DOLGOROČNO ZAGOTAVLJANJE AVTENTIČNOSTI IN VZDRŽEVANJE CELOVITOSTI ELEKOTRONSKO HRANJENEGA GRADIVA[1]

Helena Halas
Aljoša Jerman Blažič

Oddano: 2. 8. 2010 – Sprejeto: 31. 1. 2011

Pregledni znanstveni članek
UDK 004:005.921.1"746"(497.4)

Izvleček

Dolgoročna prezervacija elektronskih podatkov zahteva vpeljavo ustreznih tehnoloških rešitev in organizacijskih ukrepov, ki odgovarjajo na temeljne zahteve elektronske hrambe. Sistemske rešitve za hrambo podatkov morajo po načelih varovanja in ohranjanja elektronskega gradiva zagotavljati dostopnost, uporabnost oz. zmožnost reprodukcije in primernost reprodukcije za uporabo ter avtentičnost in celovitost hranjenega gradiva ves čas trajanja hrambe. Zaradi enostavnosti spreminjanja vsebine podatkov v elektronski obliki je v arhivskih sistemih ključnega pomena zagotavljanje sledljivosti in dokazljivosti sprememb gradiva. V prispevku je predstavljen pristop, ki je rezultat tehnološke standardizacije za dolgoročno zagotavljanje avtentičnosti in celovitosti elektronskega dokumentarnega ali arhivskega gradiva na osnovi sintakse evidenčnih podatkov. Predstavljen tehnološki koncept obravnava poljubno vrsto dokumentarnega ali arhivskega gradiva in omogoča ustvarjanje dodatnih varnostnih vsebin oz. evidenčnih podatkov, ki so potrebni za dolgoročno dokazovanje avtentičnosti in celovitosti gradiva v prihodnosti, od trenutka začetka elektronske hrambe oziroma arhiviranja. Sintaksa evidenčnih podatkov temelji na dveh pomembnih tehnikah in sicer gnezdenju prstnih odtisov objektov hrambe in vključevanju (kvalificiranih) digitalnih žigov tretjih zaupanja vrednih (pravnih) oseb. Obravnavani so tudi komplementarni organizacijski ukrepi za dokazovanje celovitosti in avtentičnosti ter raziskovalni in razvojni

1 *Članek je nastal na osnovi študije, ki jo je naročil Arhiv RS pri podjetju SETCCE.*

HALAS, Helena; Aljoša JERMAN BLAŽIČ. Electronic records long term authenticity and integrity demonstration. Knjižnica, 55(2011)1, pp. 175–192

rezultati vključno z nadaljnjim delom na področju raziskav in razvoja evidenčnih podatkov za dolgoročno hrambo oziroma arhiviranje elektronskega gradiva.

Ključne besede: elektronski podatki, dolgoročna hramba, avtentičnost, celovitost, varnostne vsebine, evidenčni podatki, digitalni žigi

Review article
UDC 004:005.921.1"746"(497.4)

Abstract

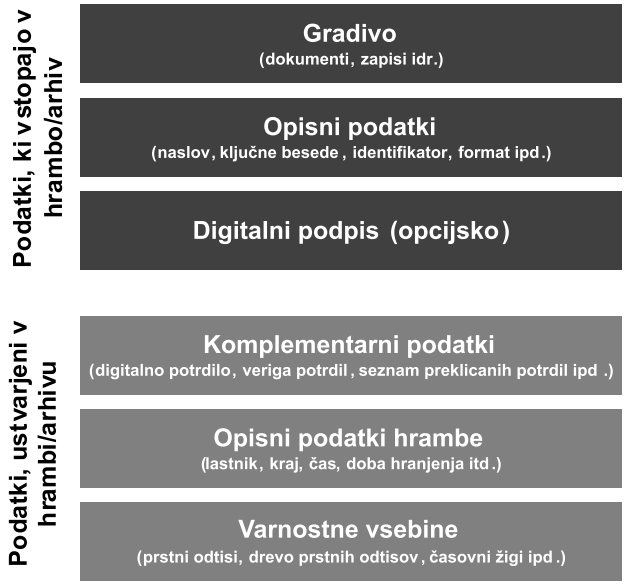
Long term preservation of electronic data requires introduction of specific technology solutions and organizational measures in order to provide stable environment for electronic record preservation. System solutions must support basic principles of electronic preservation: accessibility of data, usability or reproduction of data in usable form and integrity/authenticity provision including time existence for preserved content. Due to their nature, electronic data may become subjects of manipulation without recursive traceability of content alteration. In order to preserve usability of preserved data, electronic preservation system must provide appropriate measures for demonstrating unalterability of data for the entire preservation period. In this paper technology approach for demonstrating integrity and authenticity of archived data on long term basis is presented. Presented technological concept deals with any type of documentation or archiving material and provides creation of additional security assertions or evidence records that are needed to demonstrate the authenticity and integrity of the material anytime during the archival period. The evidence record syntax (ERS), which has been standardized by international organization body for internet standards (IETF), presents universal technique of security assertions generation and their maintenance for integrity preservation based on document hashing, hash treeing and integration of (qualified) time stamps of trusted third parties. Using re-time-stamping methods created security assertions may endure their validity for longest periods of time until retention periods of archived data expires. In the paper complementary organizational rules for technology solutions are presented as well, providing an all around overview of long term preservation of data in authentic, reliable and secure manner.

Keywords: electronic data, long-term preservation, authenticity, integrity, evidence record, digital time stamp

1 Uvod

Proces elektronske hrambe vključuje postopke zajema in vzdrževanja dokumentarnega elektronskega gradiva za poljubna časovna obdobja, pri čemer lahko čas hrambe v osnovi ločimo na kratkoročno in dolgoročno hrambo. Elektronsko hrambo namenoma označujemo kot proces, ki se začne z zajemom (pred zaje-

mom so običajno izvedeni še postopki urejanja, klasifikacije ipd.) in zaključi z odbiranjem ali izbrisom gradiva. Logično strukturo podatkov, ki vstopajo v sistem elektronske hrambe, in podatkov oz. vsebin, pripravljenih za potrebe hrambe, označujemo kot objekt hrambe (ang. archive object) (Slika 1).



