenta, brisanja ipd.
- **celovitost**: dokument ni bil spremenjen. Potrebno preprečiti nepooblaščene in beležiti ostale dostope do dokumenta;
- **uporabnost**: dokument mora biti dostopen in berljiv. Ohraniti se mora povezanost dokumenta z morebitnimi drugimi dokumenti ali aktivnostmi;
- **pravno veljavnost** arhiviranega dokumenta. V nadaljevanju si podrobneje oglejmo smernice trenutno znanih rešitev.

3.1 IZPAD MEDIJEV IN ZASTARANJE STROJNE IN PROGRAMSKE OPREME

Medij za hranjenje elektronskih podatkov, tj. trdi diski, zgoščenke, trakovi niso tako zanesljivi kot klasični nosilci podatkov in njihovo staranje je dosti hitrejše, kot je na primer življenjska doba mikrofilma.

Za razliko od dokumenta na papirju potrebuje dokument v elektronski obliki ustrezno strojno, kot tudi programsko opremo. Podatki nastajajo v različnih formatih in za njihovo berljivost potrebujemo ustrezna programska okolja ustreznih različic. Nenehne izboljšave strojne in programske opreme lahko povzročijo njihovo zastaranje v zelo kratkem času. Diskete velikosti "5.25", ki smo jih uporabljali v zgodnjih 90-ih letih v programih pod operacijskem sistemom MS DOS, so danes že zastarele in jih je težko najti ali celo uporabljati v današnjih računalnikih. Podatki izpred desetih let so danes tako rekoč nedostopni. Problem zastaranja opreme je v primerjavi z napakami medijev težje predvidljiv in temu primerna so tudi zagotovila trenutnih rešitev.

Rešitve

Za zmanjšanje možnosti napak medijev je potrebno izbirati visoko zanesljivo tehnologijo (namesto trakov, na primer zgoščenke) ter medij hraniti v optimalnem okolju (temperatura, vlažnost, ..). Arhivska baza lahko uporablja visoko zanesljive medije, lahko pa zanesljivost poveča z varnostnimi kopijami oz. distribucijo baze na različne lokacije, z rednim nadzorom za odpravo morebitnih napak. Odločitev med obema rešitvama je odvisna od cene in zanesljivosti, ki jo mora izvedba zagotoviti.

Zastarelost opreme je velik problem in odprava tega problema se lahko rešuje na različne načine:

- z ohranjanjem programske in strojne opreme v "računalniških muzejih",
- z "emulacijo" zastarele opreme na novejših "platformah" na nivoju strojne opreme, operacijskih sistemov, programske opreme in formata podatkov,
- z migracijo podatkov na novejšo tehnologijo,

- z arhiviranjem podatkov v predpisanih, prenosljivih formatih, t.j. najmanj občutljivih na strojno in programsko opremo (na primer "TXT" ali "XML").

V vseh zgoraj navedenih rešitvah je potrebno zadostiti zahtevam po ohranjanju vsebinskih, kontekstnih in strukturnih lastnosti dokumentov.

Perspektiven je koncept arhiviranja podatkov v predpisanem formatu. Najbolj razširjen format je Extensible Markup Language "XML", ki postaja "de facto" standard aplikacij e-poslovanja, za katere je potrebno zagotoviti varnost in zaupanje. Ta koncept pričenjajo uporabljati, na primer Nacionalni Arhivi Avstralije. Podatke, ki jih morajo shranjevati, prevedejo v "XML", za shranjevanje slikovnega materiala pa uporabljajo format "PNG" 0. Podobno je mehanizem vključen tudi v nekatere komercialne produkte, na primer Archive (http://www.archive.com/default.asp).

