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

Končna verzija

Sektor za komunikacijsko infrastrukturo
Sektor za projektno upravljanje
V 1.0-končna verzija, 14. avgust 2012

Stanje dokumenta

Namen dokumenta:	Analiza možnosti za uvedbo varnejših in uporabniku prijaznejših e-identitet na podlagi sklepa o imenovanju medresorskega delovnega telesa za pripravo dokončne usmeritve za uvedbo varnejših in uporabniku prijaznejših e-identitet št. 024 – 18/2011/4 z dne 19.4.2011
Status:	Končni izdelek
Verzija:	1.0, glej »Zgodovina sprememb«
Datum verzije:	31. julij 2012
Avtorji:	Člani medresorske delovne skupine za pripravo dokončne usmeritve za uvedbo varnejših in uporabniku prijaznejših e-identitet (v nadaljevanju *medresorska delovna skupina*)
Člani skupine:	dr. Alenka Žužek Nemec, MPJU, vodja mag. Aleš Pelan, MPJU mag. Katarina Čepon, MPJU Tamara Gliha, MPJU mag. Brane Kren, MPJU Marko Ambrož, MPJU dr. Simona Kralj-Zatler, MIZKŠ Peter Strle, MIZKŠ mag. Andrej Tomšič, IP Vladimir Logofetov, MNZ dr. Mišo Vukadinović, MNZ mag. Andrej Lesjak, MNZ – Policija Jure Logar, IP Maruška Damjan, MIZKŠ

Zgodovina sprememb

Verzija	Datum	Razlog za spremembe	Spremenil
0.1	4.5.2011	Prvi osnutek.	MPJU
0.2	13.5.2011	Drugi osnutek, dopolnitve na podlagi 1. sestanka skupine z dne 5.5.2011.	MPJU, IP, MNZ
0.3	26.5.2011	Tretji osnutek, dopolnitve na podlagi 2. sestanka skupin z dne 17.5.2011 in spremembe kazala, dogovorjenega na sestanku ožje skupine (MIZKŠ, IP, MPJU) z dne 26.5.2011.	MPJU
0.4	31.5.2011	Četrti osnutek, dopolnitve na podlagi 3. sestanka skupine z dne 31.5.2011 in popravkov ciljev, ki jih je pripravil IP. Dokument tudi usklajen s skupino.	MPJU, IP
0.5	2.6.2011	Peti osnutek, dopolnitve na podlagi 4. sestanka skupine z dne 2.6.2011.	MPJU
0.6	4.7.2011	Šesti osnutek, dopolnitev na podlagi sestanka MPJU dela skupine z dne 17.6.2011.	MPJU
0.7	6.6.2012	Sedmi osnutek z vključenim odločitvenim	MPJU, Fakulteta za

		modelom, rezultati vrednotenja in občutljivostno analizo. Spremenjena struktura dokumenta. Dodana zunanja mnenja, vključene organizacijske spremembe ter posodobljena vsebina glede EU projektov, ZEPEP in uredbe EK. Dodan povzetek stanja v Avstriji in na Švedskem ter sklepne ugotovitve.	upravo, IPRI, ZPS, ZBS
0.8	29.6.2012	Osmi osnutek, dopolnitve in spremembe na osnovi pripomb skupine.	MPJU, IP, MNZ
0.9	5.7.2012	Končni osnutek – nelektorirana verzija.	MPJU
1.0	14.8.2012	Končna verzija.	MPJU

VSEBINA

SEZNAM UPORABLJENIH KRATIC IN IZRAZOV

BPL	Biometrični potni list
CEN	Evropski odbor za standardizacijo, angl. *European Committee for Standardisation*
CIP	Okvirni program za konkurenčnost in inovacije, angl. *Competitiveness and Innovation Framework Programme*
eOI	Elektronska osebna izkaznica
EK	Evropska komisija
EU	Evropska unija
HSM	Strojni varnostni modul, angl. *High Security Module*
ISA	Komitološki program za interoperabilnost javnih uprav držav EU, angl. *Interoperability Solutions for European Public Administrations*
KZZ	Kartica zdravstvenega zavarovanja
MPJU	Ministrstvo za pravosodje in javno upravo
OECD	Organizacija za gospodarsko sodelovanje in razvoj, angl. *Organisation for Economic Co-operation and Development*
OI	Osebna izkaznica
RFID	angl. *Radio Frequency IDentification*
QAA	Nivoji zaupanja e-identitet, določeni za potrebe projekta STORK, angl. *Quality Assurance Authentication Assurance*
SIGEN-CA	Izdajatelj digitalnih potrdil SIGEN-CA v okviru Overitelja na Ministrstvu za pravosodje in javno upravo
SIGOV-CA	Izdajatelj digitalnih potrdil SIGOV-CA v okviru Overitelja na Ministrstvu za pravosodje in javno upravo
SSCD	Naprava za varno tvorjenje podpisa, angl. *Secure Signature-Creation Device*
STORK	Projekt velikih razsežnosti za čezmejno priznavanje e-idenitet iz programa CIP, angl. *Secure Identity Across Borders Linked*
WPKI	Brezžična infrastruktura javnih ključev, angl. *Wireless Public Key Infrastructure*
ZEPEP	Zakon o elektronskem poslovanju in elektronskem podpisu
ZOIzk	Zakon o osebni izkaznici
ZPP	Zakon o pravdnem postopku
ZPPDFT	Zakon o preprečevanju pranja denarja in financiranju terorizma
ZVOP-1	Zakon o varstvu osebnih podatkov
ZUP	Zakon o splošnem upravnem postopku

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. Pričujoči dokument predstavlja podrobno analizo možnosti, ki so na voljo za dosego tega cilja, njegov namen pa je 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.

1. UVOD

Upravljanje z elektronskimi identitetami postaja ključni element e-poslovanja. Dandanes se tako v javnih upravah in podjetjih v državah Evropske unije (v nadaljevanju *EU*) uporabljajo različne rešitve za upravljanje z elektronskimi identitetami. Rešitve se osredotočajo predvsem na nacionalne potrebe in sredstva, kar je pripeljalo do zapletenega sistema z različnimi rešitvami. Pomanjkanje skupnih pristopov odpira mnogo vprašanj v zvezi z zasebnostjo in varnostjo. V vedno večji ekonomski povezljivosti pomenijo te različnosti rešitev za elektronske identitete prepreko za zagotavljanje ustreznih rešitev in nove ovire za čezmejne trge in delovanje enotnega trga znotraj EU. K odpravljanju teh ovir so se zavezali tudi ministri, pristojni za razvoj e-uprave, v Ministrski deklaraciji za razvoj e-uprave na ravni EU do l. 2015.

V Sloveniji že od leta 2000 velja Zakon o elektronskem poslovanju in elektronskem podpisu (v nadaljevanju *ZEPEP*), ki ureja e-poslovanje z uporabo informacijske in komunikacijske tehnologije in uporabo e-podpisa. V letu 2011 je bil pripravljen predlog za spremembo ZEPEP[1] za boljšo uskladitev z Direktivo o 1999/93 ES o e-podpisu (v nadaljevanju *Direktiva o e-podpisu*). Uskladitev se je nanašala predvsem na zahteve v zvezi z obvezno uporabo naprav za varno tvorbo e-podpisa za t.i. kvalificirani e-podpis, ki je skladno s slovensko in evropsko zakonodajo ter uveljavljenimi tehnologijami enakovreden lastnoročnemu podpisu. E-podpis namreč omogoča enakovrednost z lastnoročnim podpisom, če se tvori s t.i. kvalificiranim digitalnim potrdilom in napravo za varno tvorbo e-podpisa (s tem so mišljene na primer pametne kartice, varnostni strojni moduli, za uporabo digitalnih potrdil podprte kartice SIM pri mobilnih telefonih ipd.).

V Sloveniji imamo različne izdajatelje kvalificiranih digitalnih potrdil, uporaba naprav za varno tvorbo e-podpisa pa je manj uveljavljena. Poleg novih pravnih okvirjev prevladuje tudi dejstvo, da je uporaba e-podpisa kot tudi samih kvalificiranih digitalnih potrdil relativno zahtevna in ne zadovoljivo razširjena, da bi dejansko omogočala širšo uveljavitev e-poslovanja tako v poslovnem svetu kot tudi v javni upravi.

Ministrstvo za pravosodje in javno upravo (v nadaljevanju MPJU) izdaja kvalificirana digitalna potrdila tako za javne uslužbence za e-poslovanje znotraj državnih organov (izdajatelj SIGOV-CA) kot tudi za državljane in poslovne subjekte kot uporabnike storitev javne uprave oz. e-uprave (izdajatelj SIGEN-CA). Javni uslužbenci imajo s strani MPJU že zagotovljene naprave za varno tvorbo e-podpisa, državljani in poslovni subjekti pa trenutno lahko pridobijo zgolj kvalificirano digitalno potrdilo brez naprave za varno tvorbo e-podpisa, zato je to potrdilo večinoma shranjeno kar v shrambi digitalnih potrdil uporabnikovega brskalnika.

Uporaba kvalificiranih digitalnih potrdil, shranjenih v shrambi brskalnika[2], tudi z vidika varnosti ni najbolj primerna, saj uporabniki prepogosto shrambe potrdil navkljub drugačnim priporočilom nimajo zaščitene z osebnim geslom. Obenem je v primeru digitalnih potrdil, ki niso shranjena v napravi za varno tvorbo e-podpisa, nemogoče preprečiti oz. celo zaznati podvajanje potrdil, zato pogosto uporabniki niti sami ne vedo, koliko različic potrdila imajo in kje jih hranijo. Nenazadnje je

[1] Postopek spremembe ZEPEP je bil zaradi političnih sprememb v letu 2011 prekinjen.

[2] To pomeni, da se v shrambi brskalnika shrani tudi zasebni ključ uporabnika.

potrebno omeniti tudi različne zlonamerne programe, ki lahko neprevidnemu uporabniku prevzamejo nadzor nad njegovim potrdilom v spletnem brskalniku. Večini teh groženj oz. pomanjkljivosti se uporabnik izogne, če ima svoje potrdilo shranjeno v napravi za varno tvorbo e-podpisa, saj ima tako bistveno večji nadzor nad njim, ga uporablja z večjo pozornostjo in pazljivostjo, obenem pa so tudi možnosti njegove zlorabe bistveno manjše.

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. Možnosti so različne:

- Že nekajkrat je bil v Sloveniji pričet projekt elektronske osebne izkaznice, ki bi združil klasično osebno izkaznico z elektronsko identiteto ali pa celo uvedel multifunkcijsko kartico, ki bi združila še druge identifikatorje. Projekt do sedaj zaradi različnih razlogov še ni zaživel.
- Za kvalificirana digitalna potrdila SIGEN-CA za državljane in poslovne subjekte bi lahko kot napravo za varno tvorbo e-podpisa izkoristili kartice zdravstvenega zavarovanja ali pa izdali svoje v obliki pametnih USB ključkov ali pametnih kartic.
- Glede na razširjenost uporabe mobilnih telefonov in tehnološke možnosti se vse bolj širi tudi njihova uporaba kot naprav za varno tvorbo e-podpisa.

Ta dokument predstavlja podrobno analizo vseh navedenih možnosti. Sama izhodišča te analize so bila predstavljena na seji projektne koordinacije dne 22. decembra 2010, z njimi so bili seznanjeni tudi člani Sveta za informatiko na svoji seji, dne 23. marca 2011. Na tej seji so sprejeli sklep št. 11, s katerim je Svet predlagal ministru, pristojnemu za javno upravo, da čim prej imenuje medresorsko skupino, v katero bodo vključeni predstavniki Ministrstva za notranje zadeve (MNZ), Ministrstva za visoko šolstvo, znanost in tehnologijo (sedaj Ministrstvo za izobraževanje, znanost, kulturo in šport oz. MIZKŠ), Informacijskega pooblaščenca (IP) in ministrstva, pristojnega za e-upravo, ki naj pripravi dokončne usmeritve za uvedbo varnih in uporabniku prijaznih elektronskih identitet3. Naloge te skupine so naslednje:

- pripraviti natančno analizo možnosti uvedbe e-identifikatorjev s pravnega, organizacijskega in tehničnega vidika,
- na podlagi analize predlagati najustreznejšo rešitev za izkazovanje identitete na elektronski način in
- identificirati ustrezne potrebne pravne, organizacijske in tehnične ukrepe.

Delo medresorske skupine je bilo od jeseni 2011 do pomladi 2012 začasno prekinjeno zaradi organizacijskih in varčevalnih ukrepov.

1.1. Namen in cilji projekta

Namen analize je 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. Pri vpeljavi je potrebno upoštevati izhodišča, dognanja in koncepte rešitev, ki

[3] Medresorska skupina je bila imenovana s sklepom ministra, pristojnega za javno upravo, z dne 19.4.2011, št. 024 – 18/2011/4.

so bili razviti v pilotnem projektu velikih razsežnosti, t.i. STORK. Medresorska delovna skupina je z analizo zasledovanih ciljev opredelila naslednje temeljne cilje za prenovo sistema e-identitet:

1. **Enostavnost uporabe:** e-identiteta bo prijazna do uporabnikov in enostavna za uporabo.
2. **Široka uporabnost:** e-identitete bodo namenjene posameznikom oz. fizičnim osebam, uporaba pa bo ob vzpostavitvi ustreznega sistema pooblaščanja mogoča tudi za organizacije oz. pravne osebe.
3. **Zagotovljen visok nivo varnosti:** e-identitete bodo varne in zaupanja vredne.
4. **Zagotovljeno varstvo osebnih podatkov:** izbrana rešitev bo upoštevala temeljna načela varstva osebnih podatkov.
5. **Enostavnost integracije**: v aplikacije ponudnikov storitev bo e-identitete enostavno integrirati.
6. **Poenoteno upravljanje:** predlagana rešitev bo v največji možni meri poenotila upravljanje in uporabo e-identitet v Sloveniji.
7. **Sorazmerno hitra uvedba**: predlagani model e-identitete bo mogoče vpeljati v sorazmerno kratkem času, tako z vidika njihovih izdajateljev kot z vidika ponudnikov e-storitev, ki bodo v svojih sistemih podpirali varnostne rešitve z uporabo e-identitet.
8. **Sprejemljivi stroški:** izbrana rešitev bo z vidika stroškov uvedbe in uporabe e-identitet sprejemljiva za uporabnike, izdajatelje in ponudnike e-storitev.

2. STANJE V SLOVENIJI IN V EU

2.1. Strateški dokumenti v Sloveniji

Slovenija razvoj e-uprave in tudi razvoj na področju e-podpisa in e-identitet za uporabo storitev e-uprave usmerja skozi strateške dokumente in akcijske načrte. Aktualna dokumenta sta sledeča:

- Strategija razvoja elektronskega poslovanja ter izmenjave podatkov iz uradnih evidenc (sprejeta 2009)
- Akcijski načrt e-poslovanja v javni upravi do 2015 (sprejet 2010).

Bistvena novost je v razvoju e-uprave skozi centralne horizontalne podporne funkcije in storitve, kar naj bi omogočilo lažji razvoj novih elektronskih storitev, čas za njihovo implementacijo bi se krajšal, stroški pa bi bili nižji, obenem pa zagotovljena interoperabilnost med institucijami in med rešitvami.

V povezavi z e-identitetami so v akcijski načrt vključeni kot skupni oz. ponovno uporabljivi naslednji gradniki[4]:

- Delovanje Overitelja na Ministrstvu za pravosodje in javno upravo (v nadaljevanju *MPJU*)
- Centralna storitev digitalnega podpisa
- Centralna storitev avtentikacije
- Varnostna shema

2.2. Stanje na področju e-identitet v Sloveniji

2.2.1. Overitelji kvalificiranih potrdil

V Sloveniji večina e-storitev temelji na uporabi kvalificiranih digitalnih potrdil kot sredstev za elektronsko identifikacijo uporabnikov storitve. V skladu z veljavno zakonodajo mora overitelj pred pričetkom opravljanja storitve overjanja opraviti prijavo v registru overiteljev, ki ga vodi MIZKŠ. Postopek registracije overiteljev je enostaven in se izvaja vse od sprejetja ZEPEP, vse spremembe podatkov o overiteljih in njihovih storitvah so redno objavljene v registru. V registru je trenutno prijavljenih pet overiteljev, ki izdajajo digitalna potrdila namenjena širši javnosti. Vseh pet overiteljev izdaja kvalificirana digitalna potrdila.

Registrirani overitelji digitalnih potrdil so:

1. Overitelj na Ministrstvu za pravosodje in javno upravo, http://www.ca.gov.si
2. HALCOM informatika d.o.o., Služba HALCOM-CA, http://www.halcom.si
3. AC NLB (overitelj na Novi ljubljanski banki), http://www.nlb.si/acnlb
4. POŠTA®CA (Pošta Slovenije), http://postarca.posta.si
5. Ministrstvo za obrambo, SIMoD-CA, http://www.simod-pki.mors.si

Skladno z Odločbo Evropske komisije 2009/767/ES je Register overiteljev pripravljen in dostopen tudi v obliki predpisanega zanesljivega seznama (TSL, angl. Trust-service Status List) nadzorovanih oz. akreditiranih overiteljev.

[4] Razen centralne storitve avtentikacije se vse ostale storitve že izvajajo, prva že več kot desetletje.

Vsi navedeni izdajatelji so digitalna potrdila pričeli izdajati z jasnim namenom glede ciljnih uporabnikov. Overitelj na MPJU izdaja digitalna potrdila, da bi spodbujal uporabo elektronskih storitev javne uprave, overitelja HALCOM-CA in AC NLB sta osredotočena predvsem na izdajanje potrdil za elektronsko bančništvo, POŠTA®CA pa je pričela z izdajanjem digitalnih potrdil v sklopu storitve "varni elektronski predali", ki deluje pod okriljem Pošte Slovenije. Zadnji navedeni v registru overiteljev SIMoD-CA je overitelj, ki izdaja digitalna potrdila izključno za notranje postopke Ministrstva za obrambo, zato digitalna potrdila tega overitelja niso vključena v aplikacije javne uprave.

Kljub zgoraj navedenim namenom izdajanja digitalnih potrdil vedno več neodvisnih ponudnikov storitev ponuja aplikacije in storitve, ki temeljijo na uporabi digitalnih potrdil vseh overiteljev, ki izdajajo kvalificirana digitalna potrdila. Ponudniki elektronskih storitev uporabljajo različne pristope pri izbiri digitalnih potrdil overiteljev, ki jih lahko uporabniki storitev uporabljajo. Nekateri se zanašajo na potrdila točno določenega overitelja, drugi določijo skupino overiteljev, najpogosteje pa podpirajo digitalna potrdila vseh štirih zgoraj omenjenih overiteljev. Ugotovimo lahko, da to vse bolj postaja standard za e-storitve v Sloveniji. Pri e-storitvah javne uprave je zahteva po enakovredni uporabi kvalificiranih potrdil vseh overiteljev določena v uredbi o upravnem poslovanju. Uporaba aplikacij javne uprave za državljane in poslovne subjekte je torej mogoča s katerimkoli kvalificiranim digitalnim potrdilom overitelja, navedenega v registru overiteljev (z izjemo SIMoD-CA, ki je namenjen interni uporabi). Za pridobitev kateregakoli kvalificiranega potrdila je potrebna zanesljiva identifikacija bodočega imetnika, kar pomeni, da se mora le-ta pred izdajo potrdila na predpisan način, t.j. z uradnim osebnim dokumentom s fotografijo, identificirati pri prijavni službi overitelja.

2.2.2. Identifikacija imetnikov potrdil

V Sloveniji registrirani overitelji uporabljajo različne pristope pri povezovanju posameznega digitalnega potrdila in identifikacijskih podatkov njegovega imetnika (npr. davčna številka, EMŠO), z izjemo overitelja SIMoD-CA pa vsi to povezavo vzdržujejo, saj je nujna, če želimo digitalna potrdila uporabljati tudi za avtentikacijo uporabnikov in ne zgolj za digitalno podpisovanje dokumentov. Večina overiteljev v digitalno potrdilo tako enostavno zapiše podatek o davčni številki imetnika potrdila, medtem ko Overitelj na MPJU v potrdilo zapiše enolično oznako potrdila, v posebni prevajalni tabeli pa hrani preslikavo med to oznako in identifikacijskimi podatki imetnika (davčna številka, EMŠO, davčna in matična številka organizacije). Osebni podatki v tej tabeli so dostopni samo v skladu s področno zakonodajo, dostop pa se izvaja na dva načina:

- pridobivanje podatkov (za potrebe e-storitev javne uprave),
- preverjanje podatkov (za potrebe drugih e-storitev in posameznikov).

Omenjena razlika v uporabljenih pristopih pa tudi dejstvo, da overitelji, ki identifikacijske podatke imetnika zapišejo neposredno v potrdilo, to izvajajo na različne načine, predstavlja oviro za ponudnike storitev, ki želijo v svojih sistemih podpreti vse overitelje kvalificiranih potrdil, saj integracija vsakega izmed njih pomeni izvajanje posebnega postopka. Položaj na tem področju bi se lahko izboljšal na dva načina:

- z vpeljavo enotnega profila kvalificiranega digitalnega potrdila, tako da bi bil podatek o identiteti imetnika zapisan na predpisan način in vsem aplikacijam dostopen neposredno iz potrdila,

- z vpeljavo centralnega avtentikacijskega sistema, ki bi ga uporabljale tako e-storitve javne uprave kot e-storitve ostalih ponudnikov; v tem primeru bi bil podatek o imetnikovi identiteti lahko zapisan na različne načine, ki bi jih podpiral centralni sistem. Ta izvedba je tudi skladna z rešitvijo, kot je bila za potrebe čezmejnega priznavanja in uporabe elektronskih identitet razvita v okviru projekta STORK (več o tem v razd. 2.4.1).

2.2.3. Uporaba naprav za varno tvorjenje podpisa

V Sloveniji se načeloma uporabljajo tako kvalificirana digitalna potrdila na napravah za varno tvorjenje podpisa kot kvalificirana potrdila, shranjena v shrambi brskalnika. Kljub temu pa je potrebno poudariti, **da trenutno veliko večino izdanih kvalificiranih potrdil predstavljajo slednja, torej potrdila, ki so shranjena v shrambi brskalnika**. Kvalificirana potrdila na napravah za varno tvorjenje podpisa sicer ponujajo domala vsi overitelji, vendar se uporabniki zanje iz različnih razlogov ne odločajo pogosto (predvsem višja cena potrdila in nepoznavanje prednosti). Kot naprave za varno tvorjenje podpisa se v večini primerov uporabljajo pametne kartice s kontaktnim čipom oz. pametni ključki USB, izjema so le t.i. digitalna potrdila WPKI, ki pomenijo brezžično infrastrukturo javnih ključev (angl. *Wireless Public Key Infrastructure*), kjer so zasebni ključi shranjeni na kartici SIM mobilnega aparata. Tovrstna potrdila zaenkrat ponuja le overitelj HALCOM-CA, težava pri njihovi širši uporabi je namreč ta, da zahtevajo nadgradnjo aplikacij zaradi spremenjenega načina prijave uporabnikov.