Slika 1: Objekt hrambe

Osnovo za prehod na elektronsko hrambo predstavlja uvajanje ustreznih tehnoloških rešitev in uvedba organizacijskih ukrepov, ki opredeljujejo uporabo sistemskih rešitev in rokovanje z elektronsko hranjenim gradivom. Ključne zahteve zagotavljanja elektronske hrambe lahko strnemo v naslednja načela (ZVDAGA, 2006):

- *Načelo dostopnosti dokumentarnega gradiva* – podatki so vedno dosegljivi tistim, ki imajo pooblastila za to.
- *Načelo uporabnosti dokumentarnega gradiva* – podatki so primerni za kasnejšo uporabo oz. so hranjeni na način, da je možno vedno razbrati vsebino.
- *Načelo izvirnosti dokumentarnega gradiva* – podatki so shranjeni v obliki, v kateri so bili oblikovani, poslani ali prejeti ali v kakšni drugi obliki, ki verodostojno predstavlja oblikovane, poslane in prejete podatke.
- *Načelo dolgoročnosti dokumentarnega gradiva* – podatki so shranjeni na nosilcih in v oblikah zapisov, ki so primerni za dolgoročno hrambo.
- *Načelo verodostojnosti dokumentarnega gradiva* – proces hrambe zagotavlja verodostojnost zajetih podatkov in opisnih podatkov.

- *Načelo celovitosti in avtentičnosti dokumentarnega gradiva* – tehnologija in postopki zagotavljajo točnost, nespremenljivost in popolnost gradiva oziroma reprodukcije njegove vsebine, urejenost gradiva oziroma njegove vsebine ter dokazljivost (provenience) ves čas njegove hrambe.
- *Načelo vzdrževanja veljavnosti dokumentarnega gradiva* – hranjenje komplementarnih podatkov in sredstev za preverjanje varnostnih atributov (npr. digitalni podpisi) enako dolgo, kot se hranijo dokumenti.

Pomemben del zagotavljanja hrambe dokumentov v elektronski obliki predstavlja zahteva oziroma načelo celovitosti in avtentičnosti dokumentarnega gradiva, ki je obravnavana v nadaljevanju. Predstavljeni so ustrezni aktualni tehnološki prijemi za demonstracijo celovitosti in avtentičnosti hranjenega gradiva za poljubna časovna obdobja. Podrobneje so predstavljeni tehnološki prijemi za pripravo in vzdrževanje varnostnih vsebin, saj ti predstavljajo univerzalen pristop na osnovi tehnološke demonstracije celovitosti in avtentičnosti elektronskega gradiva tudi za daljša časovna obdobja. Ob tehnoloških prijemih so obravnavani tudi komplementarni organizacijski ukrepi za zagotavljanje avtentičnosti in celovitosti.

2 Tehnološke rešitve

2.1 Osnovne tehnologije

Za zagotavljanje celovitosti in avtentičnosti podatkov so bile razvite številne tehnike, ki so se s časom in napredkom tehnologij izpopolnjevale in izboljševale. Tovrstne tehnike temeljijo na dodajanju ustreznih atributov oziroma podatkov, s pomočjo katerih je možno prek vnaprej določenih algoritmov preveriti intaktnost (nespremenljivost) podatkov. Osnovni princip demonstracije celovitosti podatkov temelji na uporabi matematičnih algoritmov, s katerimi lahko za vsak zaključen podatek izračunamo unikaten (kratek) povzetek. Konsistentnost prebranih podatkov lahko v kasnejšem času vedno potrdimo s primerjavo ponovno izdelanega izvlečka prebranih oziroma prejetih podatkov in predhodno (izvorno) ustvarjenim povzetkom.

2.1.1 Prstni odtis

Temeljno vlogo pri demonstraciji celovitosti elektronskega gradiva ima t. i. prstni odtis. Z uporabo matematičnih (zgoščevalnih) algoritmov, ki delujejo na principu izgube informacij, je za poljubno dolg (zaključen) podatkovni niz ustvarjena naključna navidezna vrednost (vedno enake dolžine), ki jo označujemo kot izvleček oziroma prstni odtis (ang. hash value, fingerprint). Zgoščevalni algorit-

mi delujejo na principu unikatnosti prstnih odtisov, saj pomeni že najmanjša sprememba vhodnega podatkovnega niza popolnoma drugačno vrednost prstnega odtisa. Spremembo podatkov preverimo s primerjavo izvornega prstnega odtisa in vrednosti prstnega odtisa, izračunanega na osnovi prejetih podatkov, tj. v času preverjanja celovitosti.

Glavno pomanjkljivost prstnih odtisov predstavlja uporaba zgoščevalnih metod za njihovo izdelavo, saj te temeljijo na javnih algoritmih, zaradi česar je manipulacija s podatki dokaj enostavna. Brez uporabe revizijskih sledi ali dodatne zaščite izvornega prstnega odtisa je poseg nad izvornimi podatki nemogoče odkriti in na ta način ugotoviti verodostojnost prvotnega prstnega odtisa (s spremembo podatkov je mogoče vedno ustvariti nov prstni odtis, ki ustreza spremenjenim podatkom in z njim nadomestiti izvorno vrednost prstnega odtisa). Hkrati ima uporaba prstnih odtisov določene omejitve, povezane s tehnološkim napredkom, saj postanejo zgoščevalni algoritmi s časom nezanesljivi in jih je treba nadomestiti z novimi in zmogljivejšimi.

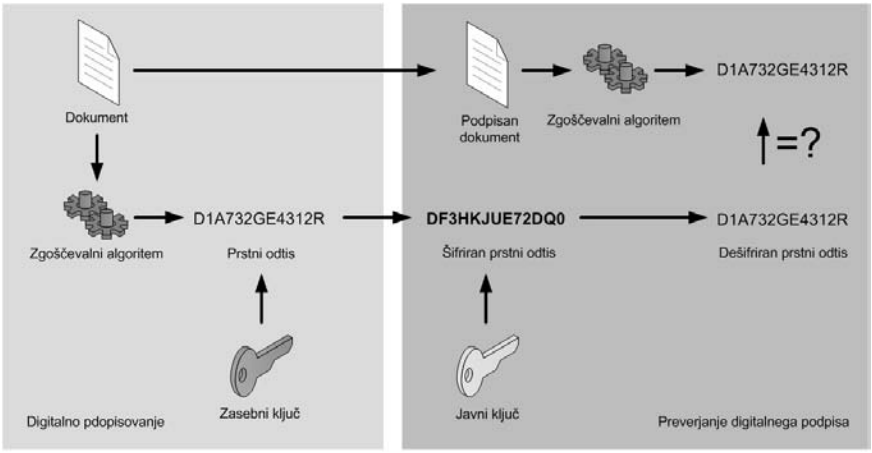
Učinkovitejše sredstvo za zagotavljanje avtentičnosti in celovitosti podatkov predstavljajo digitalni podpisi in časovni žigi. Temeljijo na principu kriptografske zaščite prstnih odtisov, s čimer se omeji poseganje v izvorno ustvarjeno vrednost prstnega odtisa.

