PRAVNA UREDITEV VARNIH E-IDENTITET

izdelal: Inštitut za ekonomijo, pravo in informatiko (c), www.iepri.si

1. Uvod

Področje e-identitet v Sloveniji trenutno ni vzpostavljeno na optimalnem nivoju, tako v javni upravi, kot tudi v zasebnem sektorju. Pri identifikaciji v javni upravi je težava v nedostopnosti naprav za tvorjenje varnih elektronskih podpisov uporabnikom upravnih storitev (javnim uslužbencem so takšne naprave zagotovljene, ostalim uporabnikom pa ne), v zasebnem sektorju pa so takšne naprave uporabnikom sicer dostopne, a zakonodajno niso ustrezno urejene, kar vnaša negotovost in heterogenost v področje elektronskega poslovanja. Varno elektronsko podpisovanje in uporaba kvalificiranih potrdil je, delno zaradi različnosti potrdil in naprav za tvorjenje varnih elektronskih podpisov, tudi precej zahtevna, tako za uporabnike (podpisnike), kot tudi za ponudnike e-storitev.

Za izboljšavo stanja bi bilo torej treba urediti uporabo varnih e-identitet, ki bi odpravljale navedene pomanjkljivosti. Pri vprašanju uvajanja varnih e-identitet so vodilo pravne ureditve cilji, ki jih sistem e-identitet zasleduje ter tehnični in organizacijski pristopi, s katerimi se te cilje uresničuje. Pravna ureditev pri tem večinoma predstavlja le izvedbeno tehniko enega ali drugega instrumenta za dosego cilja, ne predstavlja pa najpomembnejšega dejavnika, ki bi omejeval ali onemogočal določene rešitve. Če ima neka rešitev torej tehnično ali organizacijsko bistveno boljše značilnosti od druge, drugo (tehnično ali organizacijsko slabšo) rešitev pa je pravno lažje urediti, bodo verjetno dejanske pozitivne značilnosti prve pretehtale težave pri pravni regulaciji le-te.

Pravo predvsem preko načel sicer postavlja omejitve in podaja dobre prakse glede načina uvajanja rešitev (na primer posameznih deležnikov naj se pretirano ne omejuje, zagotavljati je potrebno konkurenco, racionalno porabo javnih sredstev in podobno), kljub temu pa je večji del pravne ureditve varnih e-identitet v svoji izvedbi prilagodljiv in odvisen od politike oziroma ciljev, ki se jih pri uvedbi sistema zasleduje. Pomembna je torej vsebina, ki se jo ureja (na primer zahteve glede overiteljev, zahteve glede naprav za tvorjenje varnih elektronskih podpisov, ureditev vsebine identifikatorjev v digitalnem potrdilu), manj pa je relevantno, ali se ta vsebina uredi v enem ali drugem zakonu ali podzakonskem aktu in pa, kako se posamezni instituti poimenujejo.

Uvodoma velja tudi poudariti, da mora biti vsaka izmed možnosti ureditve varnih e-identitet skladna z Direktivo Evropskega parlamenta in Sveta 1999/93/ES, z dne 13. decembra 1999 o okviru Skupnosti za elektronski podpis (Ur. l. L 13, 19/01/2000, v nadaljevanju: Direktiva).

2. Možnosti pravne in dejanske ureditve

Pravna ureditev varnih e-identitet bo vplivala predvsem na tri vrste deležnikov. To so ponudniki e-storitev, katerih storitve bodo uporabljale e-identitete, izdajatelji digitalnih potrdil, ki bodo potrjevali povezavo med osebo in njenim elektronskim podpisom in pa uporabniki, ki bodo tvorili elektronske podpise. Zaradi močne povezanosti pravne ureditve e-identitet z njihovo dejansko izvedbo in njihovim vplivom na vsakega izmed deležnikov, so v tem mnenju med drugim predstavljene tudi posledice posameznih možnosti na navedene deležnike. Pri tem so možnosti izvedbe sledeče:

- ureditev v Zakonu o osebni izkaznici (Ur. l. RS, št. 35/11, v nadaljevanju: ZOIzk-1);
- ločevanje med varnimi elektronskimi podpisi in kvalificiranimi elektronskimi podpisi, pri čemer so slednji varni elektronski podpisi, ustvarjeni z napravami za varno elektronsko podpisovanje in overjeni z digitalnimi potrdili. Ureditev se izvede s spremembo Zakona o elektronskem poslovanju in elektronskem podpisu (Ur. l. RS, št. 98/04, v nadaljevanju: ZEPEP);
- akreditirane e-identitete, ki bi se lahko uvedle na primer s pričetkom uporabe in podrobnejšo ureditvijo že obstoječega instituta akreditiranega overitelja v ZEPEP.

Ureditev v ZOIzk:

Prva možnost, to je ureditev v ZOIzk-1, je povezana predvsem z uvedbo elektronske osebne izkaznice. Takšna izkaznica bi bila lahko uvedena na različne načine, na primer kot edina osebna izkaznica ali kot alternativa oziroma dodaten instrument poleg že obstoječe. Lahko bi temeljila na tehnologiji kontaktnega čipa, brez-kontaktnega čipa, čipa ki je hkrati kontakten in brez-kontakten ali dveh čipov (kontaktnega in brez-kontaktnega) hkrati. Med navedenimi možnostmi so sicer manjše razlike (kontakten čip je na primer zaradi široke uporabe mnogim uporabnikom že poznan, brez-kontakten čip omogoča hitrejšo in enostavnejšo masovno avtentikacijo na javnih mestih), vendar te razlike s pravnega vidika na njihovo izbiro nimajo vpliva.

Pri uvajanju sistema varnih e-identitet je pomemben vidik tudi usklajenost z evropskim pravnim redom in upoštevanje dobrih praks s tega področja na evropski ravni. Glede dobrih praks velja izpostaviti dejstvo, da na ravni EU enotne smernice za evropske osebne izkaznice še niso določene in je materija (na primer glede elektronske uporabe osebne izkaznice) še v fazi dogovarjanja. Zaradi navedenega je zato treba upoštevati, da bi uvedba kakršnekoli e-osebne izkaznice pomenila vstopanje na področje, ki je trenutno neenotno in katerega smer razvoja je negotova. Šele po določitvi enotnih smernic za evropske osebne izkaznice bo namreč jasno, kakšne rešitve naj bi se uporabljale v prihodnosti in, kakšne rešitve bodo omogočale lažjo integracijo z rešitvami drugih držav članic. Odsotnost oz. pričakovanje določitve smernic predvsem glede elektronske uporabe evropske osebne izkaznice samo po sebi še ne pomeni, da uvedba rešitve e-osebne izkaznice ni priporočljiva, pomeni pa, kot ugotavlja že tudi Ministrstvo za notranje zadeve, da bi veljalo z njeno uvedbo, v kolikor bi bila izbrana kot najprimernejša rešitev, počakati.

Sprememba ZEPEP:

Trenutno predlagana sprememba ZEPEP odpravlja bistveno pomanjkljivost trenutnega sistema, to je zagotavljanje (oz. pravna ureditev) le ene vrste varnega elektronskega podpisa, ki ne zadošča raznolikosti dejanskih potreb (predlagana sprememba zakona ločuje med varnimi in kvalificiranimi elektronskimi podpisi). Z razlikovanjem med varnim elektronskim podpisom in kvalificiranim elektronskim podpisom se ohranja skladnost z Direktivo, ki ureja predvsem varni elektronski podpis, hkrati pa se tudi sledi potrebam po višjem nivoju varnega podpisovanja. Takšnega višjega nivoja Direktiva ne prepoveduje, posredno (preko uvajanja možnosti prostovoljne akreditacije) ga celo predvideva, pri tem pa (ob predpostavki, da se ohrani osnovni nivo varnega elektronskega podpisovanja) za višji nivo overjanja ne postavlja posebnih omejitev, temveč le zahteve, s katerimi se prepreči neutemeljeno omejevanje akreditiranih overiteljev. Zakonodajalec ima torej pri urejanju kvalificiranih digitalnih potrdil v veliki meri proste roke.