Razen dokaj splošnih določil v uredbi k ZEPEP trenutno tudi ni nikjer določenih zahtev glede ustreznosti naprav za varno tvorjenje podpisa, zato overitelji te naprave ponujajo predvsem po lastni presoji in se pri tem lahko sklicujejo le na zahteve oz. naprave, določene kot ustrezne v drugih državah članicah EU. Položaj naj bi se spremenil s sprejetjem spremembe uredbe k ZEPEP, ki bo natančneje določala pogoje za ustreznost naprav za varno tvorjenje podpisa.

2.2.4. Kartica zdravstvenega zavarovanja

Kljub temu, da se kartica zdravstvenega zavarovanja (KZZ) ne uporablja izven sistema obveznega in prostovoljnega zdravstvenega zavarovanja, jo je na tem mestu potrebno omeniti, saj predstavlja napravo za varno tvorjenje podpisa, v prenovljeni obliki pa omogoča tudi shranjevanje dodatnih imetnikovih digitalnih potrdil in se torej lahko uporablja tudi pri dostopu do drugih e-storitev.

KZZ je dokument, ki se uporablja pri uveljavljanju pravic iz obveznega in prostovoljnega zdravstvenega zavarovanja za identifikacijo in preverjanje istovetnosti zavarovane osebe. Izdaja se brezplačno vsaki osebi ob prvi vzpostavitvi obveznega zdravstvenega zavarovanja v Sloveniji.

Prva generacija kartic, ki je bila uvedena leta 1998, je vsebovala pomnilniški čip. Leta 2007 se je začel projekt nadgradnje sistema, ki je predvideval nadomestitev obstoječih kartic s pametnimi karticami, kjer kartica ne predstavlja več nosilca podatkov o zavarovani osebi temveč le še ključ, ki omogoča dostop do teh podatkov. Ob izdaji KZZ sta na njej dve potrdili. Prvo potrdilo zavarovane osebe, ki ni zaščiteno z geslom, omogoča dostop zdravstvenih delavcev do zavarovalniških podatkov, drugo potrdilo, zaščiteno z geslom, pa je namenjeno bodoči uporabi e-storitev zdravstvenega zavarovanja. Obe potrdili sta nekvalificirani in tako dokaj neprimerni za uporabo v drugih sistemih in e-storitvah, kjer se zahteva višji nivo zaupanja. Imetnikom kartice pa je omogočeno shranjevanje njihovih drugih, tudi kvalificiranih digitalnih potrdil, ki jih lahko uporabljajo za druge namene.

2.3. Zakonodajni in strateški dokumenti EU

Strateški dokumenti na ravni EU pomembno vplivajo na razvoj e-uprave na nacionalnem nivoju. Po eni strani moramo izvajati ukrepe za izpolnjevanje dolžnosti, ki smo jih obvezani kot država EU, po drugi strani pa nas usmerjajo pri razvoju e-uprave v nacionalnem okvirju.

Ministri držav članic v EU, pristojni za e-upravo, se vsaki dve leti zberejo na ministrski konferenci, ki jo gosti predsedujoča država Svetu EU. Področje zagotavljanja e-identitet je vedno pomenilo pomembno prioriteto in ključni dejavnik in osnovni pogoj za realizacijo drugih ciljev e-uprave. Enako je v zadnji, t.i. Malmö deklaraciji, http://www.egov2009.se/. To področje je eno izmed štirih poglavitnih političnih ciljev, predvsem s stališča čezmejnega priznavanja e-identitet.

Akcijski načrt za razvoj e-uprave do l. 2015 na EU nivoju politične cilje iz deklaracije razdela v konkretne ukrepe. V zvezi z e-identifikacijo, e-avtentikacijo in e-podpisi določa sledeče naloge:

- revizija Direktive o e-podpisu,
- zagotavljanje medsebojnega (čezmejnega priznavanja) e-identitet,
- vzpodbujanje rešitev za e-identitete.

Direktiva o storitvah na notranjem trgu[5] predstavlja pomembno prelomnico pri razvoju čezmejnih storitev e-uprave, ki določa pravno zahtevo za zagotavljanje tovrstnih rešitev. Ena izmed ključnih zahtev je upravljanje in čezmejno priznavanje elektronske identifikacije. Problemi so tehnične, organizacijske in tudi pravne narave (eno izmed aktualnih rešitev prinaša projekt STORK, podrobnosti v nadaljevanju).

Evropska komisija je sprejela tudi nekatere druge dokumente, povezane z avtentikacijo in identifikacijo:

- Akcijski načrt o e-podpisih in e-identifikaciji za lažje opravljanje čezmejnih javnih storitev na enotnem trgu (2008)[6],
- Sklep Evropske komisije 2011/130/EU o določitvi minimalnih zahtev glede čezmejne obdelave dokumentov z elektronskim podpisom pristojnih organov v skladu s storitveno direktivo (Ur. l. Evropske unije, L 2011/53/66[7]),
- Odločba Evropske komisije 2009/767/EC in Sklep Evropske komisije 2010/425/EU v zvezi z vzpostavitvijo, vzdrževanjem in objavo zanesljivih seznamov overiteljev, ki jih nadzorujejo/akreditirajo države članice (Ur. l. Evropske unije, L 2009/274/36[8] in L 2010/199/30[9]).

[5] Direktiva 2006/123/ES o storitvah na notranjem trgu, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0123:EN:NOT

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0798:FIN:SL:HTML

[7] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:053:0066:01:SL:HTML

[8] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:274:0036:01:SL:HTML

[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:199:0030:01:SL:HTML

2.3.1. Predlog nove Uredbe na ravni EU v zvezi z e-podpisi in sorodnimi storitvami

Na ravni EU se pripravlja nova uredba, ki bo Direktivo o e-podpisu nadgradila z novimi določbami za povečanje zaupanja in varnosti pri opravljanju e-storitev na notranjem trgu EU. Predvidena so nova določila, ki jih obstoječi pravni okvirji niso obravnavali ali pa zelo pomanjkljivo, in sicer glede:

- e-avtentikacije, ki v sedanjih pravnih okvirjih ni bila obravnavana,
- čezmejnega priznavanja e-podpisa in e-avtentikacije,
- nabora identifikacijskih podatkov,
- e-žigov,
- časovnih žigov,
- e-dokumentov,
- e-vročanja,
- avtentikacije spletnih strani ter
- sistemov nadzora in akreditacijskih shem, ki po trenutni zakonodaji niso bile v celoti in zadostno vzpostavljene.

V času zaključka analize je bil predlog uredbe predstavljen na delovnih skupinah Sveta, se pa pričakuje njen sprejem v roku enega leta. Z napovedanimi novimi določili bo potrebno le-te upoštevati pri izvedbi prenove e-identitet, predvsem pa zagotoviti ustrezne skladne pravne okvirje.

2.4. Aktivnosti Evropske komisije

2.4.1. Projekt STORK in STORK 2.0

MPJU je sodeloval kot eden izmed 31 partnerjev iz 17 držav v projektu velikih razsežnosti STORK za varno priznavanje elektronskih identitet med državami EU (angl. *Secure Identity Across Borders Linked*, http://www.eid-stork.eu/) iz Okvirnega programa za konkurenčnost in inovacije (CIP, angl. *Competitiveness and Innovation Framework Programme*). Namen projekta STORK je bilo zagotoviti ravno čezmejno priznavanje in uporabo elektronskih identitet in s tem državljanom EU olajšati dostop do e-storitev uprav drugih držav članic (kot je npr. zahteva Direktive o storitvah na notranjem trgu po vzpostavitvi enotne kontaktne točke s storitvami za poslovne subjekte, v nadaljevanju na kratko *EKT*). Projekt STORK državljanom EU omogoča, da izkažejo svojo identiteto v elektronsko podprtih upravnih postopkih in pri tem uporabijo e-identifikatorje (gesla, e-osebne izkaznice, digitalna potrdila), ki so jih prejeli v svoji državi. Projekt od držav članic ni terjal nobenih sprememb nacionalnih e-identifikatorjev. Tako je bila naloga držav članic, da so vzpostavile ustrezno informacijsko infrastrukturo oz. jo prilagodile tako, da je bilo možno realizirati čezmejno priznavanje e-identifikatorjev. STORK je s šestimi različnimi piloti[10] prikazal praktično uporabo tega priznavanja s pomočjo rešitev, razvitih v projektu. Povezal in vzpostavil je različne nivoje zaupanja med državami članicami in njihovimi storitvami. Rezultati STORK so odprte, prilagodljive in prenosljive rešitve.

Ena izmed osnovnih nalog projekta je bila vzpostavitev različnih nivojev zaupanja med državami članicami in njihovimi storitvami ter posledično določitev preslikave med nivoji zaupanja posamezne

[10] Več o tem na spletnih straneh STORK: https://www.eid-stork.eu/pilots/index.htm.

države in nivoji projekta STORK. Tako so bili določeni naslednji nivoji zaupanja e-identitet oz. nivoji STORK QAA (angl. *Quality Authentication Assurance*):

- **nivo 1**: uporabniško ime in geslo brez posebnih zahtev; pri izdaji ni potrebno soglasje ali nadzor državnega organa,
- **nivo 2**: uporabniško ime in geslo z zahtevami glede ustreznosti gesla; pri izdaji je potrebno soglasje državnega organa,
- **nivo 3**: kvalificirana ali nekvalificirana digitalna potrdila v brskalniku, nekvalificirana digitalna potrdila na pametnem mediju, geselniki OTP (angl. *One Time Password*); pri izdaji je potreben nadzor državnega organa,
- **nivo 4**: kvalificirana digitalna potrdila na pametnem mediju; pri izdaji je potreben nadzor državnega organa v skladu z zahtevami Direktive o elektronskem podpisovanju.

STORK se je konec leta 2011 zaključil, načrtovan je prenos rezultatov pod okrilje komitološkega programa ISA za interoperabilnost delovanja e-storitev javnih uprav držav članic (več o tem v razd. 2.4.2).

Aprila 2012 se je pričel nov pilotni projekt velikih razsežnosti, t.i. STORK 2.0, v okviru katerega se bodo rešitve in infrastruktura obstoječega STORK prenesle tudi na poslovne subjekte, ki jih STORK ni obravnaval. Te rešitve bodo zato velikega pomena za nekatere nacionalne projekte, kot je npr. vzpostavitev EKT. Le-ta bo moral podpreti prepoznavanje tujih poslovnih subjektov in državljanov in jim na podlagi tega omogočiti uporabo storitev tega portala.

Rezultati pričujoče analize bodo vplivali tudi na izvedbo projekta STORK 2.0.

2.4.2. Projekt »e-SENS« (ali »Pilot vseh pilotov«)

Evropska komisija je v okviru razpisa CIP za leto 2012 razpisala nov pilotni projekt velikih razsežnosti (http://ec.europa.eu/information_society/activities/ict_psp/index_en.htm), ki naj bi konsolidiral vse rezultate obstoječih projektov CIP (poleg STORK in STORK 2.0 tudi SPOCS za drugo generacijo enotnih kontaktnih točk Storitvene direktive, PEPPOL za čezmejna e-javna naročila, epSOS za čezmejne storitve na področju e-zdravja itd.). Tako naj bi se poiskala skupna rešitev za osnovne gradnike, kjer so na prvem mestu prav e-identitete, e-avtentikacija in e-podpisovanje. V obstoječih projektih so namreč nastajale različne rešitve za ta področja (npr. avtentikacija v STORK, tako funkcionalnost je bilo potrebno zagotoviti tudi v epSOS), predvsem zaradi sočasnosti izvajanja teh projektov.

MPJU se je skupaj z drugimi slovenskimi partnerji priključilo temu konzorciju, sestavljenemu iz 20 različnih sodelujočih držav, pod imenom projekta e-SENS (angl. *Electronic Simple European Networked Services*). Če bo prijava konzorcija uspešna, bo projekt pričel z delom v letu 2013.

2.4.3. Program ISA

Program ISA (angl. *Interoperability Solutions for European Public Administrations*, http://ec.europa.eu/isa/) podpira čezmejno elektronsko sodelovanje javnih uprav (na nacionalnem, regionalnem in lokalnem nivoju), ki vodi v stroškovno učinkovito zagotavljanje javnih storitev, lažje izvajanje EU zakonodaje in spodbujanje enotnega trga. Program ISA oblikuje skupne okvire v podporo

interoperabilnosti, pripravlja in podpira generična orodja in infrastrukturo ter izvaja različne študije čezmejne interoperabilnosti.

Tako program ISA kot tudi njen predhodnik program IDABC (angl. I*nteroperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens*, http://ec.europa.eu/idabc/) obravnavata tudi interoperabilnost na področju e-identitet in avtentikacije.

2.4.4. Aktivnosti glede evropske osebne izkaznice (ECC)

Pobudnik za uvedbo enotnega standarda evropske osebne izkaznice (ECC, angl. *European Citizen Card*) je bila skupina Porvoo, ki se že 10 let ukvarja z elektronskimi identitetami (. Tehnično specifikacijo za ECC (Dokument CEN/TS 15480-1:2007) je pripravil Tehnični odbor CEN/TC 224 "Osebna identifikacija, elektronski podpis in kartice ter z njimi povezani sistemi in operacije", ki jo je potrdil Evropski odbor za standardizacijo (CEN, angl. *European Committee for Standardisation*) dne 17.6.2006. Obdobje veljavnosti CEN/TS je bilo sprva omejeno na tri leta. V tem času so bile države članice CEN (Avstrija, Belgija, Bolgarija, Ciper, Češka, Danska, Estonija, Finska, Francija, Nemčija, Grčija, Madžarska, Islandija, Irska, Italija, Latvija, Litva, Luksemburg, Malta, Nizozemska, Norveška, Poljska, Portugalska, Romunija, Slovaška, Slovenija, Španija, Švedska, Švica in Združeno kraljestvo) pozvane, da preko svojih nacionalnih uradov za standardizacijo objavijo obstoj CEN/TS, s potekom triletnega roka pa so se začele aktivnosti za pretvorbo CEN/TS v evropski standard in njegovo integracijo v evropski pravni red. Po uvedbi biometrične potne listine in biometričnega dovoljenja za prebivanje tujcev se pričakuje, da bo Odbor čl. 6 (Varnost potovalnih in identifikacijskih dokumentov) pri EK prevzel aktivnejšo vlogo tudi pri implementaciji ECC v državah članicah EU.

CEN/TS 15480 se sestoji iz naslednjih sklopov:

- Sklop 1: Fizične in električne karakteristike, lastnosti transportnega protokola;
- Sklop 2: Logične strukture podatkov in storitve kartice;
- Sklop 3: ECC interoperabilnost ob uporabi aplikacijskega vmesnika;
- Sklop 4: Priporočila za izdajo, delovanje in uporabo ECC.

Pristojna institucija javne uprave lahko pooblasti zasebno organizacijo, da v njenem imenu opravlja vse ali del storitev ECC.

Tehnična specifikacija CEN/TS 15480-1:2007 opredeljuje ECC kot pametno kartico, ki jo izda pristojna državna institucija. ECC mora ponujati vse ali vsaj del naslednjih storitev:

1) Preverjanje identitete;
2) Dostop do storitev e-uprave;
3) Potovalni dokument znotraj Evropske unije.

2.5. e-Identitete v drugih državah EU

V EU se vse bolj poudarja pomen delovanja notranjega trga in nudenja čezmejnih elektronski storitev, tudi za storitve javne uprave. Kot je bilo navedeno uvodoma, spada področje avtentikacije in e-podpisa med ključne storitve za zagotavljanje večine storitev, ki jih nudijo države članice na področju e-uprave.

V poročilu, ki ga je glede stanja elektronskih identitet v državah članicah Evropske unije pripravila Evropska komisija v okviru programa IDABC leta 2009 (dostopno preko spletne strani http://ec.europa.eu/idabc/servlets/Doc?id=32521, več o programu v razd. 2.4.3), **je imelo tega leta že 13 od 32 držav, zajetih v analizo, uvedene elektronske osebne izkaznice oz. e-identitete**. V 6 izmed teh držav kvalificirana digitalna potrdila za potrebe elektronske osebne izkaznice izdajajo zasebni overitelji po pooblastilu države (Avstrija, Islandija, Lihtenštajn, Luksemburg, Nizozemska, Švedska), v 7 državah pa overitelj digitalnih potrdil deluje v okviru državne uprave (Belgija, Estonija, Finska, Italija, Litva, Portugalska in Španija). V poročilu je navedeno, da 12 ostalih držav (vključujoč Slovenijo) napoveduje uvedbo elektronske osebne izkaznice v bližnji prihodnosti, le 5 držav pa v kratkem ne načrtuje njene uvedbe (Danska, Irska, Latvija, Norveška, Velika Britanija). Evropska komisija je v tem poročilu napovedala pozitiven trend uvajanja elektronskih osebnih izkaznic v prihodnjih letih na podlagi spremljanja tega področja od pričetka tega programa od l. 2005. Nemčija je bila naslednja država, ki je v letu 2010 pričela z izdajanjem elektronske osebne izkaznice, Avstrija pa je t.i. kartico občana svojim državljanom ponudila tudi preko mobilnega telefona.

Trend uvajanja e-identifikatorjev je viden prav na področju identifikacije preko mobilnih telefonov, saj se tovrstne rešitve uporabljajo v 6 državah, še 6 držav pa njihovo uvedbo načrtuje v kratkem. Ker mobilni telefoni zaenkrat (razen redkih izjem) neposredno še ne omogočajo uporabe digitalnih potrdil, se za potrebe identifikacije preko mobilnih telefonov uporabljajo trije zelo različni koncepti:

- časovno omejeno geslo z dvostopenjskim načinom avtentikacije preko sporočil SMS,
- kartica SIM, ki podpira PKI (Infrastrukturo Javnih Ključev) in predstavlja napravo za varno tvorjenje podpisa za kvalificiran podpis – WPKI (Estonija),
- varnostni strojni modul (HSM, angl. *Hardware Security Module*), s katerim upravlja institucija in dostop omogoča le na podlagi ustrezne avtentikacije uporabnika s pomočjo mobilnega telefona. HSM predstavlja napravo za varno tvorjenje podpisa za kvalificiran podpis, ker se na njem hranijo zasebni ključi (Avstrija).

V nadaljevanju je zaradi **aktualnosti** povzeto stanje v Nemčiji, Švedski in Avstriji.

2.5.1. Nova osebna izkaznica v Nemčiji

V Nemčiji so novembra 2010 začeli uporabljati nove pametne osebne izkaznice, starih pa ni mogoče več dobiti. Nove e-osebne izkaznice se od starih razlikujejo po vgrajenem čipu RFID (angl. *Radio Frequency IDentification*), ki ima v elektronski obliki zapisane podatke o imenu, naslovu, rojstnem datumu, višini, barvi oči in las, izdajatelju in sliko. Prednost novih izkaznic je širši obseg uporabe, saj se bo moč z njimi identificirati na svetovnem spletu, pri elektronskih bančnih transakcijah, pri preprečevanju ribarjenja podatkov in podobno. Z novimi osebnimi karticami naj bi bilo mogoče varno nakupovati in seveda poslovati s številnimi nemškimi vladnimi službami. Nove osebne izkaznice nemškim oblastem omogočajo hitro in natančno legitimacijo državljanov. Dostop do osebnih podatkov naj bi bil omogočen le organom pregona, davčni službi in javni upravi.

Ta nova osebna izkaznica ima vgrajene številne varnostne mehanizme, ki se nanašajo predvsem na njeno fizično zaščito. Je bila pa ta izkaznica deležna številnih kritik glede same varnosti elektronsko shranjenih podatke in same uporabe brezkontakntega čipa. Osebne podatke, ki se namreč nahajajo na osebni izkaznici in so shranjeni na delu čipovja RFID, varuje varnostna tehnologija BAC (angl. *Basic Access Control*). Ta sicer že dalj časa ni več zanesljiva, saj je »podlegla« že številnim univerzitetnim

raziskovalcem in specialistom za informacijsko varnost. Občutljivejše osebne in druge podatke sicer varuje protokol, ki je lastniški in zaprt. Nemško ministrstvo za notranje zadeve zagotavlja, da je ta, vsaj zaenkrat, dovolj varen pred nadobudnimi hekerji.

Konec leta 2011 so v Nemčiji izdali šest milijonov teh osebnih izkaznic, do konca leta 2020 pa naj bi imel vsak državljan svojo.

2.5.2. Centralni sistemi za uporabo e-identitet na Švedskem

Na Švedskem ima kar 4 milijone državljanov e-identiteto. Le-ta navadno temelji na kvalificiranih in nekvalificiranih digitalnih potrdilih ter kriptografskih ključih, pa tudi na drugih oblikah, npr. z avtentikacijo preko mobilnih telefonov. V večini primerov e-identitete izdaja zasebni sektor, predvsem banke in telekomunikacijski operaterji. Za potrebe e-storitev javne uprave le-ta izdajateljem e-identitet plačuje storitve, povezane z avtentikacijo državljanov. To odvisnost javne uprave od zasebnega sektorja in tudi zahtevnost obvladovanja različnih tehnoloških rešitev e-identitet, ki jih izdajajo v zasebnem sektorju, je švedska vlada želela urediti za daljše obdobje. Leta 2011 je zato ustanovila majhno agencijo »eIDentification Board«, ki pripravlja koncept prenove teh rešitev. Načrtujejo vzpostavitev koncepta centralnega avtentikacijskega sistema, ki bo temeljil na žetonih (angl. *identity token*) in tehnologiji SAML 2.0, podpiral pa bo različne tehnologije e-identitet, ne zgolj osnovanih na digitalnih potrdilih. Na podlagi teh žetonov se bo izvajalo tudi centralno e-podpisovanje, ki tako ne bo več omejeno samo na imetnike digitalnih potrdil, temveč bo omogočeno vsem uporabnikom, ki se bodo uspešno avtenticirali za potrebe elektronskega podpisovanja.

2.5.3. Kartica občana v Avstriji

V Avstriji se uporablja inovativen koncept »kartice občana« (nem. *Bürgerkarte*), ki je namenjena e-identifikaciji pri opravljanji e-storitev, ki jih nudi javna uprava in kjer je to zakonsko določeno. Kartice občanov vsebujejo tudi kvalificirano digitalno potrdilo, ki omogoča e-podpisovanje različnih dokumentov, kjer se običajno zahteva lastnoročni podpis. Kartica občana se lahko uporablja tudi za identifikacijo in e-podpisovanje v osebne namene, npr. za storitve e-bančništva.