2.1.2 Digitalni podpis

Digitalno podpisovanje (ang. digital signing) deluje na principu uporabe kombinacije različnih kriptografskih algoritmov, ki izvorne podatke obdelajo na način, da lahko prejemnik z ustreznimi elektronskimi sredstvi preveri avtentičnost in celovitost izvornih podatkov. V ta namen je bila razvita asimetrična kriptografija, kjer nastopa par šifrirnih ključev, zasebni, s katerim sporočilo šifriramo, in javni, s katerim sporočilo dešifriramo. Za ustvarjanje para ključev praviloma poskrbi uporabnik, ki tudi hrani zasebni del para ključev, medtem ko za distribucijo javnih ključev skrbi (javni) overitelj oziroma izdajatelj digitalnih potrdil. Digitalna potrdila vključujejo javni ključ subjekta, podatke o subjektu, namen uporabe para ključev, veljavnost digitalnega potrdila idr.

Zaradi optimizacije temelji digitalno podpisovanje na šifriranju prstnega odtisa podatkov (dokumenta), sicer bi bil postopek prepočasen. Prejemnik digitalno podpisanih podatkov mora zato ponovno ustvariti prstni odtis in ga primerjati s prejetim prstnim odtisom, ki je del digitalnega podpisa. Pred tem mora dešifrirati prejeti prstni odtis z javnim ključem pošiljatelja. V kolikor se prstna odtisa ujemata, lahko sklepamo, da je podpis pravilen, da ga je ustvaril podpisnik (imetnik digitalnega potrdila) in da so podatki nespremenjeni (Slika 2). Tehnične zahteve za varno elektronsko podpisovanje opredeljuje tudi zakonodaja (ZEPEP-UPB1, 2004).

Ker sloni postopek digitalnega podpisovanja na šifrirnih algoritmih, postanejo ti s časom zaradi tehnološkega napredka nezanesljivi. Zaradi tega je veljavnost digitalnih potrdil in s tem par šifrirnih ključev praviloma omejena na nekaj let (slovenski overitelji postavljajo mejo pri petih letih od izdaje digitalnega potrdila). Druga omejitev digitalnega podpisovanja predstavlja zasebni ključ, ki je lahko predmet zlorabe (odtujitve). V takšnem primeru je treba digitalno potrdilo preklicati, saj ni več mogoče zagotoviti avtentičnost podpisovanja. Z neveljavnimi algoritmi in neveljavnim zasebnim ključem zgubijo veljavnosti tudi vsi, že ustvarjeni digitalni podpisi, v kolikor niso pred tem ustrezno obdelani in zaščiteni.



Slika 2: Postopek digitalnega podpisovanja

Uporaba digitalnih podpisov predstavlja sicer v kontekstu elektronske hrambe naprednejši princip zagotavljanja avtentičnosti in celovitosti, saj digitalni podpis kljub nekaterim tehničnim oziroma časovnim omejitvam na nedvoumen in vedno znova preverljiv način omogoča identifikacijo podpisnika, potrjevanje povezave podpisnika z vsebino in demonstracijo celovitosti podpisanih podatkov. Za dolgoročno (trajno) uporabnost tovrstnih sredstev je treba vključiti dodatne tehnike, ki vzdržujejo veljavnost digitalnih podpisov za daljša časovna obdobja. Te so predstavljene v nadaljevanju.

2.1.3 Časovni žig

Časovni žig učinkovito rešuje probleme časovne omejitve uporabe digitalnih podpisov, saj poleg ostalih elementov podpisa vključuje še časovno komponento, pridobljeno od zaupanja vrednega časovnega vira (ang. trusted time source). V tehničnem smislu predstavlja časovni žig (ang. time stamp, TS) dopolnjen niz znakov digitalnega podpisa, ki opredeljujejo datum in/ali čas dogodka, na ka-

terega se žig navezuje. Da bi časovni žig lahko povezali z verodostojnim časovnim virom in zagotovili njegovo verodostojnost, mora postopek žigosanja izvajati zaupanja vredna tretja oseba, ki jo predstavlja overitelj časovnih žigov (ang. time stamp authority, TSA), običajno združena z vlogo overitelja digitalnih potrdil. Uporabniki časovnega žigosanja pripravijo prstni odtis zaključenega niza podatkov in predložijo izvleček v podpis overitelju časovnih žigov. Pridobljeni časovni žig demonstrira celovitost časovno žigosanih podatkov in točen čas žigosanja (Adams, Cain, Pinkas in Zuccherato, 2001).

Časovni žig predstavlja osnovni tehnološki prijem za zagotavljanje avtentičnosti in celovitosti gradiva v elektronski hrambi. Z njegovo uporabo je namreč mogoče nedvoumno ugotoviti čas vstopa gradiva v informacijski sistem. Še vedno pa ima časovni žig določene omejitve, ki so ekvivalentne omejitvam digitalnih podpisov. Tako kot digitalni podpis s časom izgublja vrednost, kakor tudi v primeru kompromitiranja zasebnega ključa, s katerim je bil ustvarjen. Da bi prešli tovrstne omejitve, je treba zagotoviti dodatne tehnološke ukrepe, ki zagotavljajo trajno veljavnost časovnih žigov, ki jih predstavljamo v nadaljevanju.