Kvalificirana digitalna potrdila je mogoče uporabljati v kombinaciji s širokim spektrom naprav za tvorjenje varnega elektronskega podpisa, na primer s pametnimi karticami s kontaktnim čipom, s pametnim USB ključem, z modulom HSM (*hardware security module*) in z mobilnimi telefonskimi napravami. Zaradi širokih možnosti dejanske aplikacije kvalificiranih digitalnih potrdil je zato ne glede na to, na kakšen način se bodo uvedle varne e-identitete, predlagana sprememba ZEPEP vsekakor dobra rešitev, kot temelj za morebitno nadaljnje pravno urejanje.

Akreditirana e-identiteta:

Akreditirana e-identiteta je tista e-identiteta, ki izpolnjuje dodatne zakonodajne zahteve glede avtentikacije uporabnika z digitalnim potrdilom. Overitelji bi tako lahko uporabnikom prostovoljno zagotavljali višji nivo avtentikacije, preverjanje ustreznosti tega nivoja pa bi se lahko izvajalo na primer ob vključitvi overitelja v akreditacijsko shemo. Možnost akreditacije ponudnikov overiteljskih storitev je bila v ZEPEP predvidena skladno z določbo Direktive, ki državam članicam dovoljuje, da uvedejo ali obdržijo prostovoljne akreditacijske sheme za zvišanje ravni overjanja. Pri tem prostovoljna akreditacija pomeni vsako dovoljenje, ki določa pravice in obveznosti v zvezi z opravljanjem overjanja, ki ga na zahtevo zadevnega overitelja izda javni ali zasebni organ, pristojen za določanje pravic in obveznosti in za nadzor njihovega spoštovanja, če overitelj pravic, ki izhajajo iz dovoljenja, teh ne sme izvajati tako dolgo, dokler ne prejme odločbe organa. Prostovoljna akreditacija overiteljev torej predstavlja institut, predviden že z evropskim pravnim redom, namenjen prav višjemu nivoju zagotavljanja varnih elektronskih podpisov.

Institut je pri nas z zakonom že predviden, za celovito ureditev tega področja pa manjka predvsem še določitev akreditacijskega organa in sprejetje pravilnika o pogojih za akreditacijo, na katerega se sklicuje predlagani spremenjeni 42. člen ZEPEP. Pri tem velja poudariti, da zakonodajno urejanje akreditacije overiteljev ni popolnoma ločen in samostojen instrument, ki bi ga lahko uporabili pri uvedbi e-identitet, pač pa je (oziroma je priporočljivo, da bi bil) povezan s trenutnim predlogom spremembe ZEPEP, kljub temu, da se predlog večinoma ne nanaša na akreditacijo. Za akreditacijo je med predlaganimi spremembami pomemben predvsem institut kvalificiranega elektronskega podpisa, podrobnejša določitev zahtev za naprave za tvorjenje varnega elektronskega podpisa in pa uvedba registra naprav za varno tvorjenje podpisa. Za navedene institute je torej priporočljivo, da so tesno povezani s pravilnikom akreditacijskega organa, ko bo le-ta sprejet, poleg tega pa se lahko v pravilniku zahteva izpolnjevanje tudi drugih (dodatnih ali strožjih) pogojev, ki se izkažejo za primerne. V tem smislu je akreditacijo mogoče obravnavati tudi kot nadgradnjo (ostalih) sprememb ZEPEP, za samo zagotavljanje višjega nivoja elektronskega podpisovanja in posredno tudi e-identitet sicer ne nujno potrebno, kljub temu pa pomembno tako za overitelje, kot tudi za uporabnike. Prvim daje akreditacija uradno potrdilo, da delujejo na višjem nivoju, »priznanje«, na katerega se lahko sklicujejo pri izkazovanju kakovosti svojih storitev na trgu, drugim pa daje zagotovilo, da z uporabo določene storitve overjanja (oziroma paketom, ki bo vključeval tudi napravo za tvorjenje varnega elektronskega podpisa) pridobijo najvišjo mero zanesljivosti pri podpisovanju svojih podatkov, ki bo v primeru dvoma v pristnost podpisa zagotavljala tudi dodatno dokazno moč v sodnem postopku (in obratno: njihove podpise bo težje poneveriti, v primeru sklicevanja na poneverbo pa bo nasprotna stranka le-to težko dokazala). Ob upoštevanju prostovoljne narave akreditacijske sheme (nikogar ne bo omejevala z obveznim vstopom) je volja države k njeni dejanski vzpostavitvi (pod pogojem, da se ta možnost izkaže za primernejšo od elektronske osebne izkaznice) dobrodošla.