Kartica občana je na voljo v različnih oblikah, saj ni odvisna od vrste tehnologije in ne zahteva posebne vrste kartice. V večini primerov je nosilec podatkov čip (na pametni kartici npr. bančni ali kartici zdravstvenega zavarovanja) ali mobilni telefon v povezavi z varnostnim modulom. Bistveno je, da kartica občana omogoča kvalificirani elektronski podpis in vsebuje »povezavo na osebo« (angl. identity link), ki vsebuje ustrezno zavarovane osebne podatke in funkcije kot tudi morebitna izdana pooblastila. Za uporabo pametne kartice občani potrebujejo računalnik in čitalnik kartic ter ustrezno programsko opremo, ki je brezplačna in pripravljena za uporabo na različnih operacijskih sistemih. Imetniki kartic morajo svojo pametno kartico (ki so jo lahko pridobili pri različnih institucijah, npr. banki) aktivirati kot kartico občana (preko spletne storitve, s katero upravlja overitelj A-Trust) in lahko takoj nato prične z njeno uporabo, ki je brezplačna. Podoben postopek registracije je predviden tudi v primeru, da se občan odloči za avtentikacijo oz. e-podpisovanje s pomočjo mobilnega telefona, pri čemer pa za tovrstno uporabo seveda ne potrebuje čitalnika kartic in dodatne programske opreme. To je tudi glavni razlog, da se ta način uporabe vzpodbuja in se mu celo daje prednost v primerjavi s pametnimi karticami.

2.6. Priporočila OECD

Mednarodna organizacija za ekonomski razvoj OECD (angl. *Organisation for Economic Co-operation and Development*) v zvezi z avtentikacijo podaja naslednja priporočila[11]:

- vzpostaviti je treba tehnološko nevtralne pristope za vzpostavitev avtentikacije oseb in poslovnih subjektov, v skladu s smernicami OECD za varstvo informacijskih sistemov in omrežij in smernicami OECD o varstvu zasebnosti in čezmejnem prenosu osebnih podatkov,
- zagotoviti razvoj, ustrezne pogoje in uporabo produktov avtentikacije, ki vključujejo poslovne prakse, vključno s tehničnimi in netehničnimi varovali, ki omogočajo varnost in zasebnost uporabnikov, njihovih podatkov in identitete,
- spodbujati združljivost in tehnično interoperabilnost avtentikacijskih shem v javni upravi in zasebnem sektorju, z namenom pospeševanja čezmejnih spletnih interakcij in transakcij ter zagotovitvijo, da bodo avtentikacijski produkti in storitve delovali na nacionalni in na mednarodni ravni,
- povečati zavedanje vseh vključenih uporabnikov o prednostih uporabe elektronske avtentikacije na nacionalni in mednarodni ravni.

Pomanjkanje pravil za e-avtentikacijo se sicer pogreša na ravni EU v splošnem, OECD pa je na to opozoril Slovenijo v času njenega vključevanja v to organizacijo. Pričakuje se ustrezna ureditev z novim predlogom uredbe, ki bo urejala to področje (glej razd. 2.3.1).

2.7. Mednarodni forum o upravljanju e-identitet

Na 8. srečanju foruma »Government Discussion Forum on Electronic Identity Management", ki vsako leto zbere strokovnjake iz celega sveta (največ pa iz Azije), v začetku leta 2011 je bilo sprejetih preko 60 sklepov, ki se nanašajo na upravljanje e-identitet. Najpomembnejši med njimi so naslednji:

- do leta 2014 se (v svetovnem merilu) pričakuje povečanje obsega izdajanja e-identitet s sedanjih 2 milijard na 3.6 milijard,
- učinek uvedbe e-identitet v državah, ki imajo vzpostavljene registre prebivalstva, je bistveno večji kot v državah, kjer teh registrov ni,
- pri uvajanju e-identitet je jasen trend njihove uporabe zgolj kot enoličnega identifikatorja osebe in ne kot nosilca aplikacij ali širokega nabora osebnih podatkov,
- različnost področij, ki jih pokrivajo posamezne državne ustanove, ter varovanje osebnih podatkov sta glavna razloga, da so multifunkcijske e-identitete prej izjema kot pravilo, saj je za njihovo uvedbo poleg ustreznih tehničnih rešitev potrebna tudi politična podpora,
- projekti uvedbe e-identitet na državnem nivoju so uspešni le v primeru, da njihova uporaba presega okvire storitev e-uprave in da je razširjena tudi na področje zasebnih ponudnikov storitev.

[11] Priporočila so dostopna na http://www.oecd.org/sti/interneteconomy/oecdrecommendationonelectronicauthenticationandguidanceforelectronicauthentication.htm

Mobilne naprave bodo v bodoče zavzemale pomembno vlogo pri vpeljavi nacionalnih rešitev na področju e-identitet in bodo tudi ena izmed glavnih tem naslednjega foruma, ki bo potekal novembra 2012 (http://www.apsca.org/getconnected/archive_detail.php?id=2141).

3. PRAVNE MOŽNOSTI UREJANJA E-IDENTIFIKATORJEV V SLOVENIJI

3.1. Pravni okvirji v Sloveniji

Osnovno pravno podlago za elektronski podpis in s tem tudi za urejanje e-identifikatorjev predstavlja ZEPEP, določila iz tega zakona pa povzemajo številni področni zakoni kot so npr. Zakon o splošnem upravnem postopku (ZUP), Zakon o pravdnem postopku (ZPP) in Zakon o preprečevanju pranja denarja in financiranju terorizma (ZPPDFT).

3.1.1. Zakon o elektronskem poslovanju in elektronskem podpisu

ZEPEP ureja elektronsko poslovanje, ki zajema poslovanje v elektronski obliki z uporabo informacijske in komunikacijske tehnologije in uporabo elektronskega podpisa v pravnem prometu, kar vključuje tudi elektronsko poslovanje v sodnih, upravnih in drugih podobnih postopkih. S tem zakonom se uvaja enakovrednost elektronskega in lastnoročnega podpisa na dokumentih, kadar so izpolnjeni nekateri pogoji.

Po ZEPEP je lastnoročnemu podpisu enakovreden in ima zato enako veljavnost in dokazno vrednost t.i. varen elektronski podpis, ki je overjen s kvalificiranim potrdilom. Varen elektronski podpis je elektronski podpis, ki izpolnjuje nekaj, v zakonu taksativno naštetih zahtev. Tako mora biti izključno povezan s podpisnikom in je tako iz njega mogoče zanesljivo ugotoviti podpisnika. Hkrati mora biti podpis tehnološko zasnovan tako, da je povezan s podatki, na katere se nanaša, in bi bila opazna vsaka sprememba teh podatkov ali povezave z njimi, ki se bi zgodila po podpisu. Podpisnik pa mora podpis oblikovati s pomočjo sredstev za varno elektronsko podpisovanje pod svojim izključnim nadzorom. Sredstva za varno elektronsko podpisovanje se od običajnih sredstev za elektronsko podpisovanje razlikujejo v tem, da izpolnjujejo posebne pogoje glede varnosti in zanesljivosti, ki jih določa ZEPEP, podrobneje pa na podlagi zakona izdana uredba. Da bi bil varen elektronski podpis enakovreden lastnoročnemu, mora biti overjen še s kvalificiranim potrdilom. Takšno potrdilo ima enake značilnosti kot običajno potrdilo, le da zakon zanj podrobneje predpisuje njegovo vsebino ter način izdaje, uporabe in preklica. Prav tako so z zakonom in uredbo predpisani posebni, strožji pogoji glede overiteljev, ki izdajajo takšna kvalificirana potrdila (obvezno zavarovanje odgovornosti, posebne zahteve glede opreme in zaposlenih, zahtevnejši postopki, notranja pravila in podobno).

Zaradi uskladitve z EU zakonodajo (več o tem v razd. 2.3), ki ureja to področje, je v predlogu sprememb ZEPEP[12] tako del, ki se nanaša na zahteve za kvalificiran podpis (kar na kratko pojmujemo kot enakovreden e-podpis lastnoročnemu), kot predlogi, ki se nanašajo na uskladitev zahteve za uporabo sredstev za varno elektronsko podpisovanje za kvalificiran e-podpis:

- Varen elektronski podpis se nadomesti z naprednim, kar bolj ustreza prevodu direktive o e-podpisu, kjer se uporablja »Advanced e-signature«.

[12] Že uvodoma je bilo pojasnjeno, da je bil postopek revizije ZEPEP zaustavljen. Nadaljevanje se pričakuje v letu 2013 oz. po sprejetju nove regulative tega področja na ravni EU.

- »Sredstva za varno podpisovanje« se nadomestijo z »napravami za varno tvorjenje podpisa«, kar bolj ustreza »Secure Signature-Creation Device" ali na kratko SSCD.
- Novost je uvedba izraza kvalificiran elektronski podpis – to je e-podpis, ki je enakovreden lastnoročnemu in določen kot napreden elektronski podpis, overjen s kvalificiranim potrdilom in oblikovan z napravo za varno tvorjenje podpisa.

3.1.2. Zakon o osebni izkaznici

Leta 2008 je bil Zakon o osebni izkaznici (ZOIzk) noveliran, da bi se vzpostavila pravna podlaga za izdajo elektronskih osebnih izkaznic, ki bi vključevale tudi kvalificirano digitalno potrdilo in imele funkcijo zdravstvene kartice. MNZ je takrat izvedlo mednarodno javno naročilo za izbor izdelovalca novih osebnih izkaznic, vendar ponudnik zaradi previsokih cen ni bil izbran. Zato je ministrstvo opustilo možnost uvedbe elektronske osebne izkaznice. Tako je bil maja 2011 sprejet novi zakon, s katerim so bile izločene določbe, ki so bile vezane na uvedbo elektronske osebne izkaznice. Pravni red Evropske unije sicer ureditev izdaje osebnih izkaznic prepušča pravu vsake posamezne članice in na tem področju nima obvezujočih smernic ali direktiv. Po ocenah MNZ bi bilo pred uvedbo novosti na področju spremembe obrazcev in funkcionalnosti osebnih izkaznic smiselno počakati na določitev enotnih smernic za evropske osebne izkaznice ECC, tako glede biometrije kot glede njihove uporabe za opravljanje elektronskih storitev.

3.2. Pravne možnosti e-identitet

Pravni okvirji (ZEPEP in drugi področni zakoni) podrobneje ne določajo načinov oz. različnih nivojev zaupanja posameznih e-identitet oz. digitalnih potrdil. Na pomanjkanje ustrezne ureditve pravil za elektronsko avtentikacijo je v svojem poročilu, pripravljenem v času vključevanja Slovenije, opozorila tudi organizacija OECD (več o tem v razd. 2.6). Skladno s tem priporočilom in zaradi očitnih potreb je tako v Akcijskem načrtu elektronskega poslovanja javne uprave do 2015 predvidena tudi priprava politike za avtentikacijo, ki bo jasno uredila pravila avtentikacije in določila nivoje zaupanja.

Kljub manjkajoči ureditvi na področju nivojev zaupanja e-identitet pa se je za potrebe uporabe storitev e-uprave izoblikovala praksa, v skladu s katero se v sistemih e-uprave uporabljajo e-identifikatorji treh različnih nivojev:

- **nivo 1**: uporabniško ime in geslo, izdano uporabniku ob prijavi na posameznem portalu,
- **nivo 2**: kvalificirana digitalna potrdila v brskalniku,
- **nivo 3**: kvalificirana digitalna potrdila na pametnem mediju.

Dejansko so identifikatorji nivoja 1 uporabni le za omejen nabor storitev e-uprave, saj zaradi nizke stopnje zaupanja omogočajo zgolj opravljanje postopkov, kjer identiteta uporabnika ni ključnega pomena. Po drugi strani zaenkrat le redko katera e-storitev dostop omejuje na e-identifikatorje nivoja 3 iz vsaj dveh razlogov:

- do vzpostavitve t.i. zanesljivega seznama nadzorovanih overiteljev v skladu z Odločbo 2009/767/ES ni bilo na voljo mehanizma, ki bi aplikacijam na enostaven način omogočal razločevanje med kvalificiranimi potrdili na pametnih medijih in kvalificiranimi potrdili v shrambi brskalnika; z vzpostavitvijo omenjenega seznama je to sorazmerno enostavno izvedljivo,

- velika večina v Sloveniji izdanih kvalificiranih potrdil ni shranjenih na pametnem mediju, zato bi zahteva po e-identifikatorjih nivoja 3 v praksi pomenila izključitev velikega števila potencialnih uporabnikov e-storitev.

Z uveljavitvijo predvidene spremembe Zakona o elektronskem poslovanju in elektronskem podpisu bodo jasneje določene zahteve glede različnih vrst elektronskega podpisa, zato lahko pričakujemo, da bodo bolj aktualne tudi zahteve po razlikovanju med e-identitetami nivojev 2 in 3 za potrebe posameznih e-storitev. **Na naslednjih straneh je tako predstavljenih nekaj možnosti zakonskih ureditev uporabe e-identifikatorjev nivoja 3**. Ne glede na pričakovano spremembo ZEPEP in način urejanja e-identitet pa splošen dvig zahtev glede obvezne uporabe e-identifikatorjev nivoja 3 ni niti smiseln niti potreben. Ponudnik vsake e-storitve mora namreč sprejeti odločitev, kateri nivo zaupanja je za njegove potrebe najnižji še sprejemljiv, pri čemer mora upoštevati predvsem vidik občutljivosti storitve glede zaupanja v uporabljene e-identitete.

V nadaljevanju so podani trije predlogi za ureditev področja kvalificiranega elektronskega podpisa upoštevajoč predlagane spremembe ZEPEP. Prvi predlog je e-osebna izkaznica, ki pomeni nadgradnjo klasične osebne izkaznice z ustreznim čipom in kvalificiranim digitalnim potrdilom. Druga možnost izkorišča akreditacijo overiteljev, ki bi pomenila višjo kakovost in varnost akreditiranih e-identitet. Tretja možnost ne prinaša bistvenih novosti, pomeni pa prilagoditev overiteljev zahtevam, ki jih prinaša novela ZEPEP.

3.2.1. E-osebna izkaznica

Pretekle aktivnosti: Multifunkcijska elektronska osebna izkaznica

Ideja o elektronski osebni izkaznici je bila predstavljena že leta 2007, vanjo naj bi bila po prvotnih predlogih vključena tudi vozniško dovoljenje in davčna številka.

S ciljem razširitve funkcionalnosti osebne izkaznice je bila leta 2008 na predlog MNZ imenovana medresorska delovna skupina za izvedbo projekta »Multifunkcijska elektronska osebna izkaznica«, vendar so bili s strani strokovne javnosti in Informacijskega pooblaščenca izraženi pomisleki glede varnosti združevanja več osebnih podatkov na takšni osebni izkaznici (EMŠO, številka zdravstvenega zavarovanja in davčna številka) ter zadržki glede varnosti povezav in dostopov do evidenc iz različnih področij.

Zaradi teh pomislekov in zaradi previsoke ponujene cene v javnem naročilu je strokovna komisija ocenila, da je projekt v danem trenutku neracionalen in je bil začasno ustavljen. Na nivoju Evropske unije je bil v okviru aktivnosti ECC letu 2010 izveden posnetek stanja na področju izdaje elektronske osebne izkaznice, katerega ključne ugotovitve so:

- v 17 državah je osebna izkaznica obvezen dokument;
- v 13 državah se izdajajo navadne osebne izkaznice, osem držav izdaja e-osebne izkaznice s kontaktnim in/ali RFID čipom, dve državi sploh nimata osebnih izkaznic (Norveška, Združeno kraljestvo);
- osem držav izdaja elektronske osebne izkaznice z možnostjo shranjevanja biometričnih podatkov, od tega 6 (Belgija, Italija, Litva, Portugalska, Španija in Švedska) ima za to zakonsko podlago;

- na vprašalnik niso odgovorile Danska, Finska, Francija, Grčija, Irska, Latvija, odgovor Združenega kraljestva ni bil vključen v tej analizi, ker se je njihova vlada v juniju 2010 odločila, da zaradi finančne krize projekt uvedbe e-osebne izkaznice zamrzne.

Glede na pozitivne izkušnje nekaterih evropskih držav, ki so že uvedle elektronsko osebno izkaznico in trend naraščanja (IDABC, 2009), pa je njena uvedba obravnavana tudi kot ena izmed možnosti v tem dokumentu.

Predlog nove e-osebne izkaznice

E-osebna izkaznica (v nadaljevanju *eOI*) bi bila javna listina, s katero bi državljan Republike Slovenije izkazoval svojo istovetnost in državljanstvo v fizičnem in elektronskem svetu in s katero bi, kot z obstoječo osebno izkaznico (v nadaljevanju *OI*), lahko potoval v določene države ter z njo opravljal e-storitve.

Vsak državljan Republike Slovenije s prijavljenim stalnim prebivališčem v Republiki Sloveniji ali v tujini bi imel pravico do e-osebne izkaznice. Polnoletni državljani s stalnim prebivališčem v Sloveniji, ki ne bi imeli druge veljavne javne listine, opremljene s fotografijo, bi morali imeti e-osebno izkaznico.

Da bi dosegli čim večji učinek uvedbe e-osebne izkaznice, bi njena uporaba morala biti zanimiva za čim širši krog uporabnikov in ponudnikov elektronskih storitev, zato bi se osebna izkaznica izdajala izključno kot e-osebna izkaznica.

Format in videz e-osebne izkaznice bi bila enaka kot pri obstoječi osebni izkaznici, le da bi bil v kartico vgrajen še čip kot nosilec digitalnega potrdila za identifikacijo in poslovanje imetnika v elektronskem svetu (identifikacija, avtentikacija, šifriranje, digitalno podpisovanje). Kvalificirana digitalna potrdila za potrebe e-osebne izkaznice bi izdajal overitelj, ki bi deloval v okviru državnega organa oz. s strani državnega organa pooblaščeni overitelj.

Uvedba e-osebne izkaznice bi zahtevala spremembo Zakona o osebni izkaznici, kjer bi bili definirani namen, upravičenost pridobitve in način izdaje e-osebne izkaznice. Z ustreznimi podzakonskimi akti k Zakonu o osebni izkaznici pa bi predpisali določene tehnične lastnosti elektronske osebne izkaznice, podatke na sami osebni izkaznici, podatke na čipu, profil potrdila itd.

Prednosti:

- ni potreb po večji prilagoditvi aplikacij, saj gre za poznan koncept, ki temelji na kvalificiranih digitalnih potrdilih
- potrdilo na uradnem identifikacijskem dokumentu, kar poveča zavedanje in zaupanje uporabnika
- za uporabnika razumljiva in sprejemljiva rešitev (isti dokument se uporablja za identifikacijo v fizičnem in elektronskem svetu)
- visok nivo varnosti e-identitete
- skladnost s trendi razvoja v drugih državah EU (po podatkih študije IDABC)
- uporaba standardizirane naprave za varno tvorjenje podpisa

Slabosti:

- izpostavljenost potrdila (npr. izročitev osebne izkaznice v hotelski recepciji)
- daljši rok za uvedbo (2 leti)
- povezava z dokumentom (potrebna zamenjava veljavne OI v primeru nedelovanja e-identitete npr. zaradi okvare čipa ali pozabljenega gesla)
- izdajatelj eOI mora skrbeti za zagotavljanje poslovnega cikla podpore (tehnična pomoč, zagotavljanje opreme in uporaba)
- razkorak med trenutnimi veljavnostmi – kvalificirana digitalna potrdila imajo veljavnost do 5 let, klasična OI pa 10 let
- zaradi potrebe po nujni zamenjavi 500.000 OI v letu 2012, je uvedba eOI iz vidika učinkovitosti na kratek rok neracionalen ter finančno nevzdržen

---

Tveganja:

- postopna izločitev drugih overiteljev
- potrebna sprememba zakonodaje
- zahtevna vzpostavitev sistema zaradi usklajevanja med institucijami
- pogodba oz. dogovor med institucijami
- politična podpora
- zagotovitev finančnih sredstev

Priložnosti:

- možnost integracije z drugimi sistemi (urbana...), uporaba v drugih sektorjih
- možnost dodajanja biometričnih podatkov in s tem povečanja nivoja varnosti dokumenta
- povečanje uporabe e-storitev
- za uporabnika predvidoma cenovno ugodna rešitev (večja količina izdanih eOI)
- skladnost s smernicami ECC
- enotnost rešitev za e-identitete za čezmejno opravljanje storitev
- možnost nadomestitve lokalno nameščene podpisne komponente s centralnim podpisnim strežnikom

---

3.2.2. Akreditirana e-identiteta

Višji nivo upravljanja e-identitet bi lahko vpeljali z določitvijo dodatnih zakonskih oz. formalnih zahtev glede e-identitet, ki bi bile primerne za potrebe identifikacije uporabnikov v različnih e-storitvah javne uprave in zasebnih ponudnikov. Ker ZEPEP že v celoti ureja pogoje za overitelje kvalificiranih potrdil z vidika elektronskega podpisovanja, bi se dodatne zahteve nanašale zgolj na avtentikacijo uporabnikov na osnovi digitalnih potrdil. Z vzpostavitvijo dodatnega, višjega nivoja delovanja overiteljev bi le-ti imeli možnost, da se prostovoljno odločijo za vključitev v tak sistem in tako svojim uporabnikom omogočijo avtentikacijo s kvalificiranimi digitalnimi potrdili v različnih e-storitvah. Na ta

način bi vzpostavili pregleden sistem upravljanja e-identitet, ki bi po eni strani overiteljem prepuščal izbiro in odločitev za vključitev v akreditacijsko shemo, po drugi strani pa omogočal sorazmerno enostavno urejanje področja upravljanja e-identitet nivoja 3 t.j. kvalificiranih digitalnih potrdil na pametnem mediju. Za ustrezno uveljavitev rešitve pa bi bilo potrebno na primeren način določiti tako upravljavca akreditacijske sheme kot e-storitve oz. področja e-uprave, kjer je uporaba e-identifikatorjev nivoja 3 obvezna. Upravljavec akreditacijske sheme bi moral biti določen npr. v ZEPEP ali ZOIzk, obvezno uporabo e-identifikatorjev nivoja 3 pa bi lahko določali tudi posamezni področni zakoni (npr. ZUP, ZPP, ZPPDFT…) ali sama politika za avtentikacijo, v kateri bodo sicer določeni različni nivoji e-identitet.

Namen predlagane akreditacijske sheme je uporabnikom omogočiti dostop do kakovostnih e-identitet ter overiteljem ponuditi ustrezen okvir za izboljšanje njihovih storitev, da bi dosegli stopnjo zaupanja, varnosti in kakovosti, kot jo zahteva razvijajoči se trg. Upravljavec akreditacijske sheme bi moral oblikovati pogoje oz. standarde na področju upravljanja e-identitet ter spodbujati razvoj najboljših praks. V predlagani rešitvi bi akreditirane e-identitete predstavljala kvalificirana digitalna potrdila, izdana s strani overiteljev, ki bi se prostovoljno vključili v predstavljeno akreditacijsko shemo. Overitelji bi za pridobitev tega statusa morali izpolnjevati zahteve, ki bi jih upravljavec sheme določil na osnovi ustreznih zakonskih določil (npr. obvezna uporaba naprav za varno tvorjenje podpisa in enotnega profila digitalnega potrdila: poenoten zapis identifikatorja imetnika, določitev namena uporabe ključa, zapis oznake kvalificiranega potrdila na pametnem mediju itd.).