2.2 Tehnologije za vzdrževanje avtentičnosti in celovitosti na dolgi rok

Sodobne tehnike zagotavljanja avtentičnosti in celovitosti elektronskega gradiva temeljijo na mehanizmih digitalnega podpisovanja oziroma na njenih izpeljankah, ki pa še vedno vsebujejo določene omejitve, kot je zastaranje digitalnega potrdila in s tem digitalnega podpisa oziroma časovnega žiga, možnost kompromitiranja zasebnega ključa itn. Za potrebe dolgoročne hrambe morajo uporabljena elektronska sredstva vključevati tudi metode dolgoročnega vzdrževanja varnostnih vsebin. S tem namenom so bile razvite tehnike razširjene oblike digitalnega podpisa in tehnika evidenčnih podatkov.

2.2.1 Razširjena oblika digitalnega podpisa

Za vzdrževanje trajne veljavnosti digitalnih podpisov je treba zagotoviti:

- razpoložljivost vseh virov oziroma komplementarnih podatkov, potrebnih za preverjanje veljavnosti digitalnega podpisa za celotno obdobje uporabe (digitalna potrdila, seznam preklicanih potrdil itn.);
- informacijo o času obstoja digitalnega podpisa;
- zaščito vsebine digitalnega podpisa in podpisanih podatkov.

Da bi lahko zadostili navedenim zahtevam, je treba skupaj z digitalnim podpisom in podpisanimi podatki vzdrževati in ustrezno zaščititi vsa sredstva, potreb-

na za uspešno preverjanje veljavnosti podpisa. V nasprotnem primeru se lahko zgodi, da podatki v nekem trenutku niso več na voljo (npr. overitelj oziroma izdajatelj digitalnih potrdil preneha obstajati; sistemsko okolje, v katerem je bil digitalni podpis kreiran, ni več na voljo).

Najbolj učinkovit način zbiranja komplementarnih podatkov (v kontekstu vzdrževanja veljavnosti podpisov na dolgi rok) predstavlja razširjena oblika digitalnega podpisa (ang. advanced electronic signature, AES) (Cruellas et. al., 2003). Omogoča zbiranje vseh komplementarnih podatkov, potrebnih za uspešno preverjanje podpisa, in vključevanje teh podatkov neposredno v samo strukturo digitalnega podpisa. Tako so vsa sredstva za preverjanje podpisa vedno na voljo.

Da bi odpravili omejitve zastaranja podpisa (po preteku digitalnega potrdila kot dela komplementarnih podatkov, izgubi veljavnost tudi podpis), je treba podpis in komplementarne podatke zaščititi še s časovnim žigom. Na podlagi (verodostojne) časovne komponente, vključene v časovni žig, je mogoče ugotoviti, kdaj točno so bili komplementarni podatki in podpis žigosani. Če je bilo to pred pretekom veljavnosti potrdila, lahko zagotovimo, da je bil podpis v času žigosanja in z njim vsi komplementarni podatki veljaven. Časovni žig tako rekoč zamrzne podpis v času, ko je bil le-ta veljaven.

Ker ima tudi časovni žig omejen rok veljavnosti, je treba še pred njegovim iztekom celotno vsebino razširjenega digitalnega podpisa ponovno časovno žigosati. Razširjena oblika digitalnega podpisa je tako sestavljena iz verige časovnih žigov, kjer aktualen časovni žig ščiti:

- vse predhodne žige,
- podpisane podatke,
- komplementarne podatke in
- digitalni podpis.

Pri sprotnem časovnem žigosanju je treba uporabljati izključno aktualne šifrirne algoritme, s čimer odpravimo pomanjkljivost zastaranja kriptografskih algoritmov, uporabljenih za digitalni podpis ali časovni žig. Tako zaščiteno gradivo je popolnoma neodvisno od sistema hrambe in omogoča enostaven prenos med sistemi, saj lahko skupaj z gradivom prenašamo varnostne vsebine za zagotavljanje celovitosti in avtentičnosti, kakor tudi komplementarne podatke za preverjanje veljavnosti digitalnega podpisa.

Uporaba razširjene oblike digitalnega podpisa je primerna predvsem v okoljih oziroma poslovnih procesih, kjer že nastopajo digitalno podpisani dokumenti, saj omogoča neposredno dodajanje varnostnih vsebin za dolgoročno vzdrževanje celovitosti v sam podpis.

Kljub vsemu ima razširjena oblika digitalnega podpisa določene omejitve:

- izhaja iz potrebe po vzdrževanju veljavnosti digitalnih podpisov in ne celovitosti podatkov, kar pomeni, da vključuje redundanten nabor varnostnih vsebin;
- digitalni podpis je primarno namenjen povezovanju podpisnika z vsebino, kar v kontekstu elektronske hrambe nima nobene uporabne vrednosti oziroma predstavlja nepotrebne dodatne prostorske in procesne zmogljivosti;
- predvideva zbiranje komplementarnih podatkov in uporabo časovnega žiga za vsak digitalni podpis posebej, kar predstavlja omejevalni faktor pri obdelavi večje količine podatkov (ločenih dokumentov) in je iz procesnega vidika težko sprejemljiv tehnološki pristop.

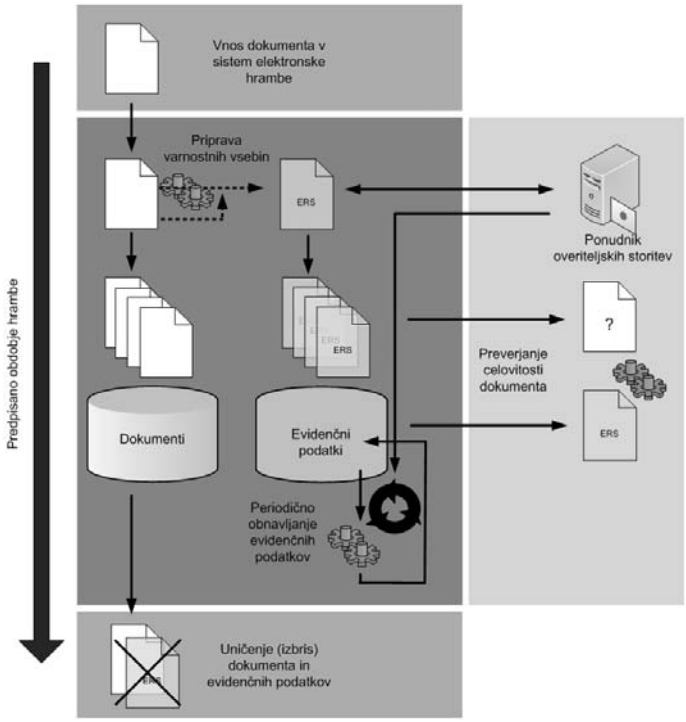
2.2.2 Sintaksa evidenčnih podatkov

Sintaksa evidenčnih podatkov (ang. evidence record syntax, ERS) predstavlja enega ključnih tehnoloških gradnikov za obdelavo gradiva v sistemih elektronske hrambe. Izhaja iz osnovnih potreb po dolgoročni demonstraciji celovitosti podatkov ne glede na izvor, obliko in namen ter predstavlja alternativno metodo razširjeni obliki digitalnega podpisa (Gondrom, Brandner in Pordesch, 2007).