V zvezi s podrobnejšim urejanjem akreditacijske sheme velja tudi poudariti, da pri tem zakonodajalec nima popolnoma prostih rok, saj to materijo delno ureja že Direktiva. Ob upoštevanju dejstva, da je akreditacijska shema le dodatek osnovni ureditvi, je treba obstoječe (oz. skladno s predlogom spremembe ZEPEP spremenjene) določbe, nanašajoče se na »osnovno« raven varnega elektronskega podpisovanja, ohraniti v veljavi. Ob uvajanju akreditacijske sheme pa je treba slediti vodilom Direktive, ki v 3. členu določa, da morajo biti vse zahteve v zvezi s temi shemami nepristranske, pregledne, sorazmerne in nediskriminacijske. Države članice tudi ne smejo omejiti števila akreditiranih overiteljev zaradi razlogov, ki spadajo v področje Direktive.

Uporaba HSM z vidika različnih zakonodajnih izvedb varnih e-identitet:

Omeniti velja tudi, da se zasebni ključ podpisnika pri vseh variantah lahko nahaja neposredno na napravi, ki jo podpisnik uporablja za tvorjenje podpisa ali pa na oddaljenem modulu HSM, podpisnikova naprava pa v primeru druge možnosti vsebuje le podatke za dostop do zasebnega ključa. Uporabo modula HSM omogoča vsaka izmed obravnavanih sprememb, pri tem pa je obseg uporabe prepuščen poslovni presoji overiteljev oz. ekonomskim dejavnikom. Če bi država želela v povezavi z varnimi e-identitetami zagotoviti vseobsežno uporabo modula HSM, pa bi za to morala uporabiti ustrezne, predvsem pravne mehanizme. Vseobsežno uporabo HSM bi bilo najenostavneje doseči v primeru uvedbe e-osebnih izkaznic (kjer država vzpostavi sistem in sama sebi postavi pogoje izvedbe), nekoliko težje izvedljiva bi bila njegova vseobsežna uporaba v primeru uvedbe sistema akreditacije (v tem primeru bi morala država pogojevati akreditacijo overitelja z integracijo njegovih naprav in storitev s HSM, kar bi lahko zmanjšalo zanimanje overiteljev oziroma jim dodatno priznanje delovanja po najboljših praksah ne bi odtehtalo težav integracije s HSM), še težje izvedljiva pa bi bila v primeru uveljavitve (le) predlaganih sprememb ZEPEP (overiteljem prilagoditve njihovih obstoječih sistemov za uporabo HSM predstavljajo strošek, zaradi česar se za investicijo ob odsotnosti večjih koristi ne bodo odločili; v tem primeru bi država lahko uvedla njegovo vseobsežno uporabo le z dodatnim predpisom oziroma nadaljnjimi spremembami ZEPEP).

3. Integracija varnih e-identitet z e-storitvami

Ob pregledu trenutnega stanja lahko ugotovimo, da uporaba e-identitet med drugim ni razširjena tudi zaradi pomanjkanja storitev, ki bi takšne identitete uporabljale (e-storitve). Uspešnost uvedbe e-identitet bo torej večja, če bo njihova uporaba presegala okvire storitev e-uprave in bo razširjena tudi na področje tržnih storitev. Pravni okvir e-identitet bi zato moral zagotoviti možnost integracije e-identitet z e-storitvami na enoten način, da je ponudnikom omogočena enostavnejša vzpostavitev e-storitev, brez potrebe po njihovem prilagajanju več različnim rešitvam certificiranja.