Eno izmed možnosti urejanja področja upravljanja e-identitet na opisani način predstavlja uporaba instrumenta prostovoljne akreditacije overiteljev, ki je sicer predvidena tudi v obstoječem ZEPEP, vendar zaradi različnih razlogov akreditacijski organ do sedaj ni bil vzpostavljen. Glavni razlog je verjetno v tem, da njegova vzpostavitev v skladu s trenutno zakonodajo za morebitne akreditirane overitelje ne predstavlja posebne dodane vrednosti, obenem pa se je dodobra uveljavil pristop, po katerem se za potrebe opravljanja e-storitev uporabljajo vsa kvalificirana potrdila overiteljev, navedenih v registru overiteljev. S predlaganimi spremembami ZEPEP se bo to spremenilo, saj bo akreditacijski organ imel možnost, da s svojim pravilnikom določi dodatne zahteve, ki jih bodo overitelji morali izpolnjevati, da bodo pridobili status akreditiranega overitelja, in prav to možnost bi lahko izkoristili za potrebe urejanje e-identitet. Akreditacijski organ naj bi že v skladu z obstoječo zakonodajo vodil javni elektronski register pri njem prostovoljno akreditiranih overiteljev, v skladu s predlaganimi spremembami ZEPEP pa bo zadolžen tudi za vodenje javnega elektronskega registra naprav za varno tvorjenje podpisa. Z novo uredbo na ravni EU pa bi bil lahko ta organ zadolžen tudi za akreditacijo ostalih, z e-identitetami povezanih storitev.

Prednosti:

- enotni profil digitalnih potrdil (kar bi poenostavilo predvsem razvoj novih aplikacij ter prepoznavnost tudi za čezmejno opravljanje storitev)
- s to rešitvijo ne izločimo drugih overiteljev (možnost vključitve komercialnih overiteljev v akreditacijsko shemo)
- visok nivo varnosti e-identitete

Slabosti:

- potrebno je zakonsko urediti akreditacijsko shemo in njenega upravljavca (v primeru akreditacijskega organa je ta sicer v ZEPEP naveden, vendar do sedaj ni bil vzpostavljen),
- dodatna ureditev na področju e-identitet, ki za ponudnike storitev predstavlja nov koncept v primerjavi z obstoječimi oz. poznanimi rešitvami
- zamenjava lokalno nameščene podpisne komponente s centralnim podpisnim strežnikom je težje izvedljiva

---

Tveganja:

- v primeru pomanjkanja interesa overiteljev za vključitev v dodatno ureditev predlagana rešitev ne bo dosegla želenega namena, obenem pa bo namesto poenostavitve postopkov integracije potrdil za ponudnike storitev pomenila predvsem povečano kompleksnost
- potrebna je sprememba zakonodaje oz. ustrezna pravna ureditev

---

Priložnosti:

- možnost formalne določitve uporabe akreditiranih e-identitet v posameznih aplikacijah
- možnost, da ponudniki storitev enostavneje določijo ustrezne nivoje zaupanja za e-storitve
- možnost razvoja drugih, z e-identitetami povezanih storitev

---

3.2.3. Kvalificirana digitalna potrdila na pametnih medijih

V nadaljevanju predstavljena rešitev ne prinaša bistvenih novosti oziroma sprememb na področju upravljanja e-identitet, saj pomeni zgolj nadgradnjo obstoječe ureditve sistema, kjer se za opravljanje e-storitev uporabljajo vsa kvalificirana potrdila overiteljev, navedenih v registru overiteljev. Predvidena sprememba zakonodaje obstoječi ZEPEP dopolnjuje z opredelitvijo kvalificiranega elektronskega podpisa in ločuje med elektronskim podpisom, naprednim elektronskim podpisom in kvalificiranim elektronskim podpisom, čemur se bodo morali prilagoditi tako ponudniki storitev kot tudi overitelji.

Za ponudnike storitev sprememba ZEPEP pomeni predvsem sprejetje odločitve o najnižjem nivoju e-identitet, ki je še sprejemljiv za opravljanje posamezne storitve; v praksi se bodo tako odločali med vsemi kvalificiranimi potrdili in kvalificiranimi potrdili na pametnem nosilcu. Podatek o tem, ali je bilo določeno kvalificirano potrdilo s strani njegovega izdajatelja shranjeno na pametnem nosilcu ali ne, je na voljo v zanesljivem seznamu nadzorovanih overiteljev, ki ga vodi MIZKŠ. Tako kot v predhodno predstavljeni možnosti bi tudi v tem primeru bilo potrebno na ustrezen način določiti e-identitete, primerne za opravljanje posameznih storitev e-uprave, kar se trenutno ureja s področnimi zakoni.

Da bi izdajatelji kvalificiranih digitalnih potrdil upoštevali predvideno spremembo ZEPEP in uporabnikom njihovih storitev omogočili kreiranje kvalificiranega podpisa, bodo morali bodočim imetnikom kvalificiranih potrdil le-ta izdajati na napravah za varno tvorjenje podpisa, kar je lahko

navedeno tudi v samem digitalnem potrdilu. Nekateri izdajatelji kvalificiranih digitalnih potrdil že sedaj izdajajo tovrstna potrdila, drugi pa bodo morali svoje postopke prilagoditi, če bodo svojim uporabnikom želeli omogočiti uporabo storitev, kjer se zahteva najvišji nivo varnosti.

Prednosti:

- kratek rok za uvedbo
- ni potreb po večji prilagoditvi aplikacij

Slabosti:

- zaradi različnih profilov potrdil posameznih izdajateljev morajo ponudniki e-storitev prilagoditi svoje aplikacije posameznim profilom
- nadomestitev lokalno nameščene podpisne komponente s centralnim podpisnim strežnikom je skoraj neizvedljiva

Tveganja:

- počasnejši razvoj na področju e-identitet in zaostajanje za rešitvami, ki se uporabljajo v drugih državah EU

Priložnosti:

- možnost uvedbe enotnega profila potrdil v uredbi k ZEPEP

3.3. Zunanje pravno mnenje

Po mnenju Inštituta za ekonomijo, pravo in informatiko (dokument je v celoti v Prilogi A) bo pravna ureditev varnih e-identitet 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 nadaljevanju predstavljene tudi posledice posameznih možnosti na navedene deležnike.

3.3.1. Možnosti pravne in dejanske ureditve

Prva možnost, to je ureditev v ZOIzk, 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. Tehnično je možnih več izvedb, a njihove medsebojne razlike s pravnega stališča niso pomembne. 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.

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. Z razlikovanjem med varnim oz. naprednim elektronskim podpisom in kvalificiranim elektronskim podpisom se ohranja skladnost z Direktivo o e-podpisu, hkrati pa se tudi sledi potrebam po višjem nivoju podpisovanja. Takšnega višjega nivoja Direktiva o e-podpisu ne prepoveduje, posredno (preko uvajanja možnosti prostovoljne akreditacije) ga celo predvideva, pri tem pa (ob predpostavki, da se ohrani osnovni nivo 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. Zaradi širokih možnosti dejanske aplikacije kvalificiranih digitalnih potrdil (mogoče jih je uporabljati v kombinaciji s širokim spektrom naprav za tvorjenje varnega elektronskega podpisa) **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.

Z uvedbo akreditirane e-identitete bi overitelji 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 o e-podpisu, ki državam članicam dovoljuje, da uvedejo ali obdržijo prostovoljne akreditacijske sheme za zvišanje ravni overjanja. Institut je pri nas z zakonom sicer že predviden, za celovito ureditev tega področja pa manjka predvsem še določitev akreditacijskega organa in sprejetje pravilnika o pogojih za akreditacijo. 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. 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 o e-podpisu. 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 o e-podpisu, ki v 3. členu določa, da morajo biti vse zahteve v zvezi s temi shemami nepristranske, pregledne, sorazmerne in nediskriminatorne.

3.3.2. 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.

3.3.3. 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 pametnih 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.

3.3.4. 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.

4. E-IDENTITETE IN VARSTVO OSEBNIH PODATKOV

4.1. Uvod in izhodišča

Pri razvoju oziroma zasnovi uporabniku prijaznega sistema e-identitet, je treba posebno pozornost nameniti varovanju osebnih podatkov. Zakonodaja o varstvu osebnih podatkov se vprašanj e-identifikatorjev/e-identitet dotika iz več vidikov. Gre predvsem za vprašanja uporabe enoličnih identifikatorjev (enotnih povezovalnih znakov), zavarovanja osebnih podatkov (ang. *data security*) ter seveda upoštevanja ostalih temeljnih načel varstva osebnih podatkov. Različne možnosti pri oblikovanju sistema za upravljanje z identitetami, kot so lokacija hrambe podatkov, uporaba identifikatorjev in mehanizmov avtentikacije imajo pomemben vpliv na raven varstva osebnih podatkov. Varstvo osebnih podatkov poleg sistemskega zakona ureja področna zakonodaja, ki bolj ali manj uspešno sledi načeloma sistemskega zakona, nikjer pa ni izrecnih določb, ki bi dajale prednost določeni izvedbeni možnosti pred drugo. Vrednotenje posameznih izvedbenih možnosti tako lahko poteka le glede skladnosti s temeljnimi načeli varstva osebnih podatkov, pri tem pa je bistveno upoštevati koncept vgrajene zasebnosti (angl. *privacy by design*), kjer se o ustreznih varovalkah razmišlja že v samem oblikovanju rešitev. Pravočasna vgradnja zasebnosti lahko minimizira možnosti za pojav naknadne širitve namena uporabe (angl. *function creep*), kraj identitete in drugih zlorab.

V Sloveniji imamo iz zgodovinskih in drugih razlogov relativno veliko število enoličnih identifikatorjev, med najširše uporabljane pa sodijo EMŠO, davčna številka in številka zdravstvenega zavarovanja. Enotni povezovalni znaki oz. enolični identifikatorji terjajo posebno varstvo, saj omogočajo povezovanje zbirk osebnih podatkov – pogosto je takšen povezovalni podatek dovolj, da se o posamezniku pridobi veliko število drugih osebnih podatkov, zato je treba skrbeti, da do obdelave teh podatkov (npr. zbiranja, javne objave ipd.) ne pride, če to ni nujno potrebno.

Načelo sorazmernosti (obdelave osebnih podatkov) iz 3. člena Zakona o varstvu osebnih podatkov (ZVOP-1) zahteva, da morajo biti osebni podatki, ki se obdelujejo, ustrezni in po obsegu primerni glede na namene, za katere se zbirajo in nadalje obdelujejo. V konkretnem primeru to pomeni, da je treba zbrati samo toliko osebnih podatkov od uporabnika, s katerimi ta (že) izkaže svojo identiteto, te podatke pa naj spremlja samo toliko podatkov, kot je to nujno potrebno za delovanje aplikacij, ki zahtevajo predstavitev uporabnika z njegovo e-identiteto. Načelo sorazmernosti se udejanja na različne načine:

- anonimni podatki imajo prednost pred osebnimi podatki,
- če brez osebnih podatkov ne gre, imajo med osebnimi podatki prednost negovoreči podatki pred govorečimi, manj občutljivi pred bolj občutljivimi in z vidika možnih zlorab in posledic za posameznika manj tvegani pred bolj tveganimi (npr. davčna pred EMŠO, naključni niz-*hash* pred davčno[13]).

[13] Tveganje upošteva možnosti zlorab glede na uporabnost podatka (tudi) v drugih okoljih.

Več obdelav osebnih podatkov povečuje tveganja za zlorabe, zato je minimizacija obdelav podatkov rdeča nit številnih strokovnjakov na področju upravljanja z identitetami[14]. Minimizacijo obdelave osebnih podatkov, kot izpeljavo načela sorazmernosti obdelave osebnih podatkov, je treba upoštevati tudi pri odločitvi, koliko in kje se bodo osebni podatki, s katerimi se bo uporabnik predstavil, nahajali. Minimizacija se mora nanašati na vse procese, pri katerih prihaja do določenih faz obdelave osebnih podatkov – zbiranje, agregiranje, hramba, kopiranje, posredovanje in povezovanje.

V pričujoči analizi je navedena tudi ugotovitev 8. srečanja foruma »Governement Discussion Forum on Electronic Identity Management« (več o tem v razd. 2.7), da se pri uvajanju e-identitet kaže **jasen trend njihove uporabe zgolj kot enoličnega identifikatorja osebe in ne kot nosilca aplikacij in širokega nabora osebnih podatkov**. Navedeno pomeni, da e-identiteta dejansko opravlja funkcijo osebne izkaznice, ki sama po sebi še ne daje nobenih pravic oziroma nalaga obveznosti, pač pa se z njo in uporabnikovo prisotnostjo lahko izpelje postopek identifikacije in avtentikacije. Šele od tu naprej pa je mogoča avtorizacija za uporabo storitev e-uprave oziroma sklepanje pravnih poslov.

4.2. E-identitete kot priložnost za višjo raven varstva osebnih podatkov

S pomanjkanjem uporabnikom prijaznih obenem pa varnih e-identitet se na področju varstva osebnih podatkov večkrat srečujemo. Težave z izkazovanjem in preverjanjem starosti pri uporabi storitev na internetu, kot so npr. spletna družbena omrežja, težave z dokazovanjem po spletu podane privolitve v obdelavo osebnih podatkov, varnost obstoječih e-identifikatorjev in pogosto nesorazmerno velik tok podatkov, ki je potreben za izkazovanje in preverjanje identitete posameznika, so le nekatere od teh težav. Ob predpostavki, da ima država pred zasebnim sektorjem določene primerjalne prednosti, je treba iskati priložnosti za večjo uporabnost e-identitete na tistih področjih, kjer zasebni sektor ne more ponuditi varnih in uporabnih rešitev. Primerjalne prednosti države tu vidimo predvsem v številnih zbirkah osebnih podatkov, ki jih vodi javni sektor, v izhodišču analiz pa mora primarno gonilo predstavljati dodana vrednost za uporabnika. Učinkovitejši dostop do teh zbirk mora primarno zagotoviti država in ena od zanimivih priložnosti se kaže v elektronski podpori pravici posameznika do seznanitve z lastnimi osebnimi podatki (30. čl. ZVOP-1) na podlagi varne in uporabniku prijazne e-identitete. Trenutno je le nekaj takšnih delujočih storitev, kjer se lahko posameznik elektronsko avtenticira državnemu organu, izvrši v vpogled v lastne osebne podatke[15] ali celo pridobi elektronsko podpisan dokument, ki ga od njega zahteva tretja oseba, kot so razna dokazila, potrdila, izpisi in podobno, pri čemer bi takšen način lahko postal gonilo razvoja tudi čezmejnih e-storitev.

Zaradi pravnih težav pri povezovanju organov iz različnih držav je bil v projektu STORK ravno ta koncept izbran kot priporočljiv, saj minimizira pravne težave in obenem nudi posamezniku nadzor

[14] Glej npr. Cameron: The Laws of Identity, rezultate projekta FIDIS-Future of Identity in the Information Society (npr. 16.2 http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables3/2009_04_16_D16.1_Framework_IDM_in_eGov_Final_2__1_.pdf) in Cameron, Posch, Ranenberg: Proposal for a Common Identity Framework: A User-Centric Identity Metasystem (http://www.identityblog.com/wp-content/images/2009/06/UserCentricIdentityMetasystem.pdf).

[15] Primer takšne storitev je VLOP – vpogled v lastne osebne podatke v Centralnem registru prebivalstva (http://ecrp.gov.si/) in eKartica, s katero lahko davčni zavezanec vpogleda v stanje davčnih obveznosti (http://edavki.durs.si).

nad povezovanjem in posredovanjem svojih osebnih podatkov med upravljavci podatkov ter uporabniki.

Uvajanje uporabnikom prijaznih in varnih e-identitet zato tudi z varstva osebnih podatkov nudi priložnosti za izboljšanje stanja. Izboljšanje stanja tako vidimo v naslednjih priložnostih:

- izboljšano varstvo enoličnih identifikatorjev (npr. umik davčne številke iz digitalnih potrdil)[16]
- minimizacija hrambe enoličnih identifikatorjev na enem mediju in obdelav enoličnih identifikatorjev,
- minimizacija tokov osebnih podatkov med posameznikom, upravljavci zbirk osebnih podatkov in uporabniki zbirk osebnih podatkov (npr. sistem »je zadetek/ni zadetka« pri storitvah, kjer je dovolj preveriti le določen podatek o posamezniku, npr. ali je polnoleten ali ne),
- izboljšana varnost e-identifikatorjev,
- širša uporabnost e-identifikatorjev:
    - možnost elektronske podpore pravici posameznika do seznanitve z lastnimi osebnimi podatki in pridobivanja elektronsko podpisanih dokumentov, kot so potrdila, dokazila, izpisi iz evidenc ipd.,
    - možnost opravljanja čezmejnih e-storitev (koncept STORK).

S tega vidika je treba dati **prednost tistim izvedbenim rešitvam**, ki:

- imajo prednost na področju prijaznosti do uporabnikov in enostavnosti uporabe (npr. izvedbene možnosti z mobilnimi telefoni v primerjavi z digitalnimi potrdili v brskalnikih),
- pri vsebini digitalnih potrdil ne zahtevajo enoličnih identifikatorjev,
- omogočajo večjo varnost e-identifikatorjev (npr. naprave za varno tvorjenje podpisa proti hrambi digitalnih potrdil v brskalniku),
- omogočajo minimizacijo in nadzor uporabnika nad tokovi svojih osebnih podatkov (npr. pri konceptih ponudnikov identitet in z izkoriščanjem pravice posameznika do seznanitve z lastnimi osebnimi podatki, kjer posameznik od upravljavca svojih podatkov zahteva želeni nabor podatkov, te pa nato posreduje uporabniku podatkov, s čimer ohranja nadzor na svojimi podatki).

4.3. Modeli urejanja e-identitet

V nadaljevanju so predstavljeni možni modeli urejanja e-identitet z vidika varovanja osebnih podatkov. Prva dva modela sta trenutno v uporabi v Sloveniji, peti pa v Avstriji.

[16] Na tem mestu je primerno opozoriti na izkušnje bank pri zniževanju tveganja bančnih prevar. Kot je bilo že navedeno lahko posameznik, natančneje prinosnik ne pa (zakoniti) imetnik, bančno kartico uporabi, če pozna njeno geslo. Kot ugotavlja npr. B. Schneier (glej spodaj) ima avtentikacija z osebnimi podatki omejeno vrednost. Osebni podatki imajo svojo vrednost, lahko jih je odtujiti, ko so odtujeni jim vrednost ne pade – tako omogočajo nadaljnje zlorabe, kraja identitete je npr. najbolj značilen primer. Banke so tako svojo pozornost namenile predvsem avtentikaciji transakcij in ne avtentikaciji posameznikov (z osebnimi podatki). Ko podatki nimajo več svoje vrednosti, kot jo imajo osebni podatki, se nevarnost zmanjša oziroma omeji na naključne opazovalce, ni pa več zanimiva za prevarante. B. Schneier v članku »Does Secrecy help protect personal information?«, v Information Security, januar 2007, dosegljiv tukaj: http://www.schneier.com/essay-168.html.

4.3.1. Obstoječi identifikator v digitalnem potrdilu

Kot osebni identifikator se uporablja obstoječ uradni identifikator osebe npr. EMŠO ali davčna številka. Identifikator je vključen v digitalno potrdilo, zato je identiteta uporabnika neposredno razvidna iz samega potrdila. Dodatni sistemi za dostop do identifikatorja tako niso potrebni, a je identifikator viden povsod, kjer se pojavlja digitalno potrdilo (v digitalno podpisanih dokumentih, imeniku digitalnih potrdil…), kar je še bolj moteče, ker gre za obstoječi identifikator, ki izhaja iz določene domene (npr. matične zadeve, davčni postopki). Poleg tega model dopušča povezovanje identitete uporabnika med e-storitvami različnih sektorjev (matične zadeve, davčni postopki, socialno zavarovanje…). Model uporablja večina overiteljev kvalificiranih digitalnih potrdil v Sloveniji (HALCOM-CA, AC NLB in POŠTA®CA).

4.3.2. Obstoječi identifikator v zalednem sistemu overitelja

Kot osebni identifikator se uporablja obstoječ uradni identifikator osebe npr. EMŠO ali davčna številka. Identifikator ni vključen v digitalno potrdilo, zato identiteta uporabnika ni razvidna iz samega potrdila, temveč je potreben dodatni sistem za dostop do identifikatorja. Na ta način identifikator ni dostopen preko imenika potrdila in vsebovan v digitalno podpisanih dokumentih. Slaba stran modela je, da uporablja obstoječi identifikator, ki izhaja iz določene domene in da dopušča povezovanje identitete uporabnika med e-storitvami različnih sektorjev. V Sloveniji model uporablja Overitelj na MPJU.

4.3.3. E-identifikator osebe v digitalnem potrdilu

Kot osebni identifikator se uporablja namenski identifikator osebe za e-poslovanje, ki je bodisi izračunan iz obstoječega identifikatorja (npr. EMŠO ali davčne številke) bodisi kot posebni identifikator uveden v uradno evidenco (npr. v Centralni register prebivalstva, v nadaljevanju *CRP*). Za upravljanje z e-identifikatorji je zadolžen državni organ (npr. MNZ, IP…). Identifikator je vključen v digitalno potrdilo, zato je identiteta uporabnika neposredno razvidna iz samega potrdila. Dodatni sistemi za dostop do identifikatorja tako niso potrebni, a je identifikator viden povsod, kjer se pojavlja digitalno potrdilo (v digitalno podpisanih dokumentih, imeniku digitalnih potrdil itd.). Prednost modela je v tem, da se za e-poslovanje uporablja namenski identifikator, iz katerega obstoječi uradni identifikatorji osebe niso neposredno razvidni. Še vedno pa model dopušča povezovanje identitete uporabnika med e-storitvami različnih sektorjev, saj se povsod uporablja isti identifikator. Uvedba modela je v skladu z obstoječim ZEPEP, ki v 28. členu govori o osebni identifikacijski oznaki in njeni povezavi s CRP.

4.3.4. E-identifikator osebe v zalednem sistemu overitelja

Kot osebni identifikator se uporablja namenski identifikator osebe za e-poslovanje, ki je bodisi izračunan iz obstoječega identifikatorja (npr. EMŠO ali davčne številke) bodisi kot posebni identifikator uveden v uradno evidenco (npr. CRP). Za upravljanje z e-identifikatorji je zadolžen državni organ (npr. MNZ, IP…). Identifikator ni vključen v digitalno potrdilo, zato identiteta uporabnika ni razvidna iz samega potrdila, temveč je potreben dodatni sistem za dostop do identifikatorja. Na ta način identifikator ni dostopen preko imenika potrdila in ni vsebovan v digitalno podpisanih dokumentih. Slaba stran modela je, da dopušča povezovanje identitete uporabnika med

e-storitvami različnih sektorjev, saj se povsod uporablja isti identifikator. Uvedba modela je v skladu z obstoječim ZEPEP, ki v 28. členu govori o osebni identifikacijski oznaki in njeni povezavi s CRP.

