Časovno žigosanje, nujna sestavina varnega e-poslovanja v javni upravi

Mitja Dečman
Univerza v Ljubljani, Fakulteta za upravo
mitja.decman@fu.uni-lj.si

Marjan Krisper
Univerza v Ljubljani, Fakulteta za računalništvo in informatiko
marjan.krisper@fri.uni-lj.si

Povzetek

Uspešno uvajanje elektronskih storitev je eden glavnih ciljev sodobne e-uprave in uspeh uvajanja je v veliki meri odvisen tudi od uporabnikov in njihovega zaupanja v storitve, varno e-poslovanje in zasebnost njihovih osebnih podatkov. Digitalni podpis je varnostni element, ki je pogosto prisoten v takih storitvah, vendar ima nekaj kritičnih pomanjkljivosti, ki jih lahko odpravimo z uporabo časovnega žiga. Časovni žig ne dodaja samo varnega zapisa časa, temveč ponuja mnoge dodatne lastnosti, ki povečujejo stopnjo varnosti in zaupanja med uporabniki. Ker so digitalna potrdila precej razširjena v današnji informacijski družbi za elektronsko identifikacijo ali overjanje, je uvedba in uporaba digitalnih podpisov dokaj preprosta. Vendar mora biti natančno načrtovana, saj imajo pomanjkljivosti, ki peljejo do zlorab, kritične razsežnosti. Brez popolnega zaupanja uporabnikov v e-upravo in njene storitve pa le-te ne bodo nikoli zaživele. Slovenska uprava ima trenutno kljub dobri infrastrukturi in pravnim podlagam zelo malo dobrih in zaupanja vrednih storitev, ki bi vključevale digitalno podpisovanje. Razlog za to je tudi pomanjkljivost digitalnega podpisa.

Abstract

Time stamping, the necessary component of safe e-business

Successful delivery of electronic services is a prime goal of modern e-government and their introduction will be successful only if users that the services, e-government and privacy of their personal data. Digital signature is an enabling security element of these services but it has a few critical deficiencies that can be surpassed with the use of time stamp. It does not only add a precise time to the data but also offers many elements that increase security and trust. Since digital certificate is widely used for authentication, digital signature should be easily implemented. However, the implementation has to be studied carefully as the abuse can have critical dimensions. Without utmost percent trust of users, e-government and its services will never come to life. Slovenian e-government is in at present supported by good infrastructure, good legal background, but has very few trusted services. One of the reasons is deficiency of digital signature.

Uvod

Javna uprava mora slediti modernizaciji družbe in najnovejšim tehnološkim dosežkom. To kažejo tudi koristi, ki so opazne v zasebnem sektorju. S pomočjo informacijske tehnologije je mogoče doseči in zadovoljiti več uporabnikov in povečati kakovost dela. Na eni od nedavnih konferenc na temo e-uprave je bilo podanih nekaj tez glede omenjenega razvoja [12]. Ena od tez govori, da je ponujanje storitev uspešno le, če imajo uporabniki storitev (državljani, zasebni sektor ali zaposleni v upravi) zaupanje pri izvajanju transakcij in zaupajo e-upravi.

Enaka raven zaupanja se je zahtevala v preteklosti in bo zaželena tudi v prihodnje. Za doseganje varnostnih ciljev je treba uporabiti različne tehnike in poiskati celovite rešitve. V primeru zaupanja in varnosti govorimo o overjanju, celovitosti, nezanikanju, zaupnosti in avtorizaciji.

Ena najbolj razširjenih tehnologij za zagotavljanje različnih varnostnih funkcij je infrastruktura javnih ključev (angl. public key infrastructure – PKI), ki temelji na asimetrični kriptografiji in digitalnih potrdilih. Pošiljatelj ob uporabi naslovnikovega javnega ključa in programske opreme, ki pozna šifrirni algoritem, izdela šifrirano sporočilo v elektronski obliki – tajnopis. Nato sporočilo digitalno podpiše z uporabo svojega tajnega ključa. Vse skupaj nato pošlje naslovniku. Postopek torej ostaja enak, le tehnike so se od rimskih časov spremenile in se bodo verjetno spreminjale tudi v prihodnje.