Enoten profil e-identitet, namenjen ponudnikom e-storitev trenutno ne obstaja, saj se identifikacijski podatki imetnika zasebnega ključa zapišejo neposredno v potrdilo, overitelji pa te podatke zapisujejo na različne načine. To predstavlja za ponudnike e-storitev nepotrebno oviro, saj morajo potrdila vsakega overitelja integrirati s svojo storitvijo po posebnem postopku. Trenutno predlagani rešitvi za odpravo te pomanjkljivosti sta (1) vpeljava enotnega profila kvalificiranega digitalnega potrdila, v katerem bo podatek o identiteti podpisnika zapisan na poenoten način in vsem aplikacijam dostopen neposredno s potrdila in (2) vpeljava centralnega avtentikacijskega sistema, ki bi ga uporabljale javne in zasebne e-storitve, pri čemer bi lahko bil podatek o imetnikovi identiteti zapisan na potrdilu vsakega overitelja

različno, za ponudnike e-storitev pa to ne bi predstavljalo težave, saj bi digitalna potrdila preverjal centralni sistem in ne njihove aplikacije same. S pravnega vidika sta sprejemljivi obe možnosti, ureditev ene tudi ne predstavlja prednosti pred ureditvijo druge, zato bo izbira odvisna predvsem od drugih dejavnikov. Za overitelje je primernejša rešitev centralni avtentikacijski sistem, saj pri tem niso omejeni z regulacijo vsebine digitalnega potrdila. V kolikor bi vzpostavitev takšnega centralnega sistema predstavljala prevelike stroške ali druge težave, pa bi bilo bolj priporočljivo predpisati overiteljem enoten zapis identifikatorjev imetnika digitalnega potrdila.

4. Regulacija overjanja elektronskih podpisov

Ne glede na izbrano rešitev bo potrebno zagotoviti, da pravna ureditev varnih e-identitet ne bo prekomerno omejevala overiteljev, da se zagotovi njihov interes za izdajo digitalnih potrdil, ki se bodo uporabljali pri e-identitetah. Za zahteve z izrazito omejujočim vplivom je zato priporočljivo presoditi, če predstavljajo najmilejši (z razumnimi sredstvi izvedljiv) način za dosego postavljenega cilja. Če se bodo zakonodajne zahteve pri urejanju e-identitet postavljale na takšen način, gre pričakovati, da nova ureditev ne bo odvrnila overiteljev od zagotavljanja storitev overjanja na tem področju.

Bistven vidik ne-omejevanja overiteljev je tudi zagotavljanje čim širših možnosti nastopanja na trgu izdajanja digitalnih potrdil, ki se bodo uporabljali za e-identitete. Z vidika zagotavljanja konkurence med ponudniki ni priporočljiva uporaba rešitev, ki bi že vnaprej onemogočale ali bistveno zmanjševale možnost sodelovanja večjega števila overiteljev. S tega vidika ni priporočljiva uporaba e-osebnih izkaznic, saj bi takšne izkaznice verjetno overjal le en overitelj, pri tem pa bi šlo za tako velik posel, da bi bila konkurenca na relevantnem trgu znatno omejena. Namesto tega je bolj priporočljiva katera izmed preostalih rešitev (akreditacija, kvalificirana potrdila na varnih medijih), saj ti rešitvi omogočata konkuriranje overiteljev ves čas izvajanja storitev, ne le v postopku izbora za dodelitev celotnega posla, hkrati pa ti rešitvi omogočata tudi vstop novih overiteljev na relevanten trg. S konkurenčno-pravnega vidika sta torej primernejši rešitvi akreditirane e-identitete in kvalificiranih digitalnih potrdil na varnih medijih.

5. Prijaznost do uporabnika

Na pravno ureditev e-identitet vplivajo tudi potrebe in preference uporabnikov, ki so pravzaprav razlog za uvajanje novega sistema. Z vidika vpliva novega sistema na uporabnika izpostavljamo predvsem vprašanji varnosti sistema in njegove cenovne ugodnosti.