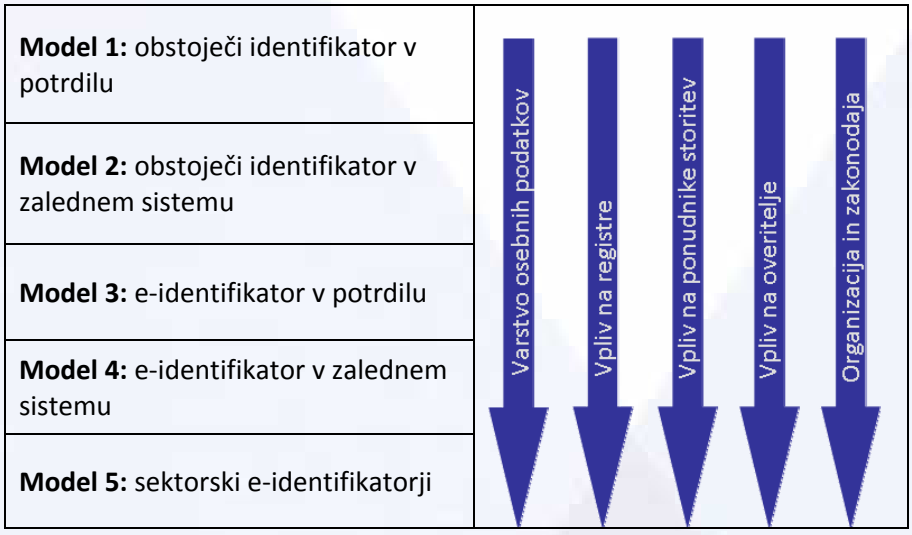
4.3.5. Sektorski e-identifikatorji osebe

Kot osebni identifikator se uporablja namenski identifikator osebe za e-poslovanje, ki je bodisi izračunan iz obstoječega identifikatorja (npr. EMŠO ali davčne številke) bodisi kot posebni identifikator uveden v uradno evidenco (npr. CRP). Za upravljanje z e-identifikatorji je zadolžen državni organ (npr. MNZ, IP…). Identifikator ni vključen v digitalno potrdilo, zato identiteta uporabnika ni razvidna iz samega potrdila, temveč je potreben dodatni sistem za dostop do identifikatorja, ki za vsako e-storitev na podlagi e-identifikatorja osebe in oznake sektorja izračuna t.i. sektorski identifikator. Le-ta se uporablja le v storitvah znotraj določenega sektorja (matične zadeve, davčni postopki, socialno zavarovanje…), ki zaradi svoje narave potrebujejo povezovanje identitete uporabnika. Poleg tega, da v tem modelu identifikator ni dostopen preko imenika potrdila in ni vsebovan v digitalno podpisanih dokumentih, model tudi učinkovito onemogoča povezovanje identitete uporabnika med e-storitvami različnih sektorjev, saj se isti (sektorski) identifikator uporablja le znotraj posameznega sektorja. Model se uporablja v Avstriji.

Zgoraj predstavljene modele lahko medsebojno primerjamo z različnih vidikov, najpomembnejši med njimi so:

- nivo varstva osebnih podatkov,
- vpliv na uradne evidence in registre,
- vpliv na ponudnike storitev (v javni upravi in zasebnem sektorju),
- vpliv na overitelje digitalnih potrdil,
- potrebne organizacijske in zakonodajne spremembe.

Medsebojno primerjavo predstavljenih modelov v smislu naraščanja teže oz. vpliva za omenjenih pet vidikov prikazuje spodnja slika. Model 5 je tako najboljši s stališča varstva osebnih podatkov, bi pa njegova uvedba zahtevala največ prilagoditev s strani overiteljev in ponudnikov e-storitev. Ta model bi povzročil tudi največ sprememb na uradnih registrih ter zahteval tudi največ organizacijskih in zakonodajnih ukrepov.



Slika 1: Medsebojna primerjava predstavljenih modelov e-identitet

5. NAPRAVE ZA VARNO TVORJENJE PODPISA

Naprave za varno tvorjenje podpisa so nosilci digitalnih potrdil, ki imajo svoj mikroprocesor in pomnilnik. Na njih so shranjena digitalna potrdila z zasebnim in javnim ključem. **Zasebnega ključa iz naprave za varno tvorjenje podpisa ni mogoče nikoli izvoziti oz. narediti njegove kopije**. Zasebni ključ naprave za varno tvorjenje podpisa ne zapusti niti ko podpisujemo ali dešifriramo podatke, saj šifriranje in digitalno podpisovanje potekata v mikroprocesorju na napravi za varno tvorjenje podpisa. Dostop do zasebnega ključa na napravi za varno tvorjenje podpisa je ustrezno zaščiten (običajno z geslom), kar nepooblaščenim osebam preprečuje dostop do zasebnega ključa, uporabniku pa omogoča le njegovo uporabo in ne njegovega spreminjanja.

Prvotno so bile naprave za varno tvorjenje podpisa le v obliki pametnih kartic, vendar so se zaradi večje funkcionalnosti, praktičnosti in različnih namenov uporabe njihove oblike spreminjale, tako da lahko danes izbiramo med različnimi napravami za varno tvorjenje podpisa.

	Pametna kartica z brezkontaktnim čipom	Pametna kartica s kontaktnim čipom	Pametni ključek	Centralni HSM in močna avtentikacija	Uporaba mobilnih telefonov
					
e-Osebna izkaznica	✓	✓		✓	
Akreditirana e-identiteta	✓	✓	✓	✓	✓
Kvalificirana digitalna potrdila na varnem mediju	✓	✓	✓	✓	✓

Slika 2: Tehnične izvedbe e-identifikatorjev

5.1. Izvedbene možnosti

5.1.1. Pametna kartica

Pametna kartica s kontaktnim čipom

Čip, na katerem je shranjeno digitalno potrdilo, je lahko vgrajen v plastično kartico standardnega formata, kot je osebna izkaznica, bančna kartica, vozniško dovoljenje… Kartico imenujemo pametna, če poleg hranjenja podatkov zagotavlja še varnostne mehanizme in je narejena v skladu s standardi, veljavnimi na tem področju. Poglavitna naloga pametnih kartic je, poleg hranjenja in varovanja podatkov ter zagotavljanja zadovoljive identifikacije, še izvajanje varnih transakcij. Za dostop do podatkov na pametni kartici je potreben čitalnik pametnih kartic, ki je lahko samostojna naprava povezana v računalnik preko vhoda USB, v obliki, namenjeni za vstavitev v ustrezno režo (običajno pri prenosnikih), ali pa je čitalnik že integriran v računalnik.

Prednosti:

- možna uporaba čitalnika z integrirano tipkovnico
- enostavna uporaba
- tehnologija je dobro poznana, obvladljiva in se uporablja

Slabosti:

- zunanji čitalnik

Pametna kartica z brezkontaktnim čipom

Pametne kartice so lahko brezkontaktne, tako da je dostop do podatkov na čipu mogoč tudi brez vstavljanja kartice v čitalnik, saj zadostuje že, če kartico dovolj približamo čitalniku. Brezkontaktne kartice omogočajo branje podatkov iz čipa in izvajanje varnih transakcij na razdalji največ 5 cm. Poleg tega obstajajo različne dodatne zaščite (npr. BAC – Basic Access Control in EAC – Extended Access Control pri e-potnih listih), ki dodatno preprečujejo nepooblaščeni dostop do podatkov na brezkontaktnem čipu. Za razliko od kartic s kontaktnim čipom, kjer je na voljo veliko različnih čitalnikov kartic, je področje čitalnikov brezkontaktnih čipov bistveno manj razvito in so zato manj primerni za zasebno uporabo.

Prednosti:

- sorodna rešitev se uporablja pri biometričnih potnih listinah in dovoljenjih za prebivanje tujcev
- rešitev že uporabljena pri eOI v Nemčiji, nekaj drugih držav o tem razmišlja

Slabosti:

- slaba prenosljivost, malo delovnih postaj in naprav je opremljenih z brezkontaktnimi čitalniki
- možna uporaba čitalnika z integrirano tipkovnico
- zahtevna vzpostavitev sistema
- sorazmerno visoka cena čitalnika

Tveganja:

- zrelost izbrane tehnologije
- izguba uporabnikov zaradi uvedbe nove tehnologije (nezaupanje uporabnikov)
- malo izkušenj s to tehnologijo

Priložnosti:

- integracija biometričnih elementov (podobno kot pri BPL)

- izbira smiselna verjetno le v povezavi z eOI
- uporaba za dodatne namene (nadzor dostopa, registracija delovnega časa,…)
- tehnologija prihodnosti (vedno širša uporaba brezkontaktnega čipa, pametni telefoni kot čitalniki,…)

Pametna kartica s čipom z dvojnim dostopom (kontaktni in brezkontaktni)

Pametne kartice so lahko izvedene tako, da je dostop do podatkov na enem samem čipu omogočen tako na kontakten kot na brezkontakten način. Za uporabo kartice se lahko glede na način dostopa, kontakten in brezkontakten, uporabljata oba tipa čitalnikov. Brezkontaktno branje podatkov je možno le na manjših razdaljah (do 5 cm), na voljo pa so tudi dodatni varnostni mehanizmi za preprečevanje nepooblaščenega dostopa.

Prednosti:

- sorodna rešitev se uporablja pri biometričnih potnih listinah in dovoljenjih za prebivanje tujcev (brezkontaktni čip)
- možna uporaba čitalnika z integrirano tipkovnico
- možna uporaba kontaktnega in brezkontaktnega čitalnika
- enostavna uporaba

Slabosti:

- zahtevna vzpostavitev sistema

Tveganja:

- zrelost izbrane tehnologije
- izguba uporabnikov zaradi uvedbe nove tehnologije (nezaupanje uporabnikov)
- malo izkušenj s to tehnologijo

Priložnosti:

- integracija biometričnih elementov (podobno kot pri BPL)
- izbira smiselna verjetno le v povezavi z eOI
- uporaba za dodatne namene (nadzor dostopa, registracija delovnega časa,…)
- tehnologija prihodnosti (vedno širša uporaba brezkontaktnega čipa, pametni telefoni kot čitalniki,…)

Pametna kartica z brezkontaktnim in kontaktnim čipom

Pametne kartice so lahko kombinirane, tako da sta na kartici dva čipa, kontakten in brezkontakten. Za uporabo kartice se lahko glede na način dostopa, kontakten in brezkontakten, uporabljata oba tipa čitalnikov. Brezkontaktno branje podatkov je možno le na manjših razdaljah (do 5 cm), na voljo pa so tudi dodatni varnostni mehanizmi za preprečevanje nepooblaščenega dostopa. Bistvena razlika v primerjavi s pametnimi karticami z dvojnim dostopom je v tem, da so pri tem vsi podatki zapisani le na enem čipu, medtem ko so pri karticah z dvema čipoma shranjeni na dveh čipih in zato načeloma medsebojno različni; do katerih podatkov dejansko pridemo, je torej odvisno od uporabljenega čitalnika.

Prednosti:

- sorodna rešitev se uporablja pri biometričnih potnih listinah in dovoljenjih za prebivanje tujcev (brezkontaktni čip)
- možna uporaba čitalnika z integrirano tipkovnico
- možna uporaba kontaktnega in brezkontaktnega čitalnika
- enostavna uporaba
- možnost omejitve dostopa do podatkov glede na uporabljen tip čitalnika

Slabosti:

- zahtevna vzpostavitev sistema
- podatki shranjeni ločeno na dveh čipih

Tveganja:

- zrelost izbrane tehnologije
- izguba uporabnikov zaradi uvedbe nove tehnologije (nezaupanje uporabnikov)
- malo izkušenj s to tehnologijo

Priložnosti:

- integracija biometričnih elementov (podobno kot pri BPL)
- izbira smiselna verjetno le v povezavi z eOI
- uporaba za dodatne namene (nadzor dostopa, registracija delovnega časa,…)
- tehnologija prihodnosti (vedno širša uporaba brezkontaktnega čipa, pametni telefoni kot čitalniki,…)

5.1.2. Pametni ključek

Kombinacijo pametne kartice in čitalnika predstavlja pametni USB ključ, ki vsebuje enak čip kot pametna kartica ter je sam po sebi čitalnik.

Prednosti:

- enostavna uporaba
- sorazmerno enostavna uvedba
- ni potreben zunanji čitalnik
- sorazmerno enostavna prenosljivost
- sorazmerno nizka cena
- tehnologija je dobro poznana, obvladljiva in se uporablja

Slabosti:

- ni možno uporabiti čitalnika z integrirano tipkovnico

Tveganja:

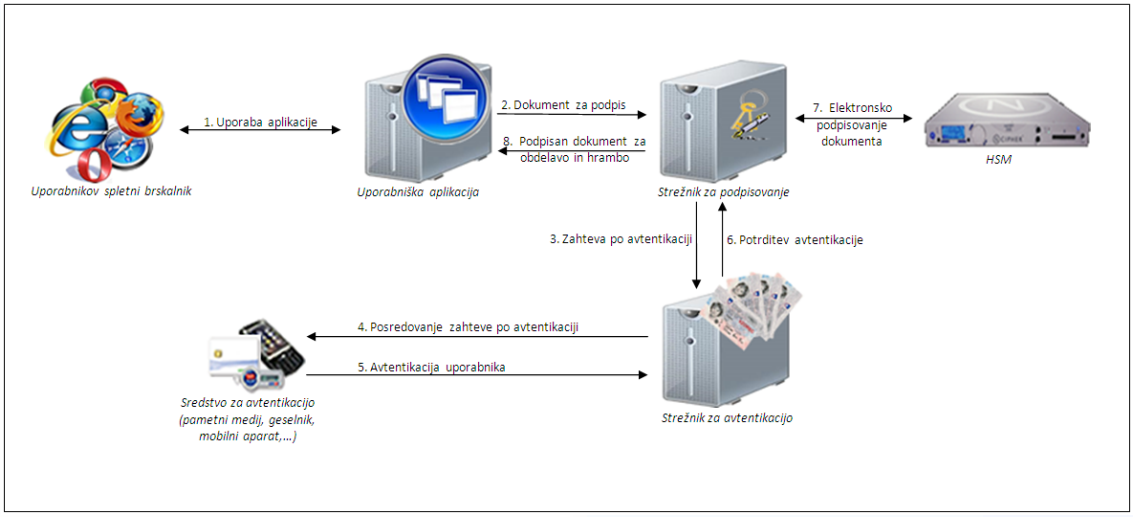
- oblika pametnega medija (odnos do pametnega USB ključka)

5.1.3. Centralni HSM z močno avtentikacijo

Centralni HSM (angl. *Hardware Security Module*) oz. strojni varnostni modul je namenska kriptografska naprava, nameščena v varovanem okolju overitelja oz. od njega pooblaščenega upravljavca HSM, na kateri se generira in je shranjeno digitalno potrdilo oz. zasebni ključ za podpisovanje. Dostop do zasebnega ključa je strogo nadzorovan s pomočjo tehničnih in organizacijskih rešitev, ki imetniku takega potrdila zagotavljajo, da ima edini možnost dostopa do ključa in s tem možnost njegove uporabe. Običajno je to izvedeno na način, da je zasebni ključ v strojnem varnostnem modulu shranjen v šifrirani obliki, geslo za dostop pa je sestavljeno iz gesla modula ter gesla uporabnika. Za dešifriranje ključa oz. njegovo uporabo je potrebna avtentikacija uporabnika na ustrezen, dovolj varen način, za kar se lahko uporabljajo pametna kartica oz. pametni USB ključ z digitalnim potrdilom za avtentikacijo, geselnik OTP, mobilni aparat ipd.

Postopek izdaje digitalnega potrdila pri prijavni službi overitelja je sicer nekoliko odvisen od izbranega načina uporabnikove avtentikacije, v vseh primerih pa gre dejansko za registracijo uporabnika, pri kateri se uporabnikovo sredstvo za avtentikacijo poveže z njegovim digitalnim potrdilom za podpisovanje, ki se istočasno generira v strojnem varnostnem modulu.

Čeprav je model zanimiv in v zadnjem času dokaj pogosto uporabljen, je njegova glavna pomanjkljivost oz. pomislek pri njegovi uporabi vprašanje, ali dejansko omogoča izdelavo elektronskega podpisa, ki bi bil enakovreden lastnoročnemu (naprava za elektronsko podpisovanje mora biti izključno pod nadzorom imetnika potrdila)



Slika 3: Elektronsko podpisovanje s centralnim HSM

Prednosti:

- prilagoditev aplikacij e-uprave je lahko postopna (v primeru, da je avtentikacijsko sredstvo pametni medij)
- namestitev medprogramja ni nujno potrebna (odvisno od izbranega avtentikacijskega sredstva)
- enostavna uporaba
- sorazmerno enostavna prenosljivost
- sorazmerno velika neodvisnost od uporabnikove opreme
- sorazmerno nizka cena za uporabnika

Slabosti:

- velika odgovornost overitelja oz. upravljavca HSM (zagotavljanje delovanja sistema 24/7, strogi varnostni mehanizmi)
- sorazmerno visoki stroški uvedbe
- daljši rok za uvedbo
- zahtevna vzpostavitev (ustrezni varnostni mehanizmi)

Tveganja:

- primernost izbrane tehnologije (ali omogoča tvorjenje kvalificiranega podpisa)
- podpora s strani ponudnikov storitev
- zaupanje uporabnikov
- izpadi delovanja zaradi kompleksnost sistema
- potrebna integracija v centralni avtentikacijski sistem

Priložnosti:

- možnost nadomestitve lokalno nameščene podpisne komponente s centralnim podpisnim strežnikom

---

5.1.4. Uporaba mobilnih telefonov

V več raziskavah, poročilih in priporočilih se v naslednjih letih predvideva skokovit porast uporabe mobilnih naprav tudi za potrebe avtentikacije oz. digitalnega podpisovanja uporabnikov. Z razvojem mobilnih aparatov in povečevanjem njihovih zmogljivosti lahko ti v določeni meri že opravljajo funkcijo skromnejšega osebnega računalnika, zato vedno več mobilnih naprav podpira tudi uporabo digitalnih potrdil neposredno tudi preko interne shrambe potrdil in vgrajenega spletnega brskalnika. Ker tovrstne rešitve po eni strani niso specifične za mobilne aparate, po drugi strani pa so omejene na lastnike zmogljivejših mobilnih aparatov, jih v pričujoči analizi nismo vključili, temveč smo predstavili dva modela, ki omogočata digitalno podpisovanje tudi na osnovnih modelih mobilnih aparatov, saj za uporabo digitalnih potrdil zadošča podpora za sporočila SMS, kar danes omogoča domala vsak mobilni aparat.

Druga skupna značilnost obeh v nadaljevanju predstavljenih modelov je ta, da zahtevata spremembo v načinu podpisovanja oz. avtentikacije uporabnika na strani e-storitve, saj digitalno potrdilo ni (neposredno ali posredno) dostopno preko shrambe potrdil brskalnika, kar je značilnost vseh klasičnih modelov e-podpisovanja, temveč mora aplikacija izrecno podpirati tudi možnost avtentikacije oz. podpisovanja s pomočjo mobilnega telefona.

Model WPKI

WPKI (angl. *Wireless Public Key Infrastructure*) je oznaka za brezžično infrastrukturo javnih ključev, pri kateri so digitalna potrdila oz. zasebni ključi shranjeni na SIM kartici mobilnega telefona. Ker kartica dejansko deluje kot naprava za varno tvorjenje podpisa in se na njej izvajajo kriptografske operacije, standardne SIM kartice tega ne podpirajo, zato mora bodoči imetnik potrdila pred pričetkom uporabe od svojega mobilnega operaterja pridobiti ustrezno SIM kartico. V tem modelu je torej ključnega pomena usklajeno in z ustrezno pogodbo urejeno sodelovanje overitelja, ki upravlja z digitalnimi potrdili, in mobilnega operaterja, ki zagotavlja SIM kartico in infrastrukturo, potrebno za mobilno podpisovanje (interni imenik mobilnih digitalnih potrdil, sistem za aktiviranje digitalnih potrdil, sistem za elektronsko podpisovanje). Model WPKI se v praksi uporablja že nekaj let, vzpostavljenega ga imajo tudi v nekaterih državah EU.

V Sloveniji storitve infrastrukture WPKI trenutno ponuja le operater Mobitel (zaenkrat le v dogovoru z overiteljem Halcom CA), ki naj bi načeloma uporabo svojega sistema omogočal tudi za druge operaterje, vendar pa bi ti morali svojim uporabnikom omogočiti zamenjavo SIM kartic s t.i. pametnimi SIM karticami ter svoje sisteme povezati s sistemom operaterja Mobitel.

V rešitvi, ki jo ponuja Mobitel, uporabnik poseduje dve digitalni potrdili: za elektronsko podpisovanje in za avtentikacijo. Pripadajoča zasebna ključa sta shranjena na kartici SIM, ki jo uporablja imetnik digitalnega potrdila, sami potrdili, katerih sestavna dela sta javni ključ za overjanje oz. avtentikacijo,

pa sta shranjeni v internem imeniku operaterja, ki ni javno dostopen in je namenjen zgolj za uporabo potrdil pri digitalnem podpisovanju in avtentikaciji uporabnika.

Prednosti

- uporaba centralnega podpisnega strežnika namesto lokalno nameščene podpisne komponente
- ni potrebna namestitev medprogramja
- promocija s strani mobilnega operaterja
- neodvisnost od zmogljivosti uporabnikovega mobilnega aparata
- rešitev že uporabljena v nekaterih državah (Baltske države, Slovaška, Finska)
- enostavna uporaba
- prenosljivost
- za uporabnika cenovno ugodna pridobitev potrdila

Slabosti

- podpora le za ključe dolžine 1K (naknadna menjava kartic SIM zaradi uvedbe ključev dolžine 2K, krajši rok veljavnost potrdil zaradi 1K ključev)…
- uporaba namenskih kartic SIM
- rešitev trenutno omogoča le Mobitel, oteženo vključevanje ostalih operaterjev
- potrebna prilagoditev aplikacij
- menjava zaradi izgube/kraje telefona
- plačljiva uporaba (podpisovanje, avtentikacija)

Tveganja

- pogodbeno razmerje z operaterji
- podpora s strani ponudnikov storitev
- potrebna integracija v centralni avtentikacijski sistem

Priložnosti

- razširjena uporaba mobilnih aparatov
- dodatne funkcionalnosti mobilnih aparatov (pametni telefoni)
- dogovor z operaterjem glede zaračunavanja storitev e-uprave
- možnost vzpostavitve prijavne službe pri mobilnem operaterju

Model s centralnim HSM

Predstavljeni model je različica zgoraj opisane rešitve centralnega HSM z močno avtentikacijo, pri katerem se kot sredstvo za avtentikacijo imetnika potrdila uporablja njegov mobilni aparat, digitalno potrdilo in uporabnikovi zasebni ključi pa so shranjeni na strojnem varnostnem modulu, s katerim

upravlja overitelj oz. ponudnik storitve e-podpisovanja in ki predstavlja sredstvo za varno elektronsko podpisovanje.