ERS predstavlja univerzalno tehnološko sredstvo za demonstracijo celovitosti in avtentičnosti podatkov na dolgi rok in obsega:

- pripravo varnostnih vsebin (za demonstracijo celovitosti in avtentičnosti) za poljubno gradivo;
- uporabo časovnega žigosanja in prenos veljavnosti varnostnih vsebin na tretjo neodvisno (zaupanja vredno) stranko;
- trajno vzdrževanje varnostnih vsebin na osnovi verig in sekvenc časovnih žigov;
- neodvisno preverjanje varnostnih vsebin;
- zagotavljanje optimizacije priprave in vzdrževanja varnostnih vsebin;
- prenos varnostnih vsebin med informacijskimi sistemi za hrambo e-gradiva.

Evidenčni podatki predstavljajo varnostne vsebine, ki jih praviloma pripravlja in vzdržuje namenski sistem oziroma je to integralni tehnološki del sistema za elektronsko hrambo. Za izbran podatkovni objekt (npr. dokument) je izdelan prstni odtis, ki je umeščen v posebno strukturo zapisa, kateri so lahko dodani komplementarnih podatki (varnostnih vsebin, ki jih podatkovni objekt že vsebuje, npr. digitalni podpis) in arhivski časovni žig (ang. archive time-stamp, ATS). Struktura evidenčnega zapisa omogoča vključevanje časovnih žigov, ki ščitijo predhodne žige, opisne in druge (komplementarne) podatke ter gradivo v sistemu hrambe (Slika 3).



Slika 3: Princip delovanja tehnike evidenčnih podatkov ERS

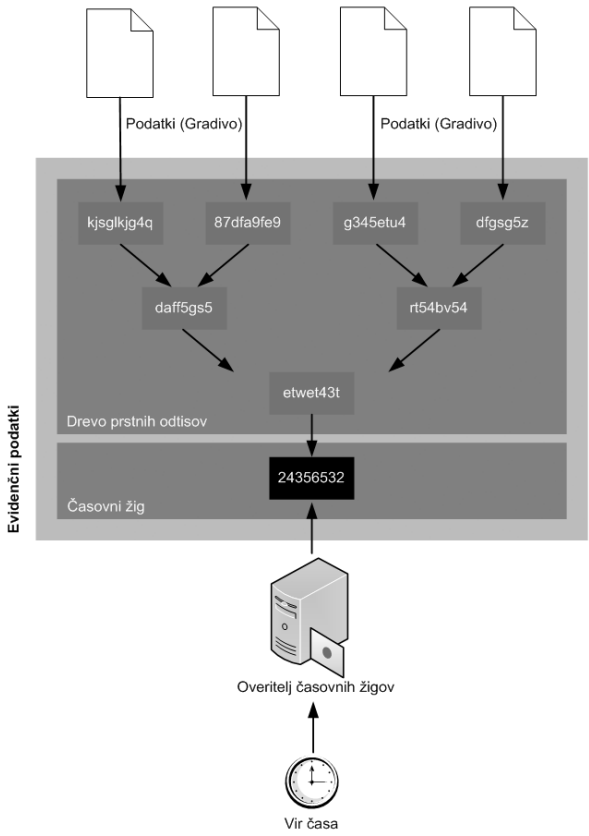
Evidenčni podatki prepoznavajo dve obliki ponovnega časovnega žigosanja. Enostavno ponovno časovno žigosanje (ang. simple re-time-stamping), namenjeno okoliščinam, ko so kriptografski algoritmi predhodnega časovnega žiga še vedno dovolj zanesljivi in posodobljen časovni žig ščiti zgolj predhodnika (skupaj s komplementarnimi podatki predhodnega žiga). Takšno zaporedje časovnih žigov označujemo kot verigo (ang. archive time-stamp chain, ATSC). Kompleksno ponovno časovno žigosanje (ang. complex re-time-stamping), namenjeno okoliščinam, ko postanejo uporabljeni kriptografski algoritmi prešibki in mora novi časovni žig v verigi ščititi vse predhodne žige, opisne ter druge podatke in gradivo v sistemu elektronske hrambe. Takšno zaporedje časovnih žigov označujemo kot sekvenco (ang. archive time-stamp sequence, ATSS).

Z namenom zagotavljanja trajne veljavnosti vseh žigov v verigi oziroma v sekvenci omogoča ERS zbiranje in vzdrževanje komplementarnih podatkov, potrebnih za preverjanje vseh predhodnih časovnih žigov (digitalna potrdila in seznami preklicanih potrdil).

Tehnika ERS omogoča vzporedno časovno žigosanje, kar pomeni, da sistem elektronske hrambe podpira vključevanje več ponudnikov storitev časovnega žigo-

sanja hkrati. Za vsakega overitelja zagotavlja ločeno zaporedje časovnih žigov za posamezen ali vse podatke in gradivo v sistemu hrambe. S tem je zagotovljena redundanca v kritičnih primerih kompromitiranja enega overitelja ali prenehanja delovanja (poslovanja) ponudnika storitev časovnega žigosanja.

Z uporabo metode dreves prstnih odtisov oziroma gnezdenja omogoča tehnika ERS optimizacijo priprave varnostnih vsebin za dokazovanje celovitosti in avtentičnosti (Slika 4). Za posamezen podatkovni objekt (npr. dokument) je s pomočjo algoritma za zgoščevanje pripravljen prstni odtis posameznega podatkovnega objekta, ki je nato združen s prstnimi odtisi drugih objektov. Iz več prstnih odtisov je na osnovi uporabe enakega zgoščevalnega algoritma pripravljen nov prstni odtis, ki ga lahko ponovno združimo s prstnim odtisom drugih objektov ali druge skupine objektov. Korensko vrednost, to je zadnji prstni odtis, izračunan iz zadnje skupine prstnih odtisov, je treba časovno žigosati. Združevanje poljubne



Slika 4: Drevo prstnih odtisov za optimizacijo priprave in vzdrževanja evidenčnih podatkov

količine dokumentov (neodvisno od konteksta ali logičnega povezovanja dokumentov) pomeni optimizacijo uporabe virov in zunanjih storitev.