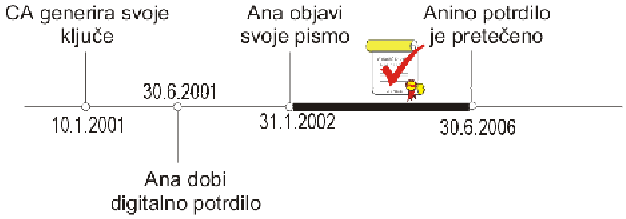
Raziskave tega perečega tehnološkega problema potekajo tudi v univerzitetnem okolju, omenimo projekt na Univerzi Stanford, ZDA. Projekt zajema raziskave različnih konfiguracij arhivskega skladišča glede na zanesljivost in ceno. Rezultati so zajeti v orodju Stanford Arhival Vault (SAV) [9], testnem okolju ArchSim, [9] in KASTS [8].

3.2 VELJAVNOST DIGITALNO PODPISANIH DOKUMENTOV

Digitalna potrdila in posledično tudi ključi, ki so v njih vsebovani, imajo omejeno življenjsko dobo. Stopnja varnosti ključa se namreč zmanjšuje s starostjo ključa. Prvič, ker lahko nekdo ukrade zasebni ključ, ki ga imetnik hrani sicer varno pri sebi, na primer na pametni kartici, drugič pa se lahko zasebni ključi razkrije po preteku določenega časa, ko se izboljšajo kriptoanalitične metode in postanejo računalniki zmogljivejši. Današnji ključi RSA, dolžine 1024-bitov, ki danes zagotavljajo visoko stopnjo varnosti, bodo lahko čez deset let precej enostavni za razkritje.

Iz tega razloga imajo digitalna potrdila omejeno obdobje veljavnosti, znotraj katerega je možnost zlorabe minimalna. Časovna omejenost uporabe digitalnih potrdil pa vpliva na varnost elektronskih dokumentov, ki jih je potrebno hraniti dlje, kot je obdobje veljavnosti digitalnih potrdil.

Za uspešno verifikacijo digitalnega podpisa morata biti vzpostavljeni dve povezavi: (*i*) enolična povezava med imetnikovim zasebnim ključem za podpis in njegovim javnim ključem za verifikacijo (v digitalnem potrdilu) ter (*ii*) imetnikovim digitalnim potrdilom in izdajateljem tega potrdila (SIGOV-CA oz. overitelja na CVI). Preverjanje digitalnega podpisa je uspešno, če lahko dokažemo, da je bilo kreirano z veljavnim in nepreklicanim digitalnim potrdilom.



Slika 3 - Časovni potek uporabe digitalnega potrdila

Oglejmo si življenjski cikel digitalno podpisanega dokumenta na zgledu Aninega pisma (Slika 2).

Slika 3 prikazuje enega izmed možnih časovnih potekov Aninega potrdila. Uspešna in varna verifikacija podpisa je odvisna od časa nastanka dokumenta in podpisa, postane pa negotova, ko Ani potrdilo poteče (30. junija 2006). Neuspešnost verifikacije bi lahko nastopila tudi pred pretekom njenega potrdila, npr. v primeru kraje njenega zasebnega ključa. Ana bi morala svoje potrdilo preklicati in od takrat naprej bi bila verifikacija njenega podpisa neuspešna.

Rešitve

Arhivi morajo za trajno hranjenje zagotoviti avtentičnost dokumenta. Zagotoviti morajo možnost nedvoumne preverbe izvora dokumenta oz. avtorstva tako dolgo, kot je potrebna njihova hramba. Nadalje morajo arhivi elektronske dokumenti zavarovati pred nepooblaščenim spreminjanjem ali brisanjem.

Za trajno hranjenje digitalno podpisanih dokumentov je potrebno zagotoviti tehnično in pravno verodostojno verifikacijo digitalnega podpisa, da je bil dokument nedvoumno podpisan v času veljavnega in nepreklicanega digitalnega potrdila.