Bodoči imetnik potrdila mora ob oddaji zahtevka za pridobitev pri prijavni službi overitelja registrirati svoj mobilni aparat oz. mobilno telefonsko številko (dokazati, da ima pravico in možnost njene uporabe), nakar overitelj generira uporabnikovo digitalno potrdilo, zasebni ključ pa v šifrirani obliki shrani v strojnem varnostnem modulu. Ob vsaki zahtevi za digitalno podpisovanje mora uporabnik oblikovanje podpisa omogočiti preko svojega mobilnega aparata, obenem pa potrditi še z vnosom gesla preko spletnega brskalnika.

Kljub nekaterim svojim omejitvam (npr. spremenjen način avtentikacije oz. podpisovanja, pomisleki glede ustreznosti hranjenja zasebnih ključev), so model pred dvema letoma uspešno vzpostavili v Avstriji, kjer se je njegova uporaba že dokaj razširila, o njegovi vzpostavitvi pa razmišljajo tudi v Romuniji, Moldaviji in na Švedskem.

Prednosti

- uporaba centralnega podpisnega strežnika namesto lokalno nameščene podpisne komponente
- ni potrebna namestitev medprogramja
- neodvisnost od operaterjev
- neodvisnost od zmogljivosti uporabnikovega mobilnega aparata
- rešitev že uporabljena v Avstriji
- enostavna uporaba
- prenosljivost
- za uporabnika cenovno ugodna pridobitev potrdila
- ni nujno potrebne menjave pri izgubi telefona

Slabosti

- velika odgovornost overitelja oz. upravljavca HSM (zagotavljanje delovanja sistema 24/7, strogi varnostni mehanizmi)
- sorazmerno visoki stroški uvedbe
- daljši rok za uvedbo
- zahtevna vzpostavitev (ustrezni varnostni mehanizmi)
- potrebna prilagoditev aplikacij
- plačljiva uporaba (podpisovanje, avtentikacija)

Tveganja

- primernost izbrane tehnologije (ali omogoča tvorjenje kvalificiranega podpisa)
- podpora s strani ponudnikov storitev
- zaupanje uporabnikov
- izpadi delovanja zaradi kompleksnost sistema
- potrebna integracija v centralni avtentikacijski sistem

- samostojen razvoj sistema oz. nakup pri tujem ponudniku

Priložnosti

- razširjena uporaba mobilnih aparatov
- dodatne funkcionalnosti mobilnih aparatov (pametni telefoni)

5.2. Zunanje pravno mnenje o ustreznosti modelov s centralnim HSM

V pravnem mnenju Inštituta za ekonomijo, pravo in informatiko (celotni dokument je v Prilogi B) so predstavljeni pomembnejši pravni vidiki sistema e-identitet, ki se nanašajo na rešitev, pri kateri bi se vsi zasebni ključi podpisnikov hranili skupaj na namenski napravi - na strojnem varnostnem modulu, in na skladnost te rešitve z obstoječo evropsko in domačo zakonodajo. Za uvajanje tega sistema so relevantne zahteve zakonodaje glede varnega elektronskega podpisa in zahteve glede sredstev, ki se uporabljajo za varno elektronsko podpisovanje. Pravno mnenje se sklicuje na Direktivo o e-podpisu, ki v 2. členu opredeljuje napreden elektronski podpis, ter na ZEPEP, ki v direktivi imenovan napreden elektronski podpis imenuje varen elektronski podpis in ga podrobneje opredeljuje.

5.2.1. Zahteve za varen elektronski podpis

Pri hrambi zasebnih ključev na strojnem varnostnem modulu izpolnjevanje večine zahtev za varen elektronski podpis ni problematično, dvom pa se pojavi glede izpolnjevanja zahteve po izključnem podpisnikovem nadzoru sredstev za podpisovanje, saj podpisnik pri takšni rešitvi nima neposrednega dostopa do modula, na katerem je shranjen njegov zasebni ključ, hkrati pa imajo takšen dostop tretje osebe. Namen zahteve po izključnem podpisnikovem nadzoru (angl. *sole control*) je podpisniku zagotavljati možnost, da zaščiti svoje podatke za ustvarjanje elektronskega podpisa pred nepooblaščenim dostopom na takšen način, da lahko izdelavo elektronskega podpisa sproži (oziroma odredi) le on. Uporabljena dikcija je splošna in pomensko široka, saj govori le o nadzoru, ne pa na primer o neposrednem fizičnem nadzoru. Splošnost ubeseditve direktive je tudi skladna z načelom, da morajo biti zakoni pisani tehnološko nevtralno, s čimer se prepreči nesorazmerno omejevanje načina njihovega izvajanja. Odsotnost izrecne omembe strojnega varnostnega modula torej sama po sebi ne pomeni njegovo neskladnost z direktivo in ZEPEP, temveč pomeni le določeno mero izvedbene svobode, ki omogoča neomejeno število rešitev, skladnih s postavljenimi pogoji.

Pravno mnenje se sklicuje tudi na Forum evropskih nadzornih organov za elektronske podpise (FESA, angl. *Forum of European Supervisory Authorities for Electronic Signatures*), ki je v delovnem dokumentu o naprednih elektronskih podpisih (angl. *Working paper on advanced electronic signatures*) zapisal, da zahteva po izključnem nadzoru ne pomeni obvezne uporabe posebnih strojnih naprav za izdelovanje podpisov (s čimer so mišljeni na primer USB ključi ali pametne kartice), pomeni pa obvezno uporabo varnostnih ukrepov s strani podpisnika, s katerimi obdrži nadzor nad svojim ključem. FESA v Javni izjavi o strežniško osnovanih storitvah podpisovanja tudi poudarja, da morata varnostna zasnova in sistemska konfiguracija strežnika zagotavljati, da ima le podpisnik nadzor nad

podatki za izdelavo podpisa. Za razumevanje takšne interpretacije kriterija izključnega nadzora FESA dalje navaja, da v primeru avtomatske izdelave varnega elektronskega podpisa, ki bi ga izdelal podpisnikov strežnik, podpisnik pri izdelavi podpisa ni nujno prisoten ob zasebnem ključu, vendar pa ima nadzor nad varnostnimi ukrepi in odgovornost za izbor ustreznih varnostnih ukrepov. Kadar pa se varen elektronski podpis izdela na oddaljenem strežniku kot storitev, podpisnik ni ne prisoten ob izdelavi podpisa, niti ne more izbrati ustreznih varnostnih ukrepov, a se kljub temu lahko odloči, ali so varnostni ukrepi, ki jih izvaja ponudnik storitve, zanj ustrezni. Za takšno odločitev mora imeti podpisnik dostop do razumljive oz. doumljive razlage varnostne zasnove sistema, poleg tega pa mora imeti tudi zaupanje, da se bodo varnostni ukrepi v resnici izvajali. Zaupanje se lahko vzpostavi ali okrepi s pregledi, izvedenimi s strani zaupanja vredne tretje osebe (na primer neodvisnega revizijskega strokovnjaka ali nadzornega organa). Ob izpolnjevanju zgoraj navedenih pogojev je po mnenju FESA mogoče doseči izključen nadzor in je posledično napredne (varne) elektronske podpise mogoče izdelovati tudi preko oddaljene naprave.

V prid takšni interpretaciji govori tudi dejstvo, da je avstrijski zakonodajni organ ob spremembi zakonodaje o elektronskem podpisovanju Evropski Komisiji posredoval pojasnjevalni memorandum, v katerem je zagovarjal stališče, da je izključen nadzor mogoče doseči tudi z drugimi, še posebej tehničnimi in organizacijskimi ukrepi in zato uporaba posebne strojne opreme (na primer USB ključa, pametne kartice) za shranjevanja zasebnega ključa ni potrebna. Memorandum tudi navaja, da so v zadnjih letih enako interpretacijo v praksi podale tudi vse države članice EU, ki so se do tega vprašanja opredelile. Hkrati pa je v memorandumu tudi poudarjeno, da morajo biti v primeru, ko je zasebni ključ shranjen na podatkovnem mediju (ki ni namensko ločen in v posesti podpisnika), zagotovljeni varnostni ukrepi, ki podpisniku omogočajo, da obdrži nadzor nad ključem.

V pravnem mnenju je podan zaključek, da **»izključen nadzor« torej ne pomeni nujno neposrednega dostopa do zasebnega ključa za tvorjenje elektronskih podpisov, prav tako ne pomeni nujno hrambe ključa na posebnem namenskem strojnem modulu.** Različni viri priznavajo možnost izpolnjevanja standarda izključnega nadzora pri rešitvah, ki uporabljajo varnostni strojni modul, pri tem pa je hkrati poudarjena tudi zahteva po ustreznem zagotavljanju zaupnosti in varnosti hranjenega zasebnega ključa. Interpretacije, rešitve in predlogi, predstavljeni v tem poglavju, so kljub njihovi navezavi na direktivo ali na pravne sisteme drugih držav članic relevantni tudi za domač pravni sistem, saj imajo implementirane zahteve direktive za varen elektronski podpis v ZEPEP enak pomen, kot izvirno besedilo direktive.

5.2.2. Naprava oz. sredstvo za varno elektronsko podpisovanje

Naprava za tvorjenje podpisa je skladno z direktivo o e-podpisu oblikovana programska ali strojna oprema za uporabo podatkov v zvezi s tvorjenjem podpisa. Naprava za varno tvorjenje podpisa pa je takšna naprava za tvorjenje podpisa, ki izpolnjuje zahteve iz Priloge III direktive. Te zahteve so implementirane tudi v 1. odstavku 37. člena ZEPEP. Z vidika hrambe zasebnih ključev na strojnem varnostnem modulu je relevantna predvsem zahteva, da mora biti podpisniku omogočeno zanesljivo varovanje njegovih podatkov za elektronsko podpisovanje. FESA v Javni izjavi o strežniško osnovanih storitvah podpisovanja glede te zahteve poudarja, da morajo biti avtentikacijski podatki zaščiteni vse od uporabniškega vmesnika do strežnika. Vsa komunikacija med podpisnikom in strežnikom mora biti torej izvedena preko zaupnih kanalov. Upravljavec strežnika poleg tega avtentikacijskih podatkov ne

sme shraniti na način, ki bi omogočal zlorabo teh podatkov s strani njegovih zaposlenih ali tretjih oseb.

Podobne zahteve podaja tudi CEN Workshop Agreement 14169 (CWA 14169), ki govori o napravah za izdelovanje podpisov. Dokument sicer ni uraden standard, vsebuje pa dobre prakse s tega področja. CWA 14169 postavlja zahtevo po zaupni poti (angl. *trusted path*) za avtentikacijo uporabnika, kadar uporabniškega vmesnika ne zagotavlja naprava za izdelavo varnega podpisa. Zakonodaja sicer ne zahteva upoštevanja navedenega ali drugih standardov, vendar pa lahko organ, ki preverja skladnost naprav za varno elektronsko podpisovanje z zakonodajo, te standarde upošteva.

Kljub temu, da je FESA v Javni izjavi izrazila dvom, da bo v bližnji prihodnosti prišlo do uporabe takšnih rešitev, se rešitev s strojnim varnostnim modulom v EU danes že uporablja (Avstrija), nekatere države pa o tem razmišljajo. Pri tem velja poudariti, da je bila avstrijska rešitev uvedena z veliko mero skrbnosti za varovanje podatkov za elektronsko podpisovanje. Avstrijski HSM strežnik se tako nahaja v visoko varovanem območju, v sefu, do katerega ima dostop samo varnostno osebje.

Pravno mnenje Inštituta za ekonomijo, pravo in informatiko tako zaključuje, da je skladno z navedenim ob izpolnjevanju relativno strogih pogojev **tudi strojni varnostni modul lahko naprava za varno elektronsko podpisovanje.**

6. ANALIZA MODELOV IDENTIFIKATORJEV, PRAVNIH IN IZVEDBENIH MOŽNOSTI

Na zelo splošni ravni lahko ugotovimo, da mora prenova sistema e-identitet slediti temeljnim ciljem, t.j. uporabniku ponuditi e-identifikator, ki je varen, enostaven za uporabo, kateremu zaupajo tako uporabniki kot kar največji krog upravljavcev osebnih podatkov/ponudnikov storitev in ki omogoča minimizacijo obdelave[17] in tokov posameznikovih osebnih podatkov[18].

Pomembno je najti rešitve, ki bi bile čim širše uporabne in bi tudi do neke mere uredile oz. poenotile obstoječe rešitve. Ta cilj je pomemben tudi z vidika vpetosti Slovenije v evropski prostor in s tem povezane vse večje zahteve po čezmejni interoperabilnosti. Nove usmeritve ne bi smele povzročati nepotrebnih dodatnih stroškov za prenovo obstoječih rešitev, tako na strani ponudnikov e-storitev, kot tudi na strani overiteljev oz. izdajateljev identitet. Zadani cilji kot izhodišče za nadaljnje usmeritve so podani v razd. 1.1.

Kot eden izmed pokazateljev, ki smo ga na podlagi natančne analize možnosti s pravnega, tehničnega in vidika varovanja osebnih podatkov uporabili pri pripravi predloga za nadaljnje usmeritve, je bil izdelan **odločitveni model** ter oblikovani **trije sklopi možnosti**, ki so jih ocenjevale različne **fokusne skupine** (ponudniki e-storitev iz javnega in zasebnega sektorja, javni uslužbenci in državljani kot končni uporabniki, strokovnjaki medresorske delovne skupine (v nadaljevanju *MDS*).

Svoji stališči o analiziranih možnosti sta podala tudi:

- Zveza potrošnikov Slovenije (v nadaljevanju *ZPS*) kot predstavnik končnih uporabnikov in
- Združenje bank Slovenije (v nadaljevanju *ZBS*) kot predstavnik ponudnikov storitev iz zasebnega sektorja, ki vključuje množico bank s svojimi rešitvami za e-bančništvo, ki je ena izmed najbolj uveljavljenih elektronskih storitev.

V nadaljevanju je predstavljeno izvedeno vrednotenje (odločitveni model, rezultati vrednotenja in izsledki občutljivostne analize). Na koncu sta podani še obe zunanji mnenji in glavne ugotovitve.

6.1. Vrednotenje na podlagi odločitvenega modela

Pri pripravi odločitvenega modela, ki je podrobno predstavljen v Prilogi C, smo sodelovali s strokovnjaki Fakultete za upravo Univerze v Ljubljani za področje odločitvenih sistemov. V modelu smo, izhajajoč iz osmih ciljev za prenovo e-identitet (glej razd. 1.1), možnosti razdelili v tri različne sklope, in sicer v **pravne možnosti e-identitet**, **modele identifikatorjev** in različne **tehnične izvedbe**.

Za pridobitev mnenja o različnih možnosti s strani vseh deležnikov, povezanih z e-identitetami, smo za vsakega od sklopov razvili ločen odločitveni model ki so ga vrednotile različne fokusne skupine:

- ponudniki e-storitev iz javnega in zasebnega sektorja,

[17] Centralni avtentikacijski sistem ima tu nekatere zelo zanimive prednosti, saj minimizira obdelavo osebnih podatkov npr. EMŠO, davčne ali številke zdravstvenega zavarovanja.

[18] Glej tudi priporočila ter identifikacijo trendov s strani OECD.

- javni uslužbenci in državljani kot končni uporabniki,
- strokovnjaki MDS.

6.1.1. Odločitveni model

Za potrebe vrednotenja možnosti so bili razviti trije odločitveni modeli, za vsak sklop poseben model:

***Sklop 1*: model za ovrednotenje **pravnih možnosti e-identitet**, ki omogoča vrednotenje treh alternativ, predstavljenih v razd. 3.2:

- e-osebne izkaznice,
- akreditirane e-identitete in
- kvalificiranega digitalnega potrdila na pametnem mediju;

***Sklop 2**: model za ovrednotenje **modelov identifikatorjev** za vrednotenje petih alternativ, predstavljenih v razd. 4.3:

- obstoječega identifikatorja v digitalnem potrdilu,
- obstoječega identifikatorja v zalednem sistemu overitelja,
- e-identifikatorja osebe v digitalnem potrdilu,
- e-identifikatorja osebe v zalednem sistemu overitelja in
- sektorskega e-identifikatorja osebe;

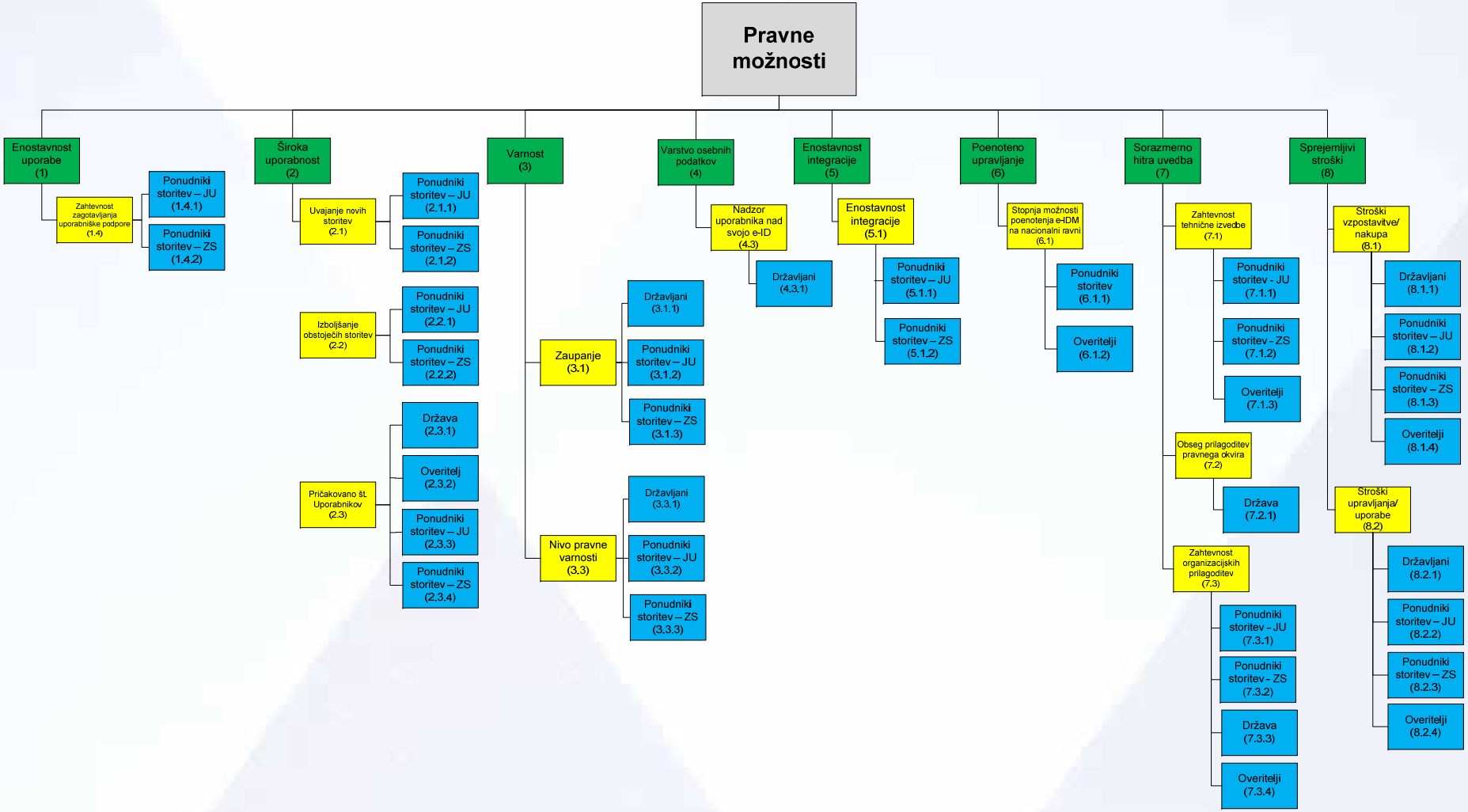
Sklop 3: model za ovrednotenje variant **tehnične izvedbe e-identitet**; izmed možnosti, predstavljenih v razd. 5.1, smo v postopek vrednotenja vključili šest najbolj smiselnih alternativ:

- pametne kartice z digitalnim potrdilom,
- pametne kartice z dvojnim dostopom (kontaktnim in brez-kontaktnim) z digitalnim potrdilom,
- pametnega ključka z digitalnim potrdilom,
- mobilnega telefona z digitalnim potrdilom na SIM kartici,
- pametnega medija (kartice, ključka) za dostop do digitalnega potrdila na varnostnem modulu in
- mobilnega telefona za dostop do digitalnega potrdila na varnostnem modulu.