Varne storitve v e-upravi

Pri prehodu v informacijsko družbo se dokumenti namesto na papirju vse pogosteje pojavljajo v elektronski

obliki. Komuniciranje poteka prek računalniških omrežij, interneta in intraneta. Lastnoročni podpis se umika elektronskemu. V procese v zasebnem in javnem sektorju se vključuje nove tehnologije in zaradi tega pogosto uvede nov način dela. V novem okolju je treba zagotoviti varnost in zaupanje za izvajanje teh procesov. Eno od področij, na katero prodira informatizacija, je tudi uprava, ki počasi postaja e-uprava. Ta je torej tisti del celotnega sistema javne uprave, ki uporabniku na podlagi uporabe sodobne informacijske tehnologije ponuja bistvene informacije in storitve kjerkoli, kadarkoli in kakorkoli, na vseh ravneh upravljanja in vodenja ter jo ta uporablja za spremembo načina in vsebine svojega delovanja – za modernizacijo. E-uprava kot nova oblika uprave in upravljanja se vsakodnevno srečuje z novimi izzivi. Večina držav že izvaja različne strategije in akcijske načrte, politiki obljubljajo boljše življenje v novi družbi. Uporabniki ob poslušanju in spoznavanju pričakujejo veliko. Če bodo storitve, ki jih ponuja e-uprava, zadovoljile njihove potrebe, jih bodo tudi uporabljali, sicer bo ves trud zaman. Zatorej je vse odvisno od uporabnikov. Storitve morajo biti učinkovite, hitre, preproste za uporabo in varne. Uporabniki morajo zaupati v tehnike, ki storitve podpirajo. Zato mora e-uprava skrbno preučiti in uporabiti najbolj napredne, a hkrati zanesljive varnostne tehnologije, da si pridobi zaupanje uporabnikov in uspe.

Digitalni podpis, digitalno potrdilo in časovni žig

V elektronskem svetu obstajajo dokumenti[1] v elektronski obliki in tako kot podpisujemo papirne dokumente, potrebujemo podoben postopek za podpisovanje dokumentov v elektronski obliki. Podobno kot lastnoročni mora tudi elektronski podpis dokazovati pristnost in dokončnost dokumenta [11]. Unikatni podpis mora biti tak, da je kasneje mogoče dokazati, da se je podpisal prav ta podpisnik. Elektronski podpis je lahko katerikoli podpis v elektronski obliki, medtem ko je digitalni podpis posebna oblika elektronskega podpisa, izdelana z uporabo asimetrične kriptografije in pripadajočih algoritmov. Asimetrična kriptografija je danes ena najpogosteje uporabljenih metod in temelji na paru različnih ključev (tajni in javni), ki sta matematično povezana[2] [1]. Tajni ključ je niz bitov, ki je varno shranjen pri lastniku, pogosto na pametni kartici ali osebnem računalniku in zaščiten z geslom. Drugi, javni ključ, je na voljo vsakemu uporabniku, vendar je ugotovitev tajnega ključa iz javnega nemogoča oz. neizračunljiva v razumnem času. Tajni ključ je uporabljen za izdelavo podpisa, medtem ko je javni ključ potreben za preverjanje podpisa. Pomembna razlika v primerjavi s simetrično kriptografijo, ki se je pojavila že prej, je, da je pri simetrični kriptografiji za šifriranje in dešifriranje uporabljen enak ključ. Vendar v tem primeru nastane problem izmenjave ključa, torej kako naj pošiljatelj, ki je generiral ključ, le-tega varno dostavi prejemniku, ki mora sporočilo dekodirati. Te težave pri asimetrični kriptografiji ni, saj je ključ za preverjanje podpisa javen in dostopen vsakomur. Uporabnik, ki želi uporabljati digitalni podpis, s pomočjo ustrezne programske ali strojne opreme izračuna par ključev. Tajni ključ varno shrani in zaščiti z geslom, javni ključ pa objavi. Lahko ga tudi pošlje osebam, s katerimi želi varno komunicirati po elektronski pošti.

V procesu podpisovanja podpisnik šifrira dokument s svojim tajnim ključem. V resnici podpisnik v praksi podpiše povzetek dokumenta. Povzetek je nekakšen prstni odtis podpisanega dokumenta in je izdelan s pomočjo zgostitvene funkcije, ki kot rezultat vrne povzetek fiksne dolžine, izračunan iz podatkov poljubne dolžine. Zgostitvena funkcija je natančneje imenovana enosmerna nekolizijska zgostitvena funkcija. Njena bistvena lastnost je, da nihče ne more na podlagi povzetka (v razumnem času) izračunati ali pridobiti podatkov ali rekonstruirati dokumenta. Prav tako je (v razumnem času[3]) nemogoče izdelati dva različna dokumenta, ki bi kot rezultat zgostitvene funkcije dala enak povzetek. Prednost uporabe kratkega povzetka pri digitalnem podpisovanju je hitrejši izračun podpisa in njegova manjša dolžina. Torej je tehnično gledano digitalni podpis niz bitov, pridobljenih s kodiranjem povzetka s pomočjo tajnega ključa podpisnika, kjer je povzetek enolična predstavitev podpisanega dokumenta.

