REPUBLIKA SLOVENIJA
MINISTRSTVO ZA PRAVOSODJE IN JAVNO UPRAVO
DIREKTORAT ZA INFORMATIKO IN E-STORITVE

Tržaška cesta 21, 1000 Ljubljana

ANALIZA MOŽNOSTI ZA UVEDBO VARNEJŠIH IN UPORABNIKU PRIJAZNEJŠIH E-IDENTITET

POVZETEK

Upravljanje z elektronskimi identitetami postaja ključni element e-poslovanja, vendar pomanjkanje skupnih pristopov odpira mnogo vprašanj v zvezi z zasebnostjo in varnostjo. V Sloveniji se za potrebe avtentikacije uporabnika pri opravljanju elektronskih storitev in za elektronsko podpisovanje že od vzpostavitve zakonske podlage leta 2000 dalje uporabljajo kvalificirana digitalna potrdila. Kljub temu, da overitelji tovrstna potrdila izdajajo že več kot deset let, pa danes ugotavljamo, da je uporaba e-podpisa kot tudi samih kvalificiranih digitalnih potrdil relativno zahtevna in ne dovolj razširjena, da bi dejansko omogočala širšo uveljavitev e-poslovanja tako v poslovnem svetu kot tudi v javni upravi, uporaba naprav za varno tvorbo e-podpisa pa je še precej manj uveljavljena.

Zaradi zgoraj naštetih dejstev in tudi glede na trenutni trend v državah EU ter razvoj informacijskih tehnologij je potrebno državljanom in podjetjem omogočiti varne, enostavne in sodobne koncepte za elektronsko podpisovanje in izkazovanje identitete na elektronski način. Izvedena je bila podrobna analiza možnosti, ki so na voljo za dosego tega cilja, z namenom pripraviti pravna, organizacijska in tehnična izhodišča za vpeljavo e-identitet, ki bodo omogočale enolično identifikacijo imetnika pri uporabi e-storitev ter tvorjenje kvalificiranega elektronskega podpisa. Na osnovi analize zasledovanih ciljev so bili opredeljeni naslednji temeljni cilji za prenovo sistema e-identitet:

- enostavnost uporabe,
- široka uporabnost,
- zagotovljen visok nivo varnosti,
- zagotovljeno varstvo osebnih podatkov,
- enostavnost integracije,
- poenoteno upravljanje,
- sorazmerno hitra uvedba,
- sprejemljivi stroški.

Na podlagi teh osmih ciljev so bile možnosti razdeljene v tri različne sklope, ki so bili analizirani in ovrednoteni neodvisno drug od drugega:

- Sklop 1: pravne možnosti e-identitet,
- Sklop 2: modeli identifikatorjev,
- Sklop 3: različne tehnične izvedbe e-identitet.

Končni rezultati analize temeljijo na več podlagah, in sicer smo upoštevali:

- rezultate vrednotenja posameznih variant odločitvenega modela, ki so jih ocenjevali različni deležniki v obliki fokusnih skupin (ponudniki e-storitev v javni upravi in zasebnem sektorju, predstavniki končnih uporabnikov iz javne uprave in državljani ter strokovnjaki medresorske delovne skupine),
- mnenje predstavnikov potrošnikov,
- mnenje predstavnikov ponudnikov e-storitev iz zasebnega sektorja,
- zunanje pravno mnenje,
- mnenje medresorske delovne skupine,
- predlog nove uredbe v zvezi z e-podpisom, e-identifikacijo, e-avtentikacijo in drugih tovrstnih storitev na ravni EU,
- najnovejše usmeritve v drugih državah in
- izsledke izvajanja EU projekta STORK.

V sklopu pravnih možnosti e-identitet smo primerjali tri rešitve: e-osebno izkaznico, akreditirano e-identiteto in kvalificirano digitalno potrdilo na pametnem mediju. V odločitvenem modelu se je kot najprimernejša izbira izkazala e-osebna izkaznica, vendar so razlike med vsemi tremi možnostmi zelo majhne. E-osebna izkaznica je dosegla najboljše rezultate pri fokusnih skupinah iz javnega sektorja, medtem ko so bili predstavniki zasebnega sektorja bolj naklonjeni trenutni situaciji, kjer imamo na voljo različne ponudnike kvalificiranih digitalnih potrdil. Ker slednja ne prinaša nobenih novosti glede prenove e-identitet v smislu večje pravne urejenosti, odločitev zanjo ni smotrna. Če primerjamo preostali dve možnosti, t.j. e-osebno izkaznico in akreditirano e-identiteto, bi uvedba druge poenostavila vzpostavitev višjega nivoja urejanja e-identitet in omogočila akreditacijo tudi drugih, z e-identitetami povezanih storitev, npr. e-žigi, časovni žigi, ipd. V odločitvenem modelu je ta možnost sicer ocenjena nekoliko slabše kot e-osebna izkaznica, vendar po mnenju medresorske delovne skupine akreditirana e-identiteta predstavlja boljšo rešitev, saj omogoča ustrezno pravno urejenost področja e-identitet in bolje sledi trendom in nenazadnje pravnim zahtevam, ki se nam obetajo na ravni EU. Če torej primerjamo e-osebno izkaznico in akreditirano e-identiteto, lahko zaključimo, da je slednja primernejša oblika prenove tega področja v slovenskem prostoru.