Varnostne vsebine posameznih podatkovnih objektov so na podlagi uporabe drevesne strukture prstnih odtisov ločene med seboj. Tako je preverjanje oziroma dokazovanje celovitosti posameznega objekta neodvisno od dostopnosti ostalih objektov v drevesni strukturi. Varnostne vsebine v procesu elektronske hrambe je treba zagotoviti neposredno ob vnosu dokumentov v sistem hrambe. Poleg tega je treba zagotoviti vzdrževanje (obnavljanje) vsebin ERS za celotno obdobje hrambe, ne glede na to ali so hranjeno gradivo in drugi podatki združeni ali ne.

Na osnovi mednarodne standardizacije omogoča ERS prenos podatkov za demonstracijo celovitosti in avtentičnosti in s tem neodvisno preverjanje varnostnih vsebin med sistemi elektronske hrambe ali drugimi informacijskimi sistemi. Z uporabo ERS in obnavljanjem vsebin ERS je možno zagotoviti trajno celovitost in avtentičnost hranjenega gradiva skladno z zahtevami, kot jih predpisujejo mednarodna priporočila, modeli sistemov elektronske hrambe (npr. Model, 2008; Reference, 2002) in zakonodaja (ZVDAGA, 2006; Uredba, 2006).

3 Organizacijski ukrepi

Do določene mere lahko izvajanje ustreznih organizacijskih ukrepov nadomešča uporaba tehnoloških sredstev, vendar je primarni namen organizacijskih ukrepov dopolnjevanje implementiranih tehnologij elektronske hrambe. Organizacijski ukrepi predstavljajo vez med obstoječimi tehnološkimi sredstvi, kjer teh iz takšnih ali drugačnih razlogov ne moremo privzeti kot edini način zagotavljanja varne in zakonsko skladne hrambe. Organizacijski ukrepi za zagotavljanje avtentičnosti in celovitosti obsegajo:

- organizacijske varnostne ukrepe in ukrepe za upravljanje z gradivom,
- urejenost in dokumentiranost izvajanja poslovnih/upravnih procesov, povezanih z zajemom in elektronsko hrambo,
- spremljanje izvajanja predpisanih organizacijskih ukrepov,
- preverjanje ustreznosti organizacijskih ukrepov (notranjih pravil[2]), preverjanje ustreznega izvajanja predpisanih organizacijskih ukrepov in
- drugo.

2 *»Notranja pravila« so pravila, ki jih kot svoj interni akt sprejme oseba glede izvajanja zajema in hrambe svojega dokumentarnega in arhivskega gradiva v digitalni obliki ter spremljevalnih storitev, oziroma ponudnik storitev izvajanja zajema in hrambe oziroma spremljevalnih storitev (Predlog, 2010).*

Potrebni organizacijski ukrepi, ki obravnavajo hrambo elektronskega gradiva na splošno, so odvisni od značilnosti organizacije, obstoječih poslovnih procesov in tveganj, s katerimi se organizacija sooča. Obseg organizacijskih ukrepov je odvisen tudi od izbranega obsega in tehnološke realizacije rešitve elektronske hrambe (implementacija rešitve na lastni infrastrukturi, zunanje izvajanje storitve ali kombinacija implementacije rešitve na lastni infrastrukturi in zunanjega izvajanja posameznih storitev). Izvajanje organizacijskih ukrepov je potrebno ne glede na to, kdo zagotavlja infrastrukturo za elektronsko hrambo, razlika je predvsem v tem, kateri del procesa hrambe je v domeni zunanjega izvajanja in kateri del zagotavlja organizacija sama z lastnimi človeškimi, organizacijskimi in tehnološkimi resursi.

3.1 Zagotavljanje celovitosti in avtentičnosti z organizacijskimi ukrepi

Organizacijski ukrepi za zagotavljanje celovitosti in avtentičnosti elektronskega gradiva so tesno povezani z nadzorom dostopa in poseganja v vsebino gradiva. Da bi preprečili neavtoriziran poseg v vsebino, je treba zagotoviti ustrezna pravila rokovanja s tehnološkimi sredstvi, vezanimi na pravice dostopa, preprečevanje vdora in beleženje sprememb. Pomembna je tudi ustrezna stopnja urejenosti okolja in procesov, v katerih gradivo nastaja in je shranjeno, zato je treba vzpostaviti konsistentno organizacijsko strukturo na vseh ravneh in čez celoten proces od zajema, prek vzdrževanja do izločanja oziroma odbiranja elektronskega gradiva. Deli organizacijskih ukrepov, ki implicitno ali eksplicitno obravnavajo celovitosti in avtentičnosti gradiva, so vezani na:

- ustrezno ravnanje z informacijskimi viri, ki so vključeni v zajem in hrambo,
- fizično in tehnično varovanje opreme in prostorov,
- upravljanje dostopov do varovanih območij in dostopov do hranjenega gradiva,
- zaščito pred zlonamerno računalniško programsko opremo in načrtnimi vdori,
- upravljanje s spremembami,
- druge organizacijske ukrepe, povezane z varno uporabo oziroma omejevanjem dostopa do hranjenega gradiva.

Organizacijske ukrepe lahko smiselno razdelimo po procesnih delih elektronske hrambe, glede na vlogo, tehnološka sredstva, organizacijo itn. Lahko pa jih obravnavamo z vidika posameznih (poslovnih/organizacijskih) domen, kot so tehnološka infrastruktura, kadrovska ureditev, poslovni procesi itn. Pri tem je pomembno, da je domena celovitosti in avtentičnosti gradiva razpršena čez vsa

relevantna vsebinska področja organizacijskih ukrepov in ni vsebinsko omejena oziroma obravnavana ločeno.