---

[1] *Dokument – informacijski objekt, ki je predstavitev kakršnihkoli podatkov, kot je besedilo, fotografija, video ali zvočni zapis, računalniški program ali kakršnakoli druga oblika podatkov oz. kombinacija le-teh, urejenih ali neurejenih, podana na neki materialni podlagi ali predstavljena digitalno [13].*

[2] *Za znani asimetrični algoritem RSA je javni ključ par števil (n,e), zasebni ključ petorček (n, p, q, e, d), kjer sta p in q naključno izbrani tuji praštevili, $n = p*q$, e tak, da velja $gcd(e,(p-1)*(q-1))=1$ in $d = e^{-1} \bmod (p-1)*(q-1)$.*

[3] *V tuji literaturi se uporablja izraz "computationally infeasible", kar pomeni, da je neko nalogo nemogoče opraviti v nekem realnem, smiselnem času, v katerem bi bil rezultat opravljene naloge še uporaben [11].*

Oseba, ki podpis preverja, dešifrira digitalni podpis s podpisnikovim javnim ključem in pridobi povzetek. Hkrati iz prejetega dokumenta z enako zgostitveno funkcijo, kot je bila uporabljena pri podpisovanju, izračuna povzetek prejetega dokumenta. Če se povzetka ujemata, je podpis overjen. Težava nastane, ko mora prejemnik sporočila ugotoviti, ali za preverjanje uporabljeni javni ključ res pripada podpisniku. Rešitev je v digitalnem potrdilu, ki vsebuje javni ključ, njegovo verodostojnost pa potrdi zaupanja vredna tretja oseba (angl. trusted third party – TTP). Digitalno potrdilo je skupek podatkov, ki najpogosteje vključuje osebne ali identifikacijske podatke lastnika, javni ključ, rok veljavnosti in dodatne tehnične podatke in ga je digitalno podpisal t. i. overitelj digitalnih potrdil (angl. certification authority – CA). Prav tako vključuje identifikacijske podatke overitelja. Digitalno potrdilo je identifikacijski dokument digitalnega sveta, tako kot je npr. osebna izkaznica identifikacijski dokument analognega sveta. Če oseba, ki preverja veljavnost digitalnega podpisa, zaupa overitelju digitalni potrdil, zaupa torej podatkom v digitalnem potrdilu in tako zaupa verodostojnosti javnega ključa, ki ga uporablja za preverjanje digitalnega podpisa. Da bi uporabnik lahko zaupal overitelju, mora zaupati njegovemu digitalnemu potrdilu. Overitelji se lahko povezujejo v različne hierarhične ali drugačne strukture, kjer je najpogosteje eden med njimi korenski overitelj, torej najvišja instanca, potrebna absolutnega zaupanja. Če je overitelj del hierarhije, je njegovo digitalno potrdilo podpisano od overitelja z višje ravni hierarhije, ki mu mora uporabnik ravno tako zaupati. Ker uporabnik ne more preveriti verodostojnosti digitalnega potrdila korenskega overitelja, saj je sam sebi podpisan, mora korenski overitelj objaviti svoje digitalno potrdilo, torej svoj javni ključ na zaupanja vreden način, npr. v znanem časopisu, v splošno razširjenih programih, kot so spletni brskalniki, ali programih za elektronsko pošto svetovno znanih proizvajalcev.

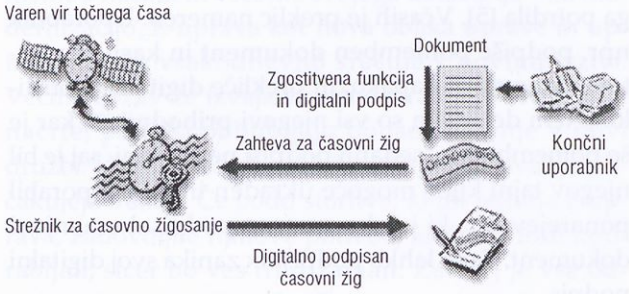
Vsak uporabnik, ki želi uporabljati digitalne podpise, mora torej dobiti digitalno potrdilo od overitelja. Overitelji so državne ali mednarodne javne ali zasebne organizacije. Ob izdaji digitalnega potrdila digitalno podpišejo podatke o lastniku in njegov javni ključ in s tem jamčijo za verodostojnost teh podatkov.

Vsako digitalno potrdilo ima časovno omejitev, t. i. rok veljavnosti (tudi korensko digitalno potrdilo korenskega overitelja). Ko rok veljavnosti poteče, digitalni podpis, izdelan in overjen z javnim ključem iz pretečenega digitalnega potrdila, ni več veljaven. To je med drugim varnostni ukrep zaradi novih tehnologij in vedno hitrejših računalnikov, ki se bodo pojavljali v prihodnosti. Če bi bilo digitalno potrdilo trajno, bi bilo namreč mogoče čez nekaj desetletij z osebnim računalnikom tistega časa v kratkem času s poizkušanjem ugotoviti ključ in ponarejati podpise. Zato vsi digitalni podpisi, izdelani po preteku digitalnega potrdila, niso več veljavni. Še več, vsi obstoječi digitalni podpisi postanejo neveljavni. To velja tako za uporabniška digitalna potrdila, kot tudi za digitalna potrdila overiteljev. Ker so digitalna potrdila lahko tudi preklicana, npr. zaradi ogrožene varnosti ali kraje tajnega ključa, velja enako tudi ob preklicu digitalnega potrdila [5]. Včasih je preklic nameren. Uporabnik npr. podpiše pomemben dokument in kasneje ugotovi, da je storil napako, in prekliče digitalno potrdilo. S tem dejanjem so vsi njegovi prihodnji in, kar je še pomembnejše, sedanji podpisi neveljavni, saj je bil njegov tajni ključ mogoče ukraden in ga je uporabil ponarejevalec, ki je zlonamerno podpisal omenjeni dokument. Tako lahko podpisnik zanika svoj digitalni podpis.