Ohranjanje digitalno podpisanih dokumentov se lahko zagotovi na dva načina, 0:

1. *Hranijo se podatki o verifikaciji podpisa*: za vsak dokument se ob njegovem nastanku ali pa kmalu zatem izvede verifikacija, dokazilo o zanesljivo opravljeni verifikaciji pa se hrani kot atribut tega dokumenta. Poleg tega je pristop manj občutljiv na zastarelost opreme, zato je primeren za dokumente, ki zahtevajo trajno hranjenje.
2. *Možnost kasnejše verifikacije podpisa:* poleg dokumenta samega je potrebno ohranjati tudi možnost kasnejše verifikacije podpisa. V ta namen je potrebno ohranjati vse, kar je potrebno za verifikacijo:

- digitalno potrdilo javnega ključa za verifikacijo podpisa,
- listo preklicanih potrdil, ki ustreza času nastanka digitalnega podpisa,
- potrdilo overitelja in politiko delovanja itd.

Zaradi večje odvisnosti od strojne in programske opreme v času nastanka dokumenta je pristop manj primeren za trajno hranjenje dokumentov.

Slika 4 - Veljavnost digitalnega podpisa s časovnimi žigi

Rešitve problema varne verifikacije vključujejo pretežno tehnologijo časovnega žigosanja. Časovni žig potrjuje obstoj digitalnega podpisa ob določenem času. Dodeli ga zaupanja vredna ustanova (angl. TSA: *time-stamp authority*). Tretja stran, ki

podpis verificira, je lahko z visoko stopnjo zaupanja prepričana, da je podpisan dokument obstajal pred navedenim časom.

Ena izmed metodologij za ohranjanje možnosti verifikacije podpisa je KASTS 0. Za verodostojno verifikacijo podpisa tudi po preteku ključev in potrdila, se časovno ožigosa hranjen dokument (prikazano na Sliki 4), kot tudi ostale podatke, ki so potrebni za verifikacijo. Časovne žige je potrebno obnavljati skladno s stopnjo varnosti, ki jo lahko zagotavljajo. Podoben princip predvidevajo tudi komercialni produkti, na primer Archive (http://www.archive.com/default.asp), Cuculus (http://www.cyber.ee/research/cuc-feat.html). Namesto časovnega žiga se lahko veljavnost podpisa podaljšuje tudi z žigi drugih ustanov, na primer notarjev oz. arhivov.

5. PREGLED PRIPOROČIL IN STANDARDOV

V svetu, kot pri nas, še ni tehnološko dorečenih enostavnih rešitev oz. standardov, posledično pa tudi ne pravnih oz. zakonskih podlag, ki bi na splošno oz. globalno določale načine in pravno veljavo arhiviranja elektronskih dokumentov. Izvajajo pa se že različne iniciative in priporočila, tako za, tehnološki kot pravni vidik arhiviranja elektronskih dokumentov. Del trenutnega stanja v svetu je opisan v nadaljevanju:

Med aktivnimi vladnimi institucijami sta na primer Združene države Amerike in Avstralija:

- "National Archives and Records Administration" - ZDA je izdala priporočila vladnim službam pri upravljanju z arhivskimi podatki, 0. Priporočilo vključuje tudi zahteve za digitalno podpisane dokumente.
- "Department of defence" (DoD) - ZDA je z "National Archives and Records Administration" določil standard DoD 5015.2-STD. Določa osnovne tehnološke in pravne zahteve, ki jih morajo izpolnjevati aplikacije za upravljanje z arhivskimi podatki institucij DoD (http://jitc.fhu.disa.mil/recmgt).
- Avstralija je na podlagi svojega standarda AS 4390 (1996) "*Records Management*" v preteklem letu izdala priporočilo za design in implementacijo, *DIRKS: A Strategic Approach to Managing Business Information* (September 2001). Med aktivnejšimi avstralskimi zveznimi državami je Viktorija, ki je že sprejela svoj standard, "Standard for the Management of Electronic Records PROS 99/007, 2000 (http://www.prov.vic.gov.au/vers). Osnova za novi standard ISO 15489, "International Records Management Standard", je avstralski standard AS 4390 (1996).

Po priporočilih Evropske unije (standard ETSI TS 733 V1.2.2, [6] se za trajno hranjenje digitalno podpisanih dokumentov priporoča uporaba časovnih žigov in hranjenje vseh podatkov, potrebnih za verifikacijo (opisano v pogl. 4).