Z vidika procesa je zagotavljanje avtentičnosti in celovitosti elektronskega gradiva z organizacijskimi ukrepi v največji meri vezano na postopke razvrščanja, zajema in upravljanja z elektronskim gradivom. Organizacijski ukrepi morajo torej obsegati naslednje postopke, ki imajo sicer neposredno implikacijo na zagotavljanje avtentičnosti in celovitosti gradiva:

- sprejemanje gradiva,
- evidentiranje in razvrščanje prejetega gradiva (na osnovi klasifikacijskega načrta),
- prevzem razvrščenega gradiva,
- evidentiranje in razvrščanje gradiva za zajem in pretvorbo,
- urejanje gradiva v fizični obliki pred zajemom in pretvorbo,
- evidentiranje zajema in pretvorbe (gradivo in pripadajoči metapodatki),
- kontrola celovitosti in kakovosti zajetega in pretvorjenega gradiva (gradivo in pripadajoči metapodatki),
- dodatne občasne kontrole kakovosti in celovitosti zajetega gradiva.

Vsi postopki morajo biti dovolj natančno opredeljeni, kot tudi odgovornosti za njihovo izvajanje. Zaposleni, ki so odgovorni za upravljanje z elektronskim gradivom in za zagotavljanje informacijske varnosti, morajo naloge izvajati v skladu s predpisanimi postopki, izvajanje pa evidentirati oziroma dokumentirati. Celovitost in avtentičnost hranjenega gradiva je namreč dokazljiva zgolj in izključno ob nadzoru in dokazljivosti izvajanja celotne verige organizacijskih ukrepov in ustrezne zaščite informacijskih virov.

Področje informacijske varnostne politike obsega organizacijske ukrepe za zagotavljanje informacijske varnosti in upravljanje dostopov do gradiva in ima neposredno implikacijo na vsa tri zgoraj omenjena področja (razvrščanje, zajem in upravljanje). Informacijska varnostna politika mora obsega najmanj:

- organizacijo in izvajanje fizičnega in tehničnega varovanja: zagotovitev ustreznega strežniškega prostora, primerna fizična zaščita varnostnih kopij, upravljanje dostopov do sistemskih in drugih prostorov, izvajanje drugih oblik varovanja (varnostna služba, vratar, receptor itd.);
- organizacijo upravljanja dostopov do elektronskega gradiva: uporabniški račun in varna gesla, upravljanje dostopa do omrežja, upravljanje pravic dostopa do sistema.

Redno vzdrževanje in posodabljanje strojne in programske opreme ter formatov zapisov je ključnega pomena pri zagotavljanju dolgoročne uporabnosti elektronskega gradiva. Organizacijski ukrepi na ravni upravljanja so v večji meri name-

njeni zagotavljanju obstojnosti hranjenega gradiva in imajo hkrati implicitno vlogo pri zagotavljanju avtentičnosti in celovitosti. Ti ukrepi obsegajo:

- izbiro veljavnih oblik zapisa za dolgoročno hrambo,
- izbiro primernih oblik varnostnih vsebin za demonstracijo celovitosti in avtentičnosti,
- izvajanje pretvorbe in vzdrževanje gradiva v obliki zapisa za dolgoročno hrambo,
- izvajanje pretvorbe dokumentov v novo obliko zapisa za dolgoročno hrambo,
- prenos dokumentov oziroma zapisov na nove nosilce zapisa,
- osveževanje in/ali posodabljanje varnostnih vsebin,
- vzdrževanje in zamenjava programske opreme za predstavitev vsebine hranjenega gradiva ter demonstracijo celovitosti in avtentičnosti.

Uspešno izvajanje organizacijskih ukrepov je v največji meri odvisno od zaposlenih, ki so vključeni v proces upravljanja dokumentarnega gradiva in elektronske hrambe. V kontekstu zagotavljanja celovitosti in avtentičnosti je zato pomembno tudi izvajanje ustreznih kadrovskih (varnostnih) politik, ki obsegajo:

- sistemizacijo in opis delovnih mest (zahtevana dela in naloge),
- postopke zaposlovanja (podpis izjave o varovanju informacij),
- načrtovanje in izvajanje usposabljanja zaposlenih za delo in varovanje informacij,
- postopke ob zamenjavi dela v okviru organizacije ali ob prekinitvi delovnega razmerja (preklic uporabniških pravic v informacijskih sistemih).

Organizacijski ukrepi lahko pripomorejo k zagotavljanju oziroma vzdrževanju celovitosti in avtentičnosti vsebine hranjenega gradiva, vseeno pa imajo organizacijski ukrepi določene omejitve, med katere štejemo: kompleksnost organizacijskih ukrepov in njihovega izvajanja, nekonsistentnost, zahtevnost nadzora in preverjanja izvajanja, pomanjkanje ustreznih sredstev za sistematično spremljanje organizacijskih ukrepov, dokazljivost celovitosti in avtentičnosti hranjenega gradiva itd.

Na razpolago je širok nabor organizacijskih ukrepov, ki lahko učinkovito pripomorejo k zagotavljanju celovitosti in avtentičnosti elektronskega gradiva ne glede na izvor in obliko. Vendar pa je zagotavljanje avtentičnosti in celovitosti brez prisotnosti vsaj osnovnih tehnoloških prijemov omejeno. Pri uporabi zgolj organizacijskih ukrepov lahko operiramo le z določeno stopnjo zaupanja v avtentičnost in celovitost hranjenega gradiva. Za doseganje verodostojnosti gradiva v digitalni obliki na dolgi rok je pomembna kombinacija ustreznih organizacijskih ukrepov, ki določajo najmanj tip in obliko uporabljenih tehnoloških sredstev, ter tehnologij, namenjenih ohranjanju celovitosti in avtentičnosti gradiva, hkratne uporabe programske opreme za varovanje pred škodljivo kodo itd. Temu je treba dodati še tehnologije za dokazljivost celovitosti in avtentičnosti gradiva. V takšnih okolišči-

nah govorimo o komplementarnosti organizacijskih ukrepov in podpornih tehnologij za doseganje čim višje stopnje celovitosti in avtentičnosti, njeno dokazovanje pa je predmet namenske tehnologije, neodvisne od človeškega faktorja.