Časovno žigosanje

Kot lahko vidimo iz zgornjega besedila, je časovna komponenta pomemben dejavnik v primeru digitalnega podpisovanja. Poleg tega lahko iz izkušenj pri uporabi papirnih dokumentov ugotovimo, da ima skoraj vsak uradni dokument časovni zaznamek (datum), ki pove, kdaj je dokument nastal ali kdaj je bil podpisan. Enake potrebe se pojavljajo v primerih elektronskih dokumentov. Včasih lahko zaupamo datumu v dokumentu, ker tako trdi zaupanja vredna oseba, vendar v določenih primerih to ni dovolj. Treba je zagotoviti varen in zanesljiv zapis časa, ki je pripet na podatke ali kako drugače povezan s podatki in določa, da so podatki v takšni obliki obstajali v tistem trenutku ali prej. To dosežemo s časovnim žigom. Časovni žig je dodatek k dokumentu, zapisanem v elektronski obliki, ki določi čas obstoja, medtem ko digitalni podpis določi avtorja in vsebino. Je digitalno podpisan par podatkov – čas in povzetek dokumenta (ali digitalni podpis dokumenta) s strani overitelja časovnih žigov. Za časovno žigosanje obstaja več metod, ki omogočajo določiti, da je dokument obstajal v določeni obliki v določenem času (ne pa, kdaj je nastal). Včasih časovni žig omogoča le določitev časovnega zaporedja, tj. ali je dokument A obstajal pred dokumentom B ali

obratno. Seveda je nadvse praktično, če je zapis časa čim bliže uradno veljavnemu času, torej tistemu, ki ga uporabniki uporabljajo v vsakdanjem življenju [1]. Obstajati mora zaupanja vreden časovni vir, ki mu uporabniki zaupajo, in zaupanja vredna organizacija, ki bo ponujala tako storitev. V praksi po navadi deluje zaupanja vredna tretja oseba, imenovana overitelj časovnih žigov (angl. time stamping authority – TSA). Ponuja storitev časovnega žigosanja (angl. time stamping service – TSS). Časovni žig je torej elektronsko podpisano potrdilo overitelja, ki potrjuje vsebino podatkov, na katere se nanaša, v navedenem času [10]. Potek žigosanja je prikazan na sliki 1.



Slika 1: **Potek časovnega žigosanja [2]**

Uporabnik napiše dokument, ga digitalno podpiše in pošlje zahtevo overitelju časovnih žigov. Ta pridobi točen čas od zaupanja vrednega vira točnega časa,[4] ga doda prispeli zahtevi in vse skupaj digitalno podpiše s svojim tajnim ključem, izdelani časovni žig pa nato vrne uporabniku. Ker overitelj časovnih žigov prejme le povzetek uporabnikovega dokumenta, je s tem zagotovljena njegova tajnost. Ker je pri postopku uporabljena tehnologija digitalnega podpisovanja, sta pri tem zagotovljena celovitost in overjanje. Uporabnik lahko preveri pravilnost časovnega žiga takoj po prejetju in s tem prepreči spregled napak pri prenosu podatkov. Zapisani čas lahko preveri in se prepriča, ali je le-ta res pravi. Preveri lahko v časovnem žigu vključeni povzetek ter tako ugotovi, da je bil časovno žigosan povzetek njegovega dokumenta.

Uporaba časovnih žigov zagotavlja overjanje digitalnih podpisov tudi za nazaj. Kot je bilo omenjeno, bi bili brez časovnega žigosanja vsi digitalni podpisi neveljavni v trenutku, ko poteče veljavnost pripadajočega digitalnega potrdila ali pa je bilo le-to preklicano. Če pa je dokument časovno žigosan, lahko oseba, ki preverja veljavnost digitalnega podpisa, preveri, ali je bil dokument podpisan pred potekom veljavnosti digitalnega potrdila, torej ko je bilo potrdilo še veljavno, ali ne.