Brez podrobnejšega obravnavanja tehnične in organizacijske varnostne izvedbe, je mogoče že na prvi pogled ugotoviti, da je varnejši sistem tisti, ki se uporablja samo v enem sektorju ali pa v primeru uporabe v več sektorjih omogoča uporabo različnih identifikatorjev za posamezne sektorje. Uporaba istega instrumenta v več sektorjih je sicer praktična, hkrati pa za uporabnike predstavlja dodatno tveganje, ki lahko pretehta praktičnost uporabe, ki jo prinese združitev identifikacijskih instrumentov. S tega vidika v primeru uvedbe e-osebne izkaznice le-te ni priporočljivo integrirati z identifikacijskimi instrumenti na nekaterih drugih področjih, kjer je zaupnost podatkov bistvenega pomena (na primer z zdravstveno izkaznico).

Cenovna ugodnost za uporabnike je odvisna od cene za uporabo naprav za zagotavljanje e-identitete in od obveznosti njihove uporabe. S tega vidika so ustreznejše rešitve, pri katerih se čim več infrastrukture zagotavlja centralno za vse uporabnike skupaj, saj takšne rešitve znižujejo stroške uporabnikov. Priporočljivejše pa so tudi rešitve, ki za uporabnike niso obvezne, saj obvezen nakup naprav za tvorjenje varnega elektronskega podpisa brez dejanske potrebe po njihovi uporabi za uporabnike ne pomeni optimalne rešitve. S tega vidika je ob uvedbi e-osebne izkaznice priporočljivo njeno uporabo določiti kot fakultativno, saj še tako nizke cene dokumenta, ki jih dosežemo zaradi velikega obsega proizvodnje, za uporabnika, ki dodatnih funkcij takšnega dokumenta ne bo uporabljal (z vidika uporabnika je dodana vrednost enaka nič), niso dovolj nizke.

6. Zaključek

Vprašanje, ali sistem e-identitet urediti v ZOIzk-1 ali v ZEPEP je odvisno predvsem od tega, kateri model varnih e-identitet se bo izkazal za najboljšega. Zakonodajna ureditev vsakega od modelov ne bi smela biti težavna, saj je ureditev kvalificiranih digitalnih potrdil na varnih medijih že vzpostavljena v predlagani spremembi ZEPEP, akreditacija overiteljev je v veliki meri urejena v že veljavnem zakonu (v primeru njene vzpostavitve se tudi priporoča navezava na že predlagane spremembe ZEPEP, v smislu nadgradnje), nekatere določbe o e-osebni izkaznici pa je vseboval že tudi ZOIzk pred sprejetjem novega zakona (ZOIzk-1), poleg tega bi urejanje v ZOIzk temeljilo na nekaterih institutih in rešitvah, predlaganih s spremembo ZEPEP. Pri zakonodajnem urejanju bo treba pozornost posvetiti tudi skladnosti z evropsko ureditvijo, predvsem ohranjanju obstoječe implementirane ureditve varnih elektronskih podpisov.

Ne glede na to, katera izmed obravnavanih rešitev bo izbrana za vzpostavitev varnih e-identitet, pa so spremembe ZEPEP za uveljavitev kvalificiranih elektronskih podpisov, oblikovanih z napravami za varno tvorjenje podpisa, poleg tega, da predstavljajo eno izmed možnih končnih rešitev, hkrati tudi osnova, na kateri je mogoče dograditi preostali rešitvi (elektronska osebna izkaznica, akreditirana e-identiteta), zaradi česar za spremembo ZEPEP ni ovir ne glede na dejstvo, da končna rešitev še ni izbrana. V kolikor se kasneje izkaže, da bi veljalo vzpostaviti eno od kompleksnejših možnosti, se poleg spremembe ZEPEP spremeni oz. sprejme še ustrezne druge akte (predvsem podzakonske akte ZEPEP za vzpostavitev akreditiranih e-identitet oz. ZOIzk za vzpostavitev elektronske osebne izkaznice).