Za drugi sklop je bilo identificiranih pet različnih možnosti: obstoječi identifikator v digitalnem potrdilu oziroma zalednem sistemu, e-identifikator osebe v digitalnem potrdilu oziroma zalednem sistemu in sektorski e-identifikator. Prva dva modela temeljita na uporabi obstoječih identifikatorjev in odražata trenutno stanje v Sloveniji. Nekateri overitelji v skladu s prvim modelom namreč v digitalno potrdilo vključijo davčno številko imetnika, kar predstavlja veliko izpostavljenost osebnega identifikatorja. Te možnosti zato ni mogoče predlagati kot priporočljive rešitve za potrebe identifikacije imetnika digitalnega potrdila oz. e-identitete. Tretji in četrti model predvidevata uvedbo novega identifikatorja, t.i. e-identifikatorja, namenjenega izključno e-poslovanju. Taka uvedba bi zahtevala ustrezno pravno podlago novega identifikatorja in njegovo umestitev v primeren obstoječ register, obenem pa bi močno vplivala na ponudnike obstoječih e-storitev, saj bi zahtevala prilagoditev le-teh na nov način avtentikacije. Največ sprememb bi vnesla odločitev za sektorske e-identifikatorje. Ta model je

zgleden z vidika varstva osebnih podatkov, vendar je primeren predvsem za države, ki še nimajo tako razširjenih e-storitev, kot so npr. v Sloveniji, zato izbira te možnosti ni smotrna. Uvedba bi namreč povzročila precejšnje spremembe v načinu avtentikacije in zahtevala obsežne organizacijske, pravne in tehnične spremembe. Zaradi vsega navedenega in glede na razširjenost e-storitev v Sloveniji ter upoštevajoč obstoječe rešitve za avtentikacijo je za potrebe identifikacije uporabnika najbolj smotrna odločitev za rešitve, ki predvidevajo uporabo obstoječega osebnega identifikatorja v zalednem sistemu.

V okviru tretjega sklopa smo analizirali in ocenjevali naslednje možnosti: pametna kartica s kontaktnim in/ali brez-kontaktnim čipom, pametni ključek, mobilni telefon z digitalnim potrdilom ter dve različici rešitev z digitalnim potrdilom na varnostnem modulu. Izvedba s pametnimi karticami je edina možna v primeru odločitve za uvedbo e-osebnih izkaznic, dopuščata pa jo tudi obe drugi možnosti v sklopu pravnih možnosti, t.j. akreditirana e-identiteta in kvalificirano digitalno potrdilo na pametnem mediju. Po drugi strani bi mobilne naprave lahko uporabili kot nosilce e-identifikatorjev v primeru odločitve za akreditirano e-identiteto ali v primeru ohranitve obstoječega modela overiteljev kvalificiranih potrdil, niso pa primerne za uporabo v modelu e-osebne izkaznice. Pri analizi možnosti smo ugotovili, da lahko z vidika osmih ciljev različne rešitve v grobem združimo v dve skupini in sicer na rešitve z digitalnim potrdilom na pametnem mediju ter na rešitvi z digitalnim potrdilom na varnostnem modulu. Če upoštevamo predstavljene prednosti in slabosti posameznih izvedb, se izmed rešitev z digitalnim potrdilom na pametnem mediju kot najbolj primerna izbira izkaže pametna kartica s kontaktnim čipom. Sicer po rezultatih vrednotenja na podlagi odločitvenega modela rešitev, ki predvideva uporabo mobilnega telefona v povezavi z varnostnim modulom, ni najbolje ocenjena, vendar ima določene prednosti (npr. široka uporabnost, neodvisnost od operaterjev in tehnologije kartic SIM), zato po mnenju medresorske delovne skupine predstavlja resno alternativo rešitvam z digitalnim potrdilom na pametnem mediju, zahteva pa podrobnejšo analizo potrebnih ukrepov za njeno morebitno vzpostavitev. Uporaba mobilnega telefona z varnostnim modulom omogoča tudi nadgradnjo rešitve v povezavi z vzpostavitvijo centralne storitve avtentikacije, na nivoju katere bo možno dokaj enostavno vključevati dodatne rešitve za avtentikacijo (npr. pametne kartice), ki bi služile kot sredstvo za prijavo, medtem ko bi se dejansko podpisovanje izvajalo na varnostnem modulu.