S časovnim žigosanjem zato lahko zagotovimo nezanikanje. Čeprav se to pripisuje že uporabi digitalnih podpisov, je to napačna trditev. Le z uporabo časovnega žigosanja uporabnik namreč ne more s preklicem digitalnega potrdila zanikati digitalnega podpisa določenega dokumenta, ker s časovnim žigom lahko dokažemo, da je bilo digitalno potrdilo v času podpisovanja, torej pred preklicem ali pretekom veljavnosti digitalnega potrdila, še veljavno.

Novi znanstveni dosežki bodo v prihodnosti omogočili, da bodo že osebni računalniki hitro določili ali izračunali tajni ključ. Zatorej bi moral podpisnik podpisovati že podpisane elektronske dokumente z vedno boljšimi in varnejšimi algoritmi. Toda podpisniki pogosto sami ne arhivirajo dokumentov, ki vsebujejo podpise. Razen tega bi morali uporabniki ponovno podpisovati vse že podpisane dokumente vsakič, ko bi pretekla veljavnost njihovemu digitalnemu potrdilu in bi si pridobili novo. Z uporabo časovnega žigosanja lahko arhivarji podaljšujejo veljavnost časovno žigosanega digitalno podpisanega dokumenta s ponovnim časovnim žigosanjem obstoječih časovnih žigov[5] ob uporabi novejše in varnejše tehnologije in tako ohranijo verodostojnost originalnega digitalnega podpisa in originalnega časovnega žiga.

Overitelj časovnih žigov

Edina težava, ki ostane, je zaupanje v overitelja časovnih žigov. Rešitev je povezovalna shema časovnih žigov. Obstaja veliko različnih shem ([4], [6]), ki vse omogočajo določevanje časovnega vrstnega reda časovnih žigov in zagotavljajo, da je overitelj časovnih žigov odgovoren za svoja dejanja ali da so le-ta (pravilna ali nepravilna) dokazljiva. Povezovalne sheme temeljijo na dejstvu, da je nemogoče napovedati prihodnje zaporedje zahtev za časovne žige in povzetke,

[4] *Overitelj časovnih žigov ima lahko svoj vir točnega časa, npr. atomsko uro, ali pa uporablja več točnih virov različnih institucij po svetu, ki tak vir zagotavljajo.*

[5] *Nikoli ponovno ne žigosamo dokumenta, saj bi mu s tem dodali nov časovni žig z novim časom. Pač pa ponovno žigosamo obstoječi časovni žig in mu s tem podaljšamo veljavnost.*

ki jih bodo le-ti vključevali. Če določen časovni žig vključuje del podatkov prejšnjega, potem obstaja dokaz, da je bil tekoči časovni žig izdelan po časovnem žigu, katerega del je vanj vključen [3]. Ker bodo podatki tekočega časovnega žiga vključeni v podatke prihodnjih časovnih žigov, je zagotovljeno, da je bil tekoči časovni žig izdelan pred časovnimi žigi, nastalimi na podlagi zahtev v prihodnosti, ki vključujejo del njegovih podatkov. Taka rešitev mora seveda omogočati preveritev časovne verige žigov. V praksi se manjša časovna veriga (najpogosteje v obliki uravnoteženega Merkelejevega drevesa) izdela v nekem časovnem intervalu, npr. v eni sekundi, in torej obsega med seboj povezane podatke vseh časovnih žigov, ki so bili izdelani v tem intervalu. Skupni povzetek vseh časovnih žigov intervala se poveže s povzetkom iz prejšnjega časovnega intervala in tako tvori novo, t. i. super verigo časovnih žigov vseh intervalov. Periodično (npr. enkrat tedensko) pa se javno objavi skupni povzetek vseh povzetkov in tako izdela splošno objavljeno in nespremenljivo obliko zapisa. Javne objave tako diseminirajo in arhivirajo skupni povzetek v različnih arhivih in knjižnicah. V primeru e-uprave je medij lahko Uradni list.

Z uporabo časovnih žigov digitalno podpisani dokumenti ne pridobijo samo časovne komponente, temveč poleg obstoječe zaupnosti, celovitosti in verodostojnosti pridobijo tudi lastnost nezanikanja in mesto v času. Z uporabo povezovalnih verig ni več potrebno slepo zaupanje v overitelja časovnih žigov. Tako uporabniki pridobijo zaupanja vreden način, ki omogoča uporabo digitalnega podpisovanja in pošiljanja elektronskih dokumentov pri različnih storitvah, ki jih ponujata tako zasebni sektor kot javna uprava.