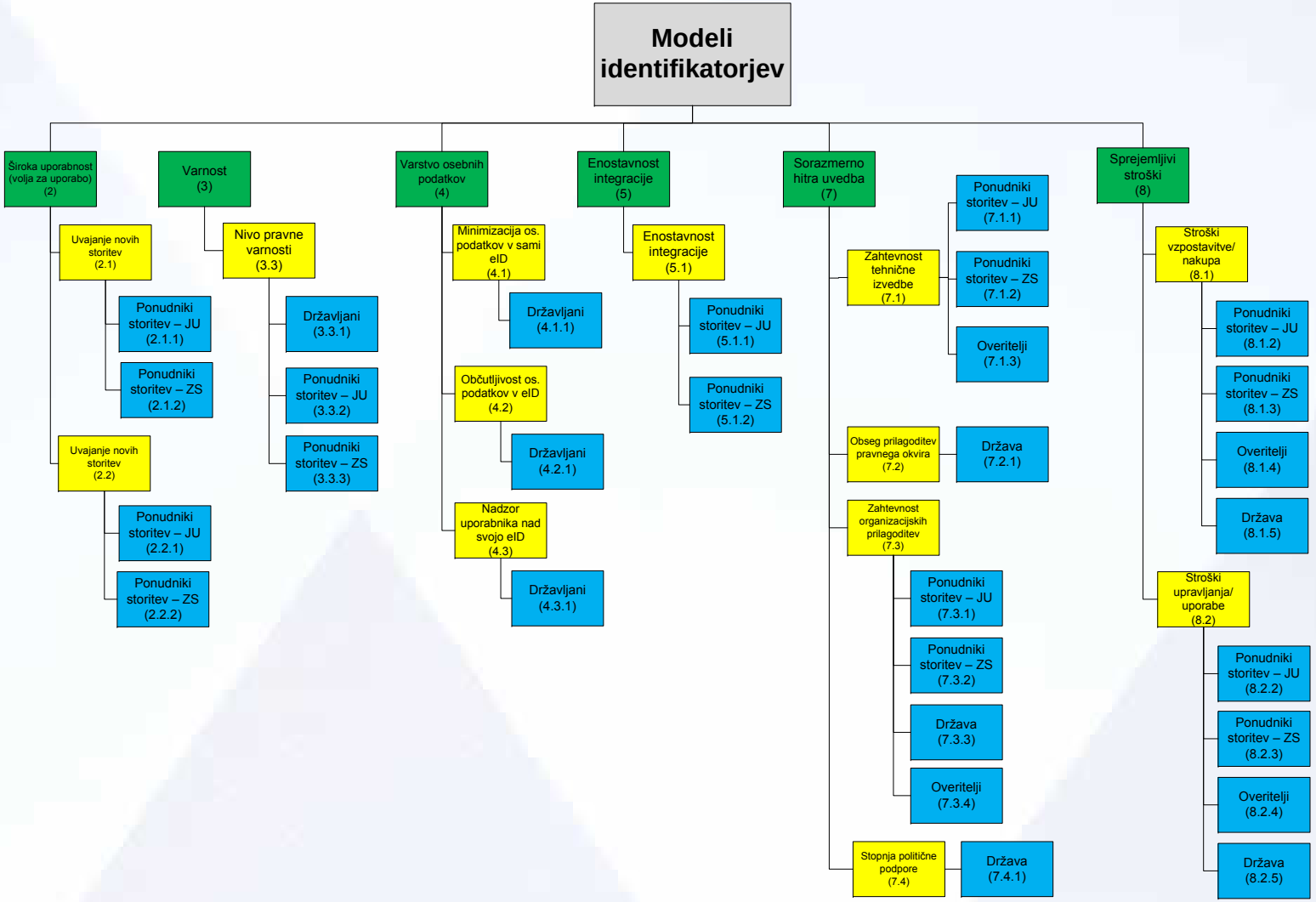
Pri vseh treh odločitvenih modelih so bile uporabljene metode večparametrskega modeliranja[19], katerega bistvena značilnost je hkratna evalvacija več kot ene lastnosti alternativ. Zaradi velikega števila ocenjevanih parametrov so ti urejeni hierarhično v več nivojev in tako tvorijo drevo oz. hierarhijo parametrov. Na prvem nivoju so pri vseh drevesih cilji, ki naj bi jih izpolnjevale implementirane rešitve, na preostalih nivojih so iz ciljev izpeljani parametri, ki jih je definirala medresorska delovna skupina. Na zadnjem nivoju so zbrani osnovni parametri, ki hkrati prikazujejo ciljne skupine, na katere se ti parametri nanašajo. Vsi osnovni parametri imajo zalogo vrednosti 1 – 5, pri čemer 1 vedno predstavlja najslabšo, 5 pa najboljšo oceno.

Uteži parametrov so bile določene znotraj medresorske delovne skupine, njihove vrednosti so podane v Prilogi C. Pri zbiranju vrednosti za osnovne parametre so sodelovali člani medresorske delovne skupine, predstavniki ponudnikov storitev v javnem in zasebnem sektorju, predstavniki javnih uslužbencev ter predstavniki državljanov. Pri prvih treh skupinah se je za zbiranje osnovnih vrednosti parametrov preko vprašalnika izvedlo srečanje, na katerem se je skupini predstavil problem, področje in cilji, s predstavniki javnih uslužbencev in državljanov pa so bili izvedeni intervjuji. Tako določene uteži in zbrane vrednosti osnovnih parametrov so bile vnesene v vse tri odločitvene modele, ki so prikazani na naslednjih slikah.

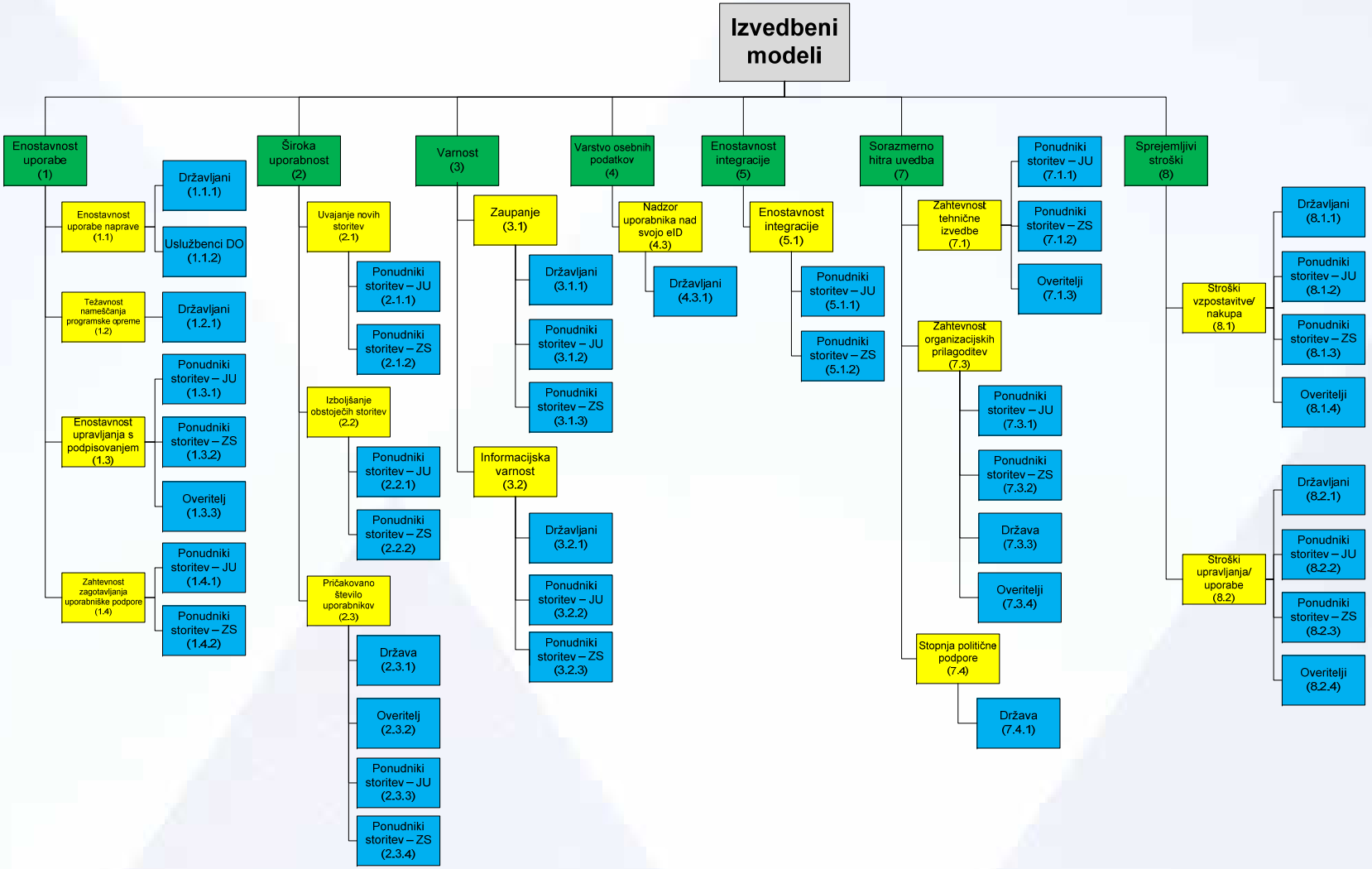
[19] Obravnavani problem je rešljiv z metodami večparametrskega modeliranja. Tako kot večina praktičnih odločitev je namreč tudi odločanje med alternativami e-identitet večparametrsko, katerega bistvena značilnost pa je hkratna evalvacija več kot ene lastnosti alternativ. Na voljo je veliko metod, s katerimi lahko podpremo večparametrsko odločanje. Obravnavani problem predstavlja hierarhični večparametrski model, saj ima razmeroma veliko število parametrov, med njimi pa obstajajo podredna in nadredna razmerja. V predstavljenem modelu je izbran nabor parametrov urejen hierarhično v več nivojev, tako da predstavlja drevo oz. hierarhijo parametrov, pri čemer podredni parametri vplivajo na pripadajoči nadredni parameter npr. cilj »enostavnost uporabe« je razdeljen na enostavnost uporabe naprave, težavnost nameščanja programske opreme, enostavnost upravljanja s podpisovanjem in zahtevnost zagotavljanja uporabniške podpore. Pri razvoju odločitvenih modelov je bilo v prvi vrsti zasledovano načelo polnosti parametrov. Poleg tega so bili upoštevani tudi naslednji kriteriji: neredundantnost, medsebojna neodvisnost oz. ortogonalnost, operativnost, vsebinska povezanost in medsebojna odvisnost podrednih parametrov v okviru posameznega nadrednega parametra ter določena mera konzervativnosti pri številu podrednih parametrov. Za realizacijo odločitvenih modelov je bilo izbrano orodje Web-HIPRE, predvsem zato, ker je prosto dostopno spletno orodje, podpira hierarhično večparametrsko modeliranje in ker nudi implementacijo metod AHP (analitično-hierarhični proces) in MAVT (teorija večatributne vrednosti).



Slika 4: Model 1 - pravne možnosti e-identitet



Slika 5: Model 2 - modeli identifikatorjev



Slika 6: Model 3 - izvedbeni modeli e-identitet

6.1.2. Predstavitev rezultatov

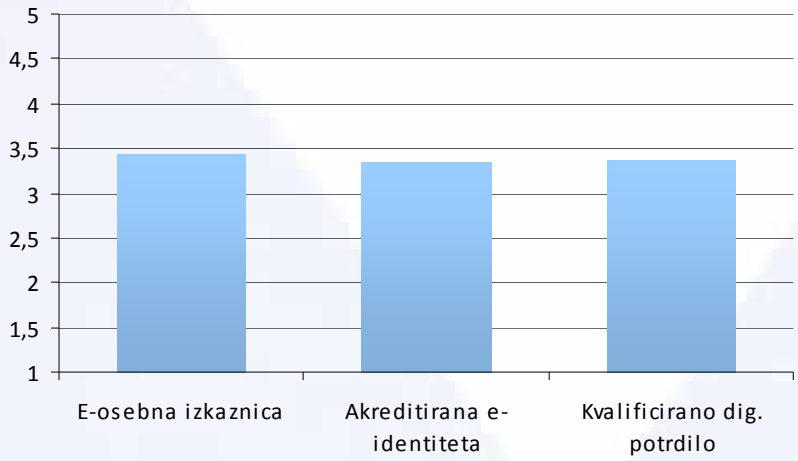
Rezultati vrednotenja so podrobno podani v Prilogi D, v nadaljevanju pa so v strnjeni obliki prikazani po posameznih modelih. Za lažjo predstavo in analogno z načinom ocenjevanja so rezultati predstavljeni na lestvici 1-5, kjer ocena 1 pomeni najnižjo, ocena 5 pa najvišjo možno oceno.

Poleg rezultatov, pridobljenih s strani vseh fokusnih skupin za vse cilje odločitvenega modela, so zaradi večje preglednosti podani tudi rezultati vrednotenja po dodatnih scenarijih in sicer po posameznih ciljih in po fokusnih skupinah. V ta namen je bilo potrebno odločitvene modele nekoliko prilagajati, zato v modelih ni možno medsebojno primerjati rezultatov za posamezno varianto (npr. eOI) med različnimi scenariji (npr. MDS, varnost), lahko pa medsebojno primerjamo rezultate za posamezne variante v istem scenariju.

Zavedali smo se možnosti, da bi bile ocene posameznih variant s strani nekaterih fokusnih skupin (predvsem državljanov) lahko podane neustrezno zaradi zahtevnosti področja in preslabega poznavanja posameznih rešitev, predvsem tistih, ki še niso v uporabi oz. razširjene, kot npr. akreditirana e-identiteta, sektorski e-identifikator, rešitve s potrdilom na varnostnem modulu. Zato smo preverili tudi scenarij, v katerem smo namesto ocen državljanov upoštevali ocene ZPS, a smo ugotovili, da ta sprememba v ničemer ne vpliva na končni vrstni red ocenjevanih variant.

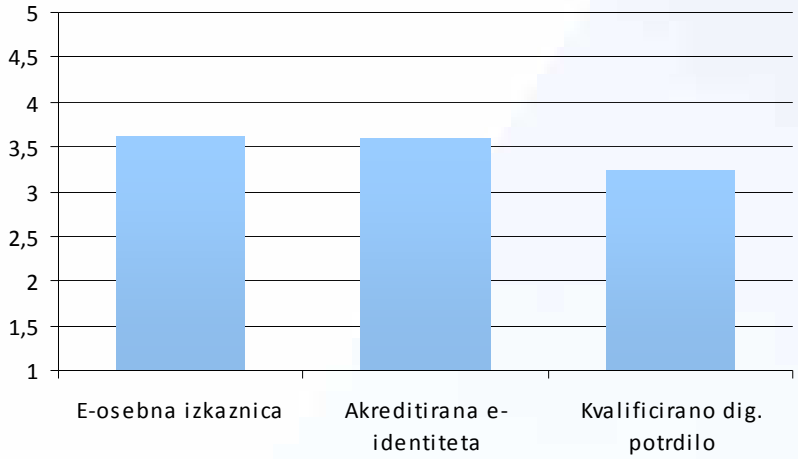
Rezultati za pravne možnosti (Sklop 1)

Na podlagi rezultatov vrednotenja s strani različnih fokusnih skupin vidimo, da v celotnem modelu najvišji rezultat dosega E-osebna izkaznica (3,440), sledi Kvalificirano digitalno potrdilo (3,360) in nato Akreditirana e-identiteta (3,340), razlike pa so zelo majhne. Rezultat prikazuje Slika 7.



Slika 7 - Rezultati za pravne možnosti

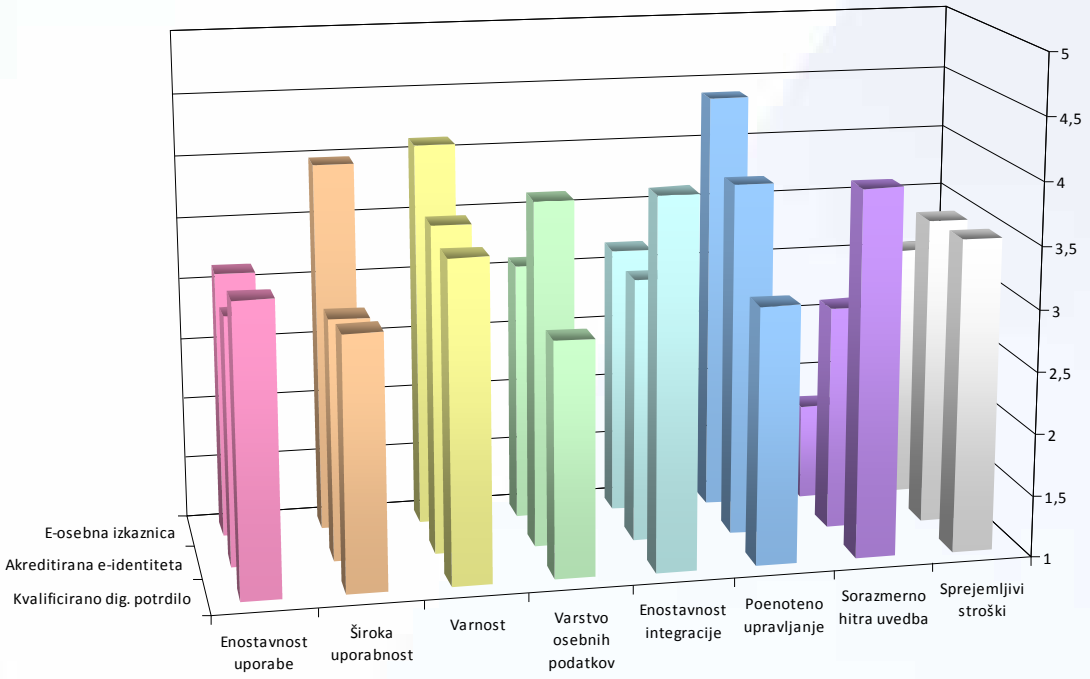
Če pogledamo rezultate posameznih skupin, je tudi medresorska delovna skupina (glej Slika 8) najbolje ocenila E-osebno izkaznico, le da ji na drugem mestu z relativno majhno razliko sledi Akreditirana e-identiteta.



Slika 8 – Rezultati za pravne možnosti – po vrednotenju MDS

Pri rezultatih državljanov je slika drugačna. Najbolje je ocenjeno Kvalificirano dig. potrdilo, najslabše pa Akreditirana e-identiteta. Enak model je vrednotila tudi Zveza potrošnikov Slovenije, kjer prvo mesto dosega Kvalificirano dig. potrdilo, E-osebna izkaznica pa je na zadnjem. Pri rezultatih ponudnikov storitev v javni upravi je vrstni red enak kot pri rezultatih medresorske delovne skupine. Pri rezultatih ponudnikov storitev v zasebnem sektorju je vrstni red enak kot pri rezultatih državljanov. Združenje bank Slovenije ima drugačno mnenje, ki se ujema z rezultati ponudnikov storitev v javni upravi oz. medresorske delovne skupine.

Če primerjamo variante glede doseganja osnovnih osmih ciljev (Slika 9), lahko pridemo do ugotovitve, da je E-osebna izkaznica najbolj sprejemljiva z vidika ciljev široke uporabnosti, varnosti in poenotenega upravljanja. Akreditirana e-identiteta je po drugi strani najbolj ugodna z vidika varstva osebnih podatkov, Kvalificirano dig. potrdilo pa je najbolje ocenjeno z vidika enostavnosti uporabe, enostavnosti integracije, sorazmerno hitre uvedbe in sprejemljivih stroškov.



Slika 9 - Rezultati za pravne možnosti – po posameznih ciljih

Povzetek

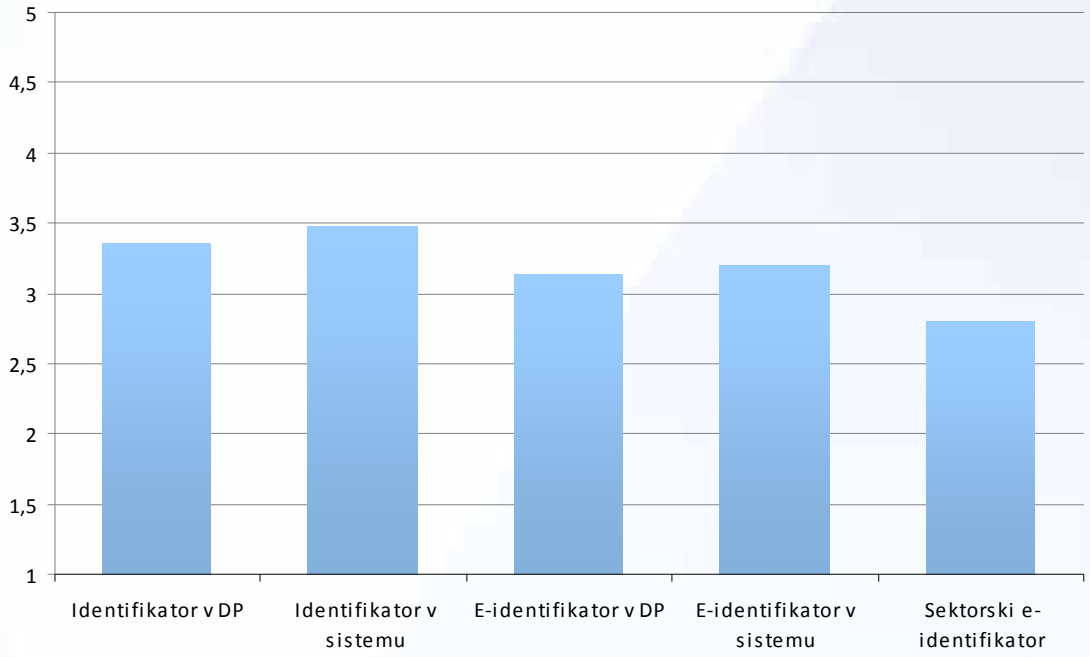
Upoštevaje rezultate ocenjevanja fokusnih skupin ugotavljamo, da lahko v grobem oblikujemo dva razreda fokusnih skupin, razred javne uprave in razred zasebnega sektorja. Javna uprava (medresorska delovna skupina in ponudniki storitev v javni upravi) kot najprimernejšo rešitev ocenjuje E-osebno izkaznico, kot najmanj primerno pa Kvalificirano dig. potrdilo; enako je tudi mnenje Združenja bank Slovenije. Zasebni sektor (državljani, Zveza potrošnikov Slovenije in ponudniki storitev v zasebnem sektorju) pa meni, da je najugodnejše prav Kvalificirano dig. potrdilo.

Z vidika kriterijev oz. ciljev se kot najprimernejša rešitev največkrat izkaže Kvalificirano dig. potrdilo, najslabši rezultat pa najmanj pogosto beleži E-osebna izkaznica. Akreditirana e-identiteta je kot najbolj primerna rešitev ocenjena le v enem scenariju, kar je očitno posledica nedorečenosti tovrstne rešitve in njenega pomanjkljivega poznavanja s strani ocenjevalcev.

V celoti gledano se izmed ocenjevanih pravnih možnosti urejanja e-identitet **kot najbolj primerna rešitev izkaže E-osebna izkaznica**, saj najboljši rezultat beleži enako pogosto kot Kvalificirano dig. potrdilo, a ima v nasprotju z njim bistveno manj najslabših rezultatov.