4 Zaključek

Tehnologije za demonstracijo celovitosti in avtentičnosti na dolgi rok so rezultat večletnih raziskav in razvoja. Osnovo za sintakso evidenčnih podatkov predstavljajo tehnike digitalnega podpisovanja, te pa temeljijo na šifrirnih algoritmih. Evidenčni podatki predstavljajo dodaten nabor atributov, ki jih je treba ustvariti za posamezen podatkovni objekt ali skupino objektov (dokumentov), in predstavljajo ločeno strukturo, ki v same podatke ne posega oziroma jih ne spreminja. Zapis ERS je tako vzporeden nabor podatkov, ki je lahko v istem sistemu elektronske hrambe ali ločeno v komplementarnem (namenskem) sistemu. S tem je omogočen tudi enostaven prehod med sistemi hrambe, kar je še posebej pomembno v procesih odbiranja arhivskega gradiva iz dokumentarnega in njegovega prevzemanja v pristojni arhiv. V takšnih okoliščinah dobi gradivo nov status arhivskega gradiva in je predmet vzdrževanja s strani namenske institucije (npr. Arhiv RS). Pri prehodu iz sistema elektronske hrambe v sistem elektronske hrambe pristojnega arhiva je treba prenesti tudi podatke, ki demonstrirajo celovitost in avtentičnost z namenom dokazovanja izvirnosti gradiva. Do enakih okoliščin lahko pride pri prenosu med sistemi elektronske hrambe iz poslovnih ali kakršnihkoli drugih razlogov. Varnostne vsebine pomen oziroma vrednost gradiva z vidika celovitosti in avtentičnosti učinkovito prenašajo v novo sistemsko okolje in omogočajo nadaljevanje vzdrževanja celovitosti in avtentičnosti.

Tehnološko priporočilo za evidenčne podatke, tj. sintakso in procesna navodila, določa mednarodna standardizacijska organizacija Internet Engineering Task Force v abstraktni obliki zapisa (ang. abstract syntax notation one, ASN.1) ali razširjeni obliki zapisa (ang. extensible markup language, XML). Medtem ko je oblika ASN.1 sprejeta kot standardizirana oblika ERS (tehnološko priporočilo RFC4998; Wallace, Pordesch in Brandner, 2007), je razširjena oblika XMLERS v času priprave prispevka predmet potrjevanja kot splošno tehnološko priporočilo (Jerman Blažič, Šaljić in Gordon, 2010). Obe obliki se med seboj dopolnjujeta kot alternativni obliki zapisa glede na izbrano tehnološko osnovo. Glede na vedno bolj razširjeno uveljavitev formata XML in s tem povezanih spletnih tehnologij, je predvidena splošna razširjenost zapisa XMLERS.

Nadaljnje raziskovalne aktivnosti so osredotočene na problematiko tehnološkega razvoja in s tem povezane spremembe oblik zapisov. Zastaranje formatov zapisa je splošen problem elektronske hrambe, saj s posodobljenimi formati vedno

obstaja nevarnost izgube uporabne vrednosti izvornih oblik zapisa. Strategije dolgoročne hrambe predvidevajo pretvorbo v aktualne formate. S tem pa lahko pride tudi do okoliščin, ko postane sled dokazljivosti celovitosti in avtentičnosti podatkov nestabilna. Med osrednje strategije dolgoročnega vzdrževanja tako uporabnosti kot tudi celovitosti in avtentičnosti podatkov vključujemo migracijo. Takšen postopek pretvorbe v aktualen format mora biti izveden strogo nadzorovano, kar velja tudi za varnostne vsebine.

Navedeni viri

1. Adams, C., Cain, P., Pinkas, D. in Zuccherato, R. (2001). *Internet X.509 public key infrastructure time-stamp protocol (TSP), RFC 3161*. Reston: The Internet Society. Pridobljeno 9. 9. 2010 s spletne strani: http://tools.ietf.org/pdf/rfc3161.pdf
2. Cruellas, J.C., Karlinger, G., Pinkas, D. in Ross, J. (2003). *XML advanced electronic signature, XAdES, W3C Note*. Sophia-Antipolis Cedex France: European Telecommunications Standards Institute (ETSI). Pridobljeno 9. 9. 2010 s spletne strani: http://www.w3.org/TR/XAdES/
3. Gondrom, T., Brandner, R. in Pordesch, U. (2007). *Evidence record syntax (ERS), RFC 4998*. Reston: IETF Trust. Pridobljeno 10. 9. 2010 s spletne strani: http://tools.ietf.org/pdf/rfc4998.pdf
4. Jerman Blažič, A., Šaljić, S. in Gondrom, T. (2010a). *Extensible markup evidence record syntax (XMLERS), 7.* Reston: The Internet Society. Pridobljeno 9. 9. 2010 s spletne strani: http://tools.ietf.org/html/draft-ietf-ltans-xmlers-07
5. *Model requirements for the management of electronic records – MoReq2 specification*. (2008). Bruxelles, Luxemburg: IDABC Programme, CECA-CEE-CEEA.
6. *Predlog Zakona o spremembah in dopolnitvah Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih* (ZVDAGA-A). (2010). Ljubljana: Arhiv RS. Pridobljeno 27. 10. 2010 s spletne strani: http://www.arhiv.gov.si/fileadmin/arhiv.gov.si/pageuploads/zakonodaja/Predpisi/ZVDAGA-A_pl.pdf
7. *Reference model for an open archival information system (OAIS): recommendation for space data system standards.* (2002). Washington: Consultative Committee for Space Data Systems (CCSDS).
8. Uredba o varstvu dokumentarnega in arhivskega gradiva. (2006). *Uradni list RS*, št. 86.
9. Wallace, C., Pordesch, U. in Brandner, R. (2007). *Long-term archive service requirements, RFC 4810*. Reston: IETF Trust. Pridobljeno 10. 8. 2010 s spletne strani: https://tools.ietf.org/html/rfc4810

10. Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP-UPB1). (2004). *Uradni list RS*, št. 98.

11. Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (ZVDAGA). (2006). *Uradni list RS*, št. 30.

Mag. Helena Halas je zaposlena v SETCCE.
Naslov: Tehnološki park 21, 1000 Ljubljana
Naslov elektronske pošte: helena.halas@setcce.si

Mag. Aljoša Jerman Blažič je zaposlen v SETCCE.
Naslov: Tehnološki park 21, 1000 Ljubljana
Naslov elektronske pošte: aljosa@setcce.si