Tehnični vidiki časovnega žigosanja v upravi

Za uvajanje storitev e-uprave morajo biti izpolnjeni določeni tehnični pogoji. Najprej potrebujemo pravne podlage na področju uporabe novih tehnologij. Brez teh e-uprava ne funkcionira. Mnogo držav je že sprejelo zakone o elektronskem poslovanju ali podpisu. Ti pravni akti so se pogosto osredotočili na dve osnovni načeli, ki sta definirani tudi v direktivi Evropske unije [7], ki so jo sprejele države članice in nekatere države kandidatke. Prvo načelo določa, da elektronski podpis, ki temelji na kvalificiranem digitalnem potrdilu[6] in je izdelan z varno napravo za podpisovanje, zadošča pravnim zahtevam podpisa v odnosu do dokumentov v elektronski obliki, kot so določene za lastnoročni podpis v odnosu do papirnih dokumentov. Drugo načelo določa, da kadarkoli katerikoli drugi pravni akt omenja papirno obliko dokumenta, imamo elektronsko obliko za enakovredno in pravno veljavno, če je dostopna in uporabna za določeno časovno obdobje.

Poleg teh pa pravni akti o elektronskih in digitalnih podpisih v različnih državah vključujejo še člene o časovnem žigosanju in časovnih žigih. Večina ponudi le opise osnovnih definicij in ne posega v potrebne dodatne razlage, kot npr. avstrijski zvezni zakon o elektronskem podpisu [8] ali slovenski zakon o elektronskem poslovanju in elektronskem podpisu [10]. Drugi, kot na primer estonski zakon o digitalnem podpisu [9], natančno in jasno določajo storitev časovnega žigosanja ter overitelja časovnih žigov. Ker časovno žigosanje danes še ni spoznano kot nujni del infrastrukture javnih ključev, je pomanjkljiva pravna podlaga naloga, ki jo je treba rešiti v bližnji prihodnosti. Glede na pomanjkljivosti digitalnega podpisovanja, tj. da postanejo vsi digitalni podpisi ob preklicu ali preteku veljavnosti digitalnega potrdila neveljavni, pa različni pravni akti ponujajo različne rešitve. Slovenski zakon zahteva od podpisnika, da ponovno podpiše vse dokumente, ki jih je podpisal in se navezujejo na določeno digitalno potrdilo, ki je prenehalo veljati. Tak način reševanja je v praksi težko izvedljiv. Druga možnost, ki jo omenjajo pravni akti nekaterih držav, pa je dodajanje (overjanje) podpisov elektronskih notarjev ali pa overiteljev časovnih žigov.

Tehnološki vidik zahteva ustrezno infrastrukturo, ki omogoča izvajanje aktivnosti. Postavitev informacijske infrastrukture je zahtevna naloga in eno od temeljnih opravil, ker upošteva vse storitve, ki na njej temeljijo, torej celotno e-poslovanje. V okviru varnostnih storitev je treba poskrbeti za ustrezne postopke, ki se nanašajo tako na ponudnika kot na odjemalca. Na strani ponudnikov je treba zagotoviti zadostno število varnih spletnih strežnikov, požarnih zidov, intranetne povezave in podatkovne baze. Na strani odjemalcev pa zadostno

[6] *Izraz je uporabljen v direktivi in slovenskem zakonu o elektronskem poslovanju in elektronskem podpisu. Takšno potrdilo ima enake značilnosti kot običajno potrdilo, le da zakon zanj podrobneje predpisuje vsebino ter način izdaje, uporabe in preklica [10].*

število ponudnikov dostopa do interneta, javne dostopne točke in cenene povezave. Vse mora potekati po varnih poteh z varnimi protokoli.

Za uporabo digitalnega podpisovanja in časovnega žigosanja je treba postaviti infrastrukturo javnih ključev. Zagotoviti je treba obstoj enega ali več overiteljev, ki so lahko organizirani s strani uprave ali pa priznani in zaupanja vredni overitelji iz zasebnega sektorja. Uprave v različnih državah pogosto vzpostavijo svojega overitelja in omogočijo obstoječim in novim overiteljem zasebnega sektorja pridobitev akreditacije za izdajanje digitalnih potrdil, ki se uporabljajo pri elektronskem poslovanju z upravo. Za potrebe časovnega žigosanja pa je treba uvesti tudi overitelja časovnih žigov. Najlažji način je, da dodelimo overitelju digitalnih potrdil še možnost overjanja časovnih žigov. Določiti in vzpostaviti je treba vir točnega časa, ga povezati z overiteljevim informacijskim sistemom za izdelavo časovnih žigov in omogočiti uporabnikom časovno žigosanje njihovih dokumentov. Ker sta v takem primeru overitelj digitalnih potrdil in overitelj časovnih žigov isti organ, je treba zaupati le enemu korenskemu potrdilu, ki podpira celotno infrastrukturo. Šele po uspešno vzpostavljeni infrastrukturi lahko uprava začne ponujati varne in zaupanja vredne storitve.

Znanje je pomemben dejavnik pri ponujanju varnih e-storitev. Zato je treba prihodnje uporabnike izobraževati za uporabo informacijske tehnologije, in jim hkrati obrazložiti varnostne postopke ter tako pridobiti njihovo zaupanje v ponujene storitve. Nihče ne bo uporabljal plinskega štedilnika, če se boji plina; nihče ne bo digitalno podpisoval dokumentov, če bi ga bilo strah, da bodo lahko poneverjeni.