Iniciative za raziskavo področja pa prihajajo tudi iz drugih (nevladnih) sektorjev. Cilj mednarodnega raziskovalnega projekta InterPARES (http://www.interpares.org/draft_reports.htm), v katerega so vključeni raziskovalci univerz, pa tudi nacionalnih arhivov iz ZDA, Italije, Kanade, Avstralije, idr., je določiti teoretično in metodološko znanje, potrebno za uspešnost trajnega ohranjanja elektronskih dokumentov ter na podlagi tega določiti politike, metode in standarde.

6. ZAKLJUČEK

Za zagotavljanje pogojev za trajno hranjenje elektronskih dokumentov, tako v svetu kot pri nas, še ni tehnološko dorečenih enostavnih rešitev oz. standardov, posledično pa tudi ne pravnih oz. zakonskih podlag, ki bi na splošno oz. globalno določale načine in pravno veljavo arhiviranja elektronskih dokumentov. Po drugi strani pa se v svetu izvajajo različne iniciative in priporočila, tako za tehnološki kot pravni vidik arhiviranja elektronskih dokumentov.

Tudi v slovenskem prostoru se zavedamo, da bo potrebno zelo hitro rešiti in zagotoviti pravno in tehnično podlago za hranjenje dokumentov v elektronski obliki. Povezati je potrebno strokovnjake različnih področij, tako z vsebinskega kot pravnega in tehničnega stališča. Rešitve in zakonodajo pa bo potrebno določiti skladno s standardi Evropske unije, "International Records Management Standard" idr.

LITERATURA:

(1) *National Archives and Records Administration: Records Management Guidance for Agencies Implementing Electronic Signature Technologies, oktober, 2000, (http://www.nara.gov/records/policy/gpea.html).*

(2) *National Archives of Australia: Recordkeeping Metadata Standard for Commonwealth Agencies, 2001 (http://www.naa.gov.au/recordkeeping/er/manage_er/contents.html).*

(3) *Records Management Application (RMA) Compliance Testing (http://jitc.fhu.disa.mil/recmgt/).*

(4) *Boža Javornik: Revidiranje delovanja kontrol za zagotavljanje verodostojnosti elektronskih izvirnikov, 9. Konferenca o revidiranju in kontroli informacijskih sistemov, str. 25-45, september 2001.*

(5) *Projekt InterPARES, oktober 2001. (http://www.interpares.org/draft_reports.htm).*

(6) *Electronic signature format, ETSI TS 733 V1.2.2 (2000-12) (http://www.ict.etsi.org).*

(7) *Spletna stran overitelja na Centru Vlade RS za informatiko (http:/www.gov.si/ca).*

(8) *H.G.Molina, A. Crespo in B. Cooper: Archival Digital Libraries Repositories, Univerza Stanford, ZDA (http://www-diglib.stanford.edu/~testbed/doc2/ArchivalRepositories/).*

(9) *P. Maniatis, M. Baker: Enabling the archival storage of signed documents, 2001 (http://identiscape.stanford.edu).*

SUMMARY

LONG-TERM MANAGEMENT OF ELECTRONICALLY-SIGNED DOCUMENTS

The rapid development of information technologies has dramatically changed the way how government authorities, corporations and individuals communicate and carry out their daily activities. With the growing quantity and diversity of e-commerce and e-communication we meet two major challenges. Firstly we have to provide a secure and legal e-commerce and secondly we have to find a solution to be certain that electronically-signed documents retain readable and prove their authenticity even a long time after having been created. Technological requirements for the legitimacy of e-commerce and e-communication in public administration and services offered to citizens and legal persons are provided by qualified digital certificates issued by the Certification Authority at the Governmental Centre for Informatics of Slovenia. The problems to keep electronically-signed records for a long time in order to preserve legal rights are presented in the paper. The problems occur because electronically-signed documents have a higher longevity than the usual software and hardware. The paper summerizes the most promising recommendations to ensure that electronically-signed records are accessible as long as they are needed.