Primer Slovenije

Slovenija je tranzicijska država, ki poizkuša kar se da hitro doseči nivo informacijsko razvitih zahodnih držav. Hkrati se pridružuje Evropski uniji in prilagaja njenemu pravnemu redu. Slovenska vlada se trudi izpeljati spremembe učinkovito in brez večjih napak. E-uprava kot politični, ekonomski in socialni cilj je na seznamu desetih najpomembnejših nalog. Ker je bila e-uprava ena od velikih obljub zadnjih volitev, pričakujejo volivci od vlade rezultate. Slovenija je bila povabljena tudi v NATO in to je še eden od pomembnih premikov v slovenski družbi. Vse to postavlja slovensko upravo v težaven položaj.

Slovenska pravna podlaga za varno poslovanje e-uprave je bila določena leta 2000, ko je bil v skladu z direktivo Evropske unije sprejet zakon o elektronskem poslovanju in elektronskem podpisu [10]. Zakon je upošteval osnovni načeli enakosti elektronske in papirne oblike ter elektronskega in lastnoročnega podpisa, podani v direktivi EU. Tudi nekateri drugi pravni akti so morali biti spremenjeni, da niso bili v protislovju z omenjenim zakonom, da niso ovirali razvoja e-uprave in da so usklajeni s strategijo e-poslovanja uprave do leta 2004. Na določenih pravnih področjih zadeve še niso urejene.

Slovenski zakon določa časovni žig kot elektronsko podpisano potrdilo overitelja časovnih žigov, ki jamči za povezavo med dokumentom, na katerega se nanaša, in časom, vpisanim v njem. Prav tako 25. člen govori, da se za časovni žig in storitve, povezane z njim, smiselno uporabljajo določbe, ki urejajo potrdilo in kvalificirano potrdilo, vendar podrobneje ne omenja storitve časovnega žigosanja in overitelja časovnih žigov. Za resno delovanje storitve časovnega žigosanja sta omenjeni zakon in pripadajoča uredba [14] premalo.

Po sprejetju zakona [10] je bila vzpostavljena tudi infrastruktura javnih ključev. Dva korenska overitelja sta bila vzpostavljena na Centru vlade za informatiko. Prvi, SIGOV-CA, izdaja digitalna potrdila za zaposlene v javni upravi in drugi, SIGEN-CA, za uporabnike, tj. državljane in zasebni sektor. Zaposleni v javni upravi so ponekod pridobili tudi naprave za uporabo pametnih kartic, medtem ko morajo uporabniki to težavo reševati sami.

Trenutno v Sloveniji še nimamo overitelja časovnih žigov za področje e-storitev uprave. Na Centru vlade za informatiko imajo vir točnega časa in uporabljajo rešitve podjetja Entrust, ki je eden vodilnih proizvajalcev na svetu. Njegove rešitve vključujejo tudi možnost vzpostavitve overitelja časovnih žigov, kar je ena od možnih rešitev za slovensko e-upravo. Po zadnjih podatkih naj bi bila ta rešitev tudi izpeljana in v določeni meri funkcionalna še letos.

Spletni portal e-uprava je postavljen in že nekaj časa ponuja prve storitve e-uprave ob uporabi digitalnih potrdil omenjenih overiteljev. Nekatere od teh storitev so na voljo brezplačno, čeprav mora zanje državljan, če jih opravi po normalni (neelektronski) poti, plačati takso. Storitev omogoča uporabnikom pridobitev izpiskov iz matičnih knjig in vpogled v

centralni register prebivalstva ob uporabi digitalnega potrdila, ki omogoča overjanje in identifikacijo uporabnika. Zaposleni, ki delajo v organih uprave in predstavljajo ponudnika storitev, uporabljajo digitalna potrdila za dostop do podatkovnih baz, ki vsebujejo vloge uporabnikov po izpiskih in te vloge rešujejo. Rezultat teh postopkov je izpis na papirju, ki ga naročnik prejme po pošti. Slaba stran tega je, da je bila ta storitev vpeljana zaradi političnih predvolilnih obljub. Od takrat se je v okviru ponujenih storitev zgodilo zelo malo. Še slabše: izpiski, pridobljeni po elektronski poti in dostavijo v papirni obliki, se ponovno uporabljajo kot priloge papirnim vlogam za postopke v javni upravi.

Trenutno za končnega uporabnika še ne obstaja storitev, ki bi uporabljala digitalne podpise ali časovne žige. Podobna situacija obstaja v mnogih drugih državah, kjer digitalna potrdila uporabljajo za overjanje in identifikacijo, medtem ko je storitev, ki uporabljajo digitalni podpis ali časovni žig, malo ali pa jih sploh ni. Vendar kaže, da bo že dolgo pričakovana e-dohodnina prvi korak v tej smeri in bo na voljo že v prihodnjem letu.

Smo pripravljeni?

Nedavno so predstavniki skupine GartnerGroup na svoji spletni strani objavili, da mnogi projekti uvajanja e-storitev v upravi ne pomagajo niti državljanom niti upravi sami. Ne samo, da politične obljube o manjših stroških z manj zaposlenimi v sodobnih upravah niso uresničljivi zaradi močnih sindikatov in strahu pred povečano nezaposlenostjo v državi, temveč tudi hitro uvajanje slabih e-storitev doseže slab učinek pri uporabnikih. Vse prepogosto so take e-storitve kompleksne in jim uporabniki ne zaupajo.

Več kot 6000 izdanih digitalnih potrdil za državljane slovenskega overitelja na Centru vlade za informatiko obljublja uporabo e-storitev, vendar bodo brez časovnega žigosanja državljani ta digitalna potrdila lahko uporabljali le za identifikacijo. Ko bo treba podpisovati vloge, priloge, elektronska sporočila, pa bo treba zagotoviti časovno žigosanje, ki bo poleg zagotavljanja nezanikanja omogočalo tudi varno in dolgoročno zagotavljanje verodostojnosti podpisov in podpisane vsebine. Le tako bo e-uprava uspela pridobiti zaupanje uporabnikov in vpeljati sodobne e-storitve kot mnoge razvite države v svetu.

Literatura

1. Admas, C., Lloyd, S.: Understanding Public-Key Infrastructure. Macmillan Technical Publishing, Indiana ZDA (1999).
2. Entrust: Entrust/Timestamp, URL="http://www.entrust.com/ entrust/timestamp/ index.htm" (2001).
3. Bayer, D., Haber, S., Stornetta, W. S.: Improving the Efficiency and Reliability of Digital Time-Stamping. Sequences II: Methods in Communication, Security, and Computer Science. Springer-Verlag, Berlin, Heidelberg, New York (1993) 329–334.
4. Buldas, A., Laud, P., Lipmaa, H., Villemson, J.: Time stamping with binary linking schemes. Advances in Cryptology – CRYPTO'98, LNCS 1462. Springer-Velrag, Berlin Heidelberg New York (1998) 486-501.
5. Maniatis, P., Baker, M.: Enabling the archival storage of signed documents, Computer Science Department, Stanford University, 24th July 2001.
6. Benaloh, J., de Mare, M.: Efficient Broadcast time-stamping. Technical report 1, Clarkson University Department of Mathematics and Computer Science (1991).
7. European Community: A European Initiative on Electronic Commerce. COM(97) 157 (1997).
8. Austrian Federal Electronic Signature Law (Signature Law - SigG) (2000).
9. Tõlge inglise keeled: Eesti Õigustõlke Keskus, Estionian Digital Signatures Act, (RT I 2000, 26, 150), Estonian Legal Translation Centre (2000). URL="http://www.riik.ee/riso/digiallkiri/digsignact.rtf".
10. Zakon o elektronskem poslovanju in elektronskem podpisu. Uradni list Republike Slovenije, 57/2000 (2000).
11. American Bar Association: Digital Signature Guidelines (1997).
12. Lenk, K., Traunmüller, R., Electronic Government: Where Are We Heading? Lecture Notes in Computer Science, Springer-Verlag Heidelberg. Volume 2456/2002, Electronic Government: First International Conference, EGOV 2002, Aix-en-Provence, France, September 2–5, 2002. Proceedings.
13. Gladney, H.M., Digital documents Quarterly, Glossary and acronyms, URL="http://home.pacbell.net/hgladney/ ddqgloss.htm" (2003).
14. Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje. Ur. list RS, št.77/2000, 2/2001.

Mag. Mitja Dečman je leta 2001 končal magistrski študij na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Zaposlen je kot asistent na Fakulteti za upravo v Ljubljani, kjer se poleg pedagoškega dela na področju informatike v upravi ukvarja še z raziskavami s področja varnosti informacijskih sistemov, infrastrukture javnih ključev in elektronskih storitev v javni upravi.

Dr. Marjan Krisper je predstojnik katedre za informatiko na Fakulteti za računalništvo in informatiko in od ustanovitve leta 1992 predstojnik Laboratorija za informatiko. Je član več znanstvenih in strokovnih združenj, med drugim ustanovitveni član AIS (Association for Information Systems) – svetovne zveze univerzitetnih učiteljev informacijskih sistemov, Slovenskega društva INFORMATIKA, Društva za umetno inteligenco in INFOS-a. Je avtor številnih raziskav, elaboratov, ekspertiz, znanstvenih in strokovnih sestavkov. Vodi številne projekte razvoja informacijskih sistemov in izvajanja metodologij razvoja v največjih sistemih v gospodarstvu, državni upravi in javnem sektorju.