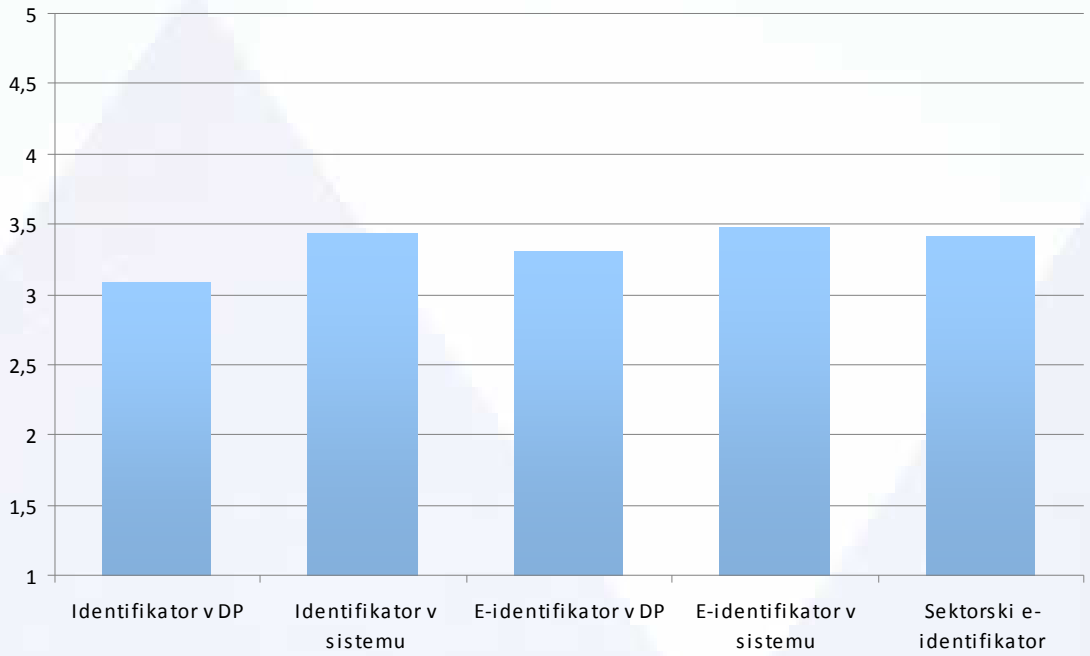
Rezultati za modele identifikatorjev (Sklop 2)

Na podlagi rezultatov, zbranih z ocenjevanjem možnosti vseh fokusnih skupin, razberemo, da najvišji rezultat dosega Identifikator v zalednem sistemu (3,480), sledijo mu Identifikator v digitalnem potrdilu (v nadaljevanju *DP*) (3,364), E-identifikator v zalednem sistemu (3,208), E-identifikator v DP (3,140) in Sektorski e-identifikator (2,792). Rezultate prikazuje Slika 10.



Slika 10 - Rezultati za modele identifikatorjev

Pri rezultatih medresorske delovne skupine (Slika 11) je najbolje ocenjen E-identifikator v zalednem sistemu, sledijo Identifikator v zalednem sistemu, Sektorski e-identifikator, E-identifikator v DP in nazadnje Identifikator v DP.

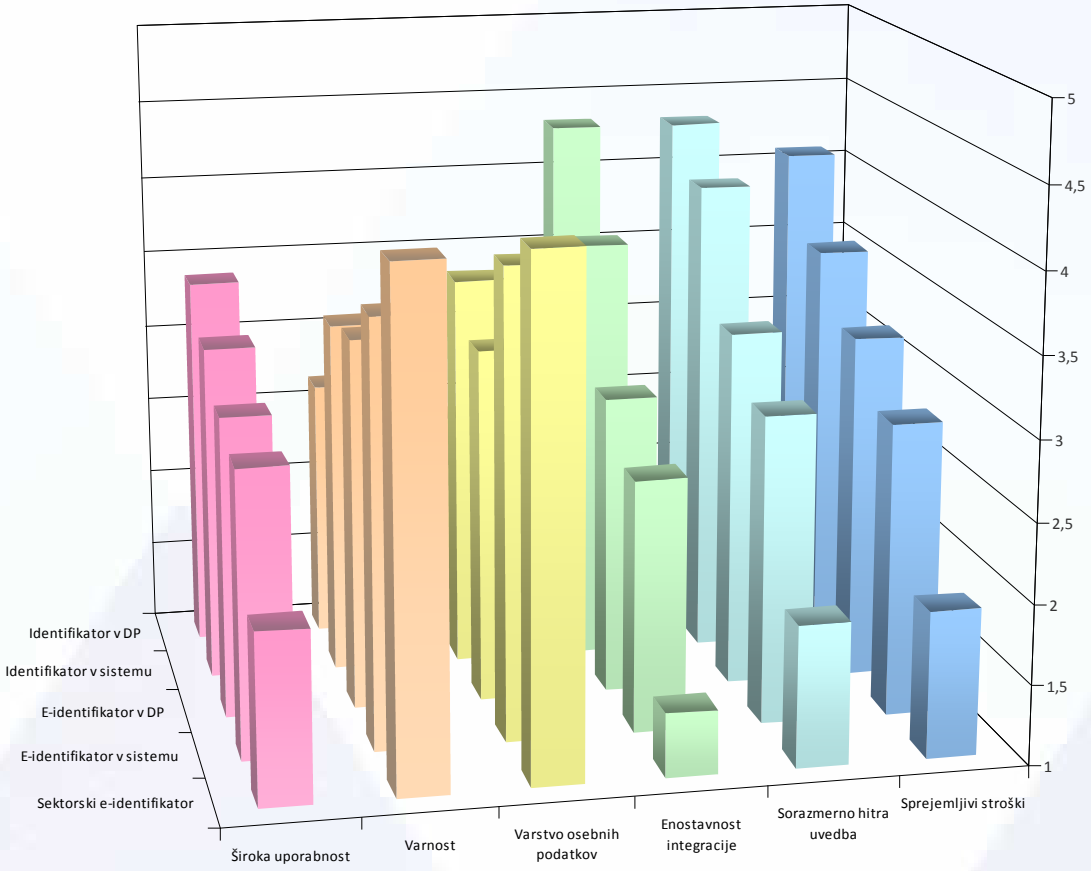


Slika 11 - Rezultati za modele identifikatorjev – po vrednotenju MDS

Pri rezultatih obeh tipov ponudnikov storitev je slika domala obrnjena: najbolj zaželen je Identifikator v DP, potem pa se zvrstijo Identifikator v zalednem sistemu, E-identifikator v DP,

E-identifikator v zalednem sistemu in na koncu še Sektorski e-identifikator z daleč najnižjo oceno. Praktično enaki so tudi rezultati Združenja bank Slovenije.

Če pogledamo rezultate po posameznih ciljih (Slika 12), vidimo, da je Identifikator v DP glede doseganja osnovnih osmih ciljev najbolj sprejemljiv z vidika široke uporabnosti, enostavnosti integracije, sorazmerno hitre uvedbe in sprejemljivih stroškov, kjer je povsod kot najmanj zaželen ocenjen Sektorski e-identifikator. Sektorski e-identifikator je najbolj primeren z vidika varnosti in varstva osebnih podatkov, v obeh primerih pa najnižji rezultat beleži Identifikator v DP. Med ostalimi variantami imata z vidika osnovnih kriterijev Identifikator v zalednem sistemu in E-identifikator v zalednem sistemu domala povsem različne rezultate, E-identifikator v DP pa skoraj vedno vmesni rezultat.



Slika 12 - Rezultati za modele e-identitet – po posameznih ciljih

Povzetek

Na podlagi zgoraj predstavljenih rezultatov ugotavljamo, da sta si po rezultatih najbolj nasprotujoča Identifikator v dig. potrdilu in Sektorski identifikator. Čeprav je Identifikator v dig. potrdilu najbolj zaželen pri vseh ponudnikih storitev, odločitev zanj ni priporočljiva zaradi nizkega rezultata z vidika varnosti in varstva osebnih podatkov. Nasprotno je Sektorski e-identifikator najboljši prav s teh dveh vidikov, vendar pri vseh ostalih vidikih in ocenah fokusnih skupin (z izjemo medresorske delovne skupine) povsod dosega najnižji rezultat, zato ne predstavlja smotrne odločitve.

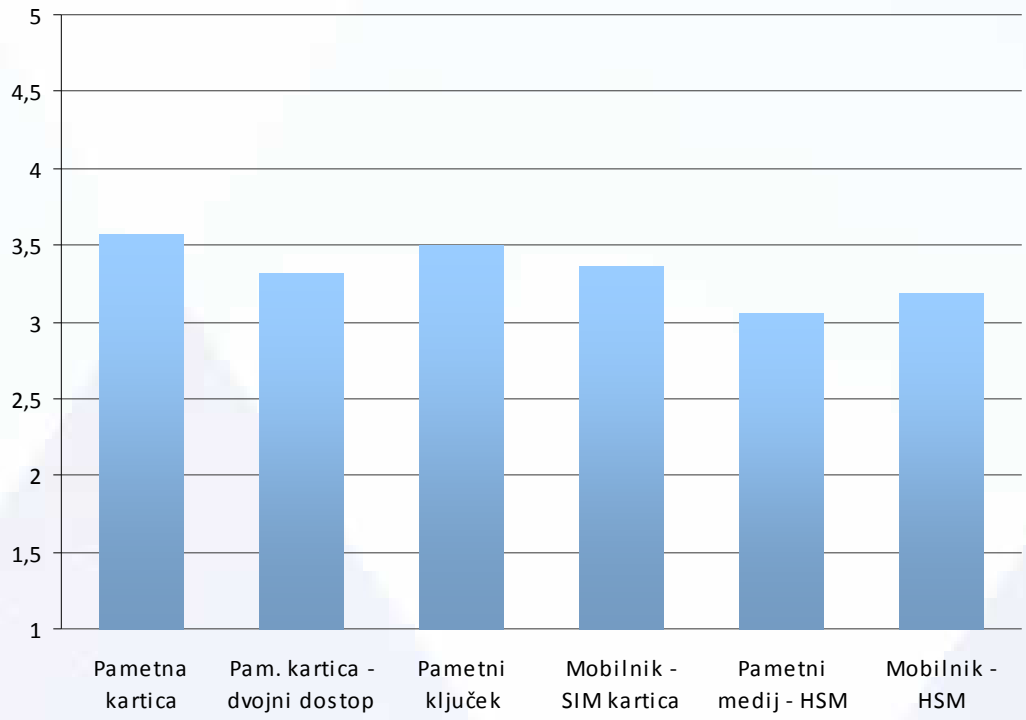
Pri primerjavi obeh variant, ki se zanašata na zaledni sistem, se kot primernejša izkaže rešitev z obstoječim identifikatorjem, saj uvedba dodatnega E-identifikatorja pomeni višje stroške, počasnejšo uvedbo, težjo integracijo in manjšo uporabnost, kljub temu, da je ugodnejša z vidika varnosti in varstva osebnih podatkov.

V medsebojni primerjavi obeh variant z e-identifikatorjem sta rešitvi precej izenačeni, E-identifikator v dig. potrdilu je nekoliko primernejši le zaradi hitrejše uvedbe in nižjih stroškov.

V celoti gledano se izmed ocenjevanih modelov identifikatorjev **kot najbolj primerna rešitev izkaže Identifikator v zalednem sistemu**.

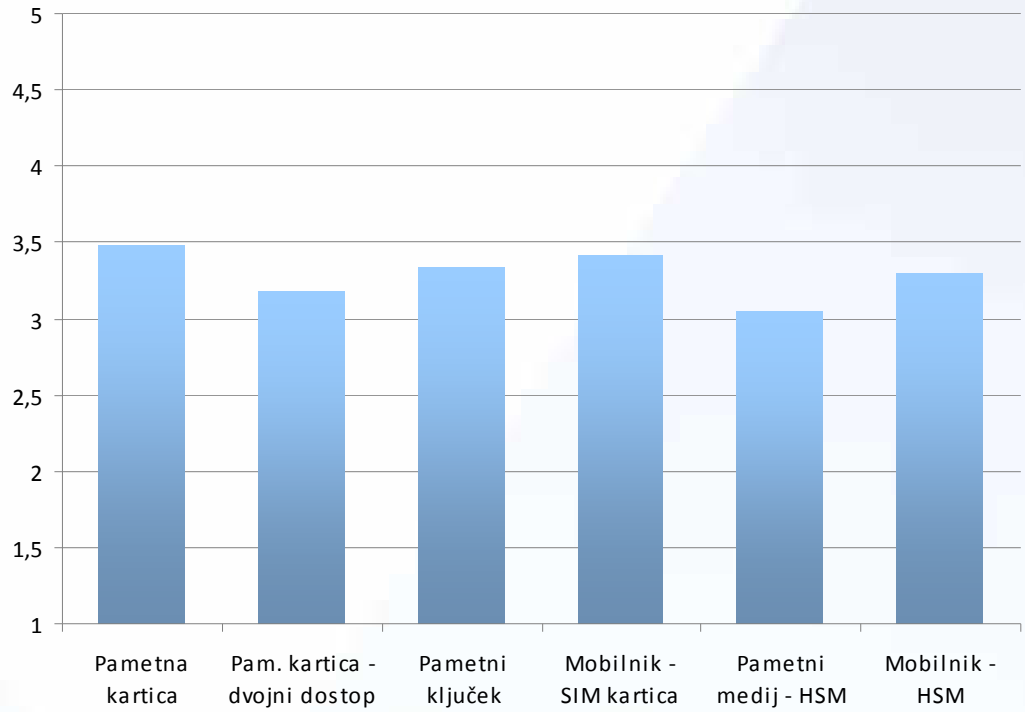
Rezultati za izvedbene možnosti (Sklop 3)

V celotnem modelu (Slika 13) najvišji rezultat dosegata Pametna kartica (3,564) in Pametni ključek (3,504), sledita Mobilni telefon s potrdilom na SIM kartici (3,360) ter Pametna kartica z dvojnim dostopom (3,316), nazadnje pa še obe varianti z varnostnim modulom, to je v kombinaciji z mobilnim telefonom (3,192) oziroma pametnim medijem (3,064).



Slika 13 - Rezultati za izvedbene možnosti

Tudi pri rezultatih medresorske delovne skupine (Slika 14) je najbolje ocenjena Pametna kartica, sledijo Mobilni telefon s potrdilom na SIM kartici, Pametni ključek, Mobilni telefon s potrdilom na varnostnem modulu, Pametna kartica z dvojnim dostopom ter nazadnje še Pametni medij s potrdilom na varnostnem modulu.

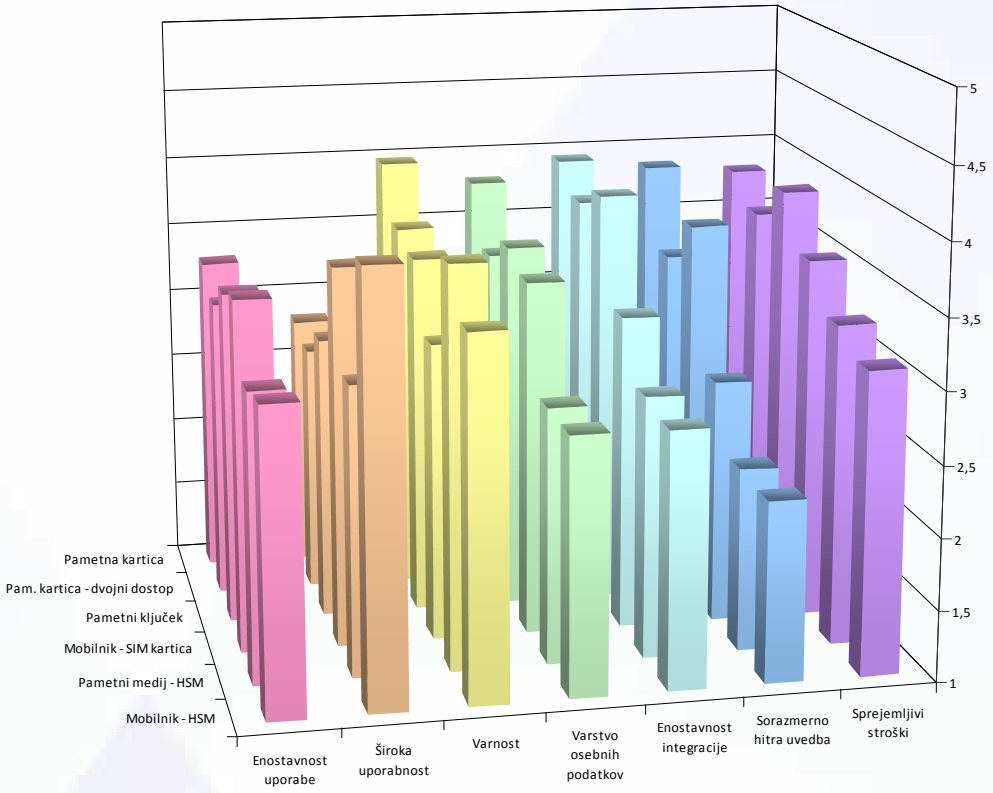


Slika 14 - Rezultati za izvedbene možnosti – po vrednotenju MDS

Tudi pri rezultatih državljanov je na prvem mestu Pametna kartica, ki ji sledijo Pametna kartica z dvojnim dostopom, Pametni ključek ter Pametni medij s potrdilom na varnostnem modulu, najslabše pa sta ocenjeni obe varianti z mobilnim telefonom, to je s potrdilom na SIM kartici oziroma na varnostnem modulu. Pri rezultatih Zveze potrošnikov Slovenije, kjer je uporabljen isti model kot za državljane, so rezultati povsem drugačni, saj je najbolje ocenjena varianta z Mobilnim telefonom s potrdilom na SIM kartici, s povsem enako oceno sledita obe varianti s potrdilom na varnostnem modulu, nato pa še Pametni ključek, Pametna kartica z dvojnim dostopom in običajna pametna kartica. Ti rezultati se sicer nekoliko razlikujejo od priloženega mnenja, v katerem ZPS navaja, da je najprimernejša varianta Mobilni telefon s potrdilom na varnostnem modulu, saj ni odvisna od mobilnih operaterjev in kartic SIM.

Pri rezultatih ponudnikov storitev v javni upravi je spet na prvem mestu Pametna kartica, ki ji najprej sledita Pametni ključek in Pametna kartica z dvojnim dostopom, nato obe varianti s potrdilom na varnostnem modulu, pri čemer je bolje ocenjena varianta z mobilnim telefonom, najslabšo oceno pa je pridobil Mobilni telefon s potrdilom na SIM kartici. Pri rezultatih ponudnikov storitev v zasebnem sektorju je najbolje ocenjen Pametni ključek, ki mu sledijo Mobilni telefon s potrdilom na SIM kartici, Pametna kartica, Mobilni telefon s potrdilom na varnostnem modulu, Pametna kartica z dvojnim dostopom ter Pametni medij s potrdilom na varnostnem modulu. Podobno kot pri večini fokusnih skupin tudi pri Združenju bank Slovenije najvišji rezultat dosega Pametna kartica, sledita ji Pametna kartica z dvojnim dostopom in Pametni ključek, zatem Mobilni telefon s potrdilom na SIM kartici, nazadnje pa še obe varianti z varnostnim modulom, to je v kombinaciji s pametnim medijem oziroma mobilnim telefonom.

Če pogledamo rezultate po doseganju zadanih osmih ciljev (Slika 15), pametna kartica najvišje rezultate dosega z vidika varnosti, varstva osebnih podatkov, enostavnosti integracije in sorazmerno hitre uvedbe. Pametni ključek je najbolj primeren z vidika sprejemljivih stroškov. Mobilni telefon s potrdilom na SIM kartici je najbolj sprejemljiv z vidika enostavnosti uporabe. Mobilni telefon s potrdilom na varnostnem modulu najvišji rezultat dosega z vidika široke uporabnosti.



Slika 15 - Rezultati za izvedbene možnosti – po posameznih ciljih

Povzetek

Z vidika doseganja osnovnih ciljev bi lahko variante (z izjemo Mobilnega telefona s potrdilom na SIM kartici) združili v dve skupini in sicer na **rešitve z dig. potrdilom na pametnem mediju** ter na **rešitvi z dig. potrdilom na varnostnem modulu**; taka delitev je zelo očitna z vidika varstva osebnih podatkov, enostavnosti integracije, sorazmerno hitre uvedbe ter sprejemljivih stroškov, opazna pa tudi z vidika enostavnosti uporabe in široke uporabnosti; razen pri slednjem vidiku višje rezultate povsod dosegajo rešitve z dig. potrdilom na pametnem mediju.

Upoštevajoč tako rezultate posameznih fokusnih skupin kot posameznih ciljev se **kot najbolj primerna varianta izkaže Pametna kartica.** Odločitev za Pametno kartico z dvojnim dostopom je smiselna v primeru, da dodatna funkcionalnost brezkontaktnega dostopa odtehta pomisleke v zvezi z varnostjo in varstvom osebnih podatkov pri tej rešitvi. Pametni ključek je kot alternativa zanimiv zaradi nekoliko enostavnejše uporabe, širše uporabnosti ter nižjih stroškov.

Izmed obeh variant z mobilnim telefonom v večini primerov višje rezultate dosega rešitev s potrdilom na SIM kartici.

V medsebojni primerjavi obeh variant s potrdilom na varnostnem modulu sta rešitvi domala izenačeni.

6.1.3. Občutljivostna analiza

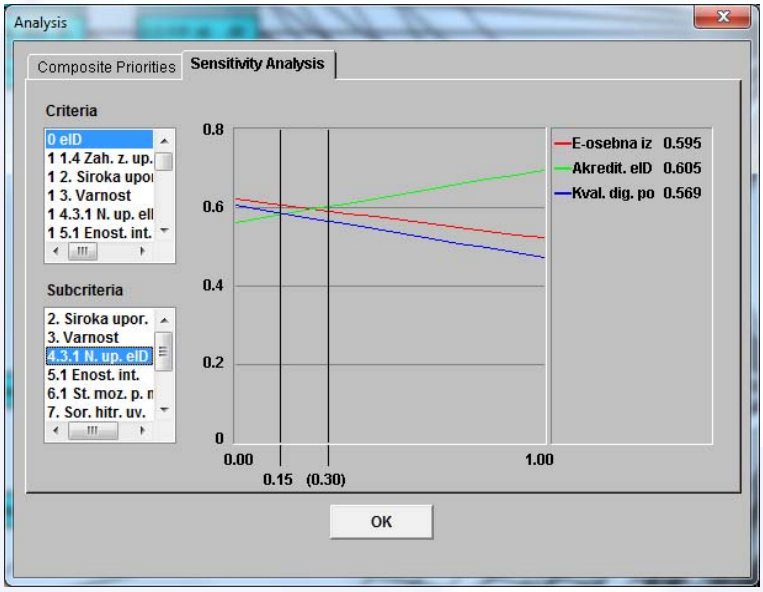
Pri občutljivostni analizi gre za preverjanje občutljivosti odločitvenega modela na sorazmerno majhne spremembe posameznih uteži, pri čemer povečanje oz. zmanjšanje uteži za posamezen kriterij povzroči normaliziranje uteži za vse ostale kriterije. Ugotovili smo, da je izvedba analize smiselna samo pri kriterijih na prvem nivoju, ki predstavljajo cilje, saj spreminjanje uteži na nižjih nivojih nima omembe vrednega učinka na končne rezultate posameznih variant.

Občutljivostno analizo smo izvajali pri vseh tistih kriterijih, kjer je podvojitev ali razpolovitev uteži povzročila opazen učinek na vrstni red ocenjevanih variant.

Izvedene analize so predstavljene v nadaljevanju, na osnovi tako pridobljenih rezultatov pa lahko ugotovimo, da so **vsi trije modeli neobčutljivi tudi na občutne spremembe uteži**, saj (razen izjemoma) **spremembe uteži ne privedejo do razlik v vrstnem redu najbolje ocenjenih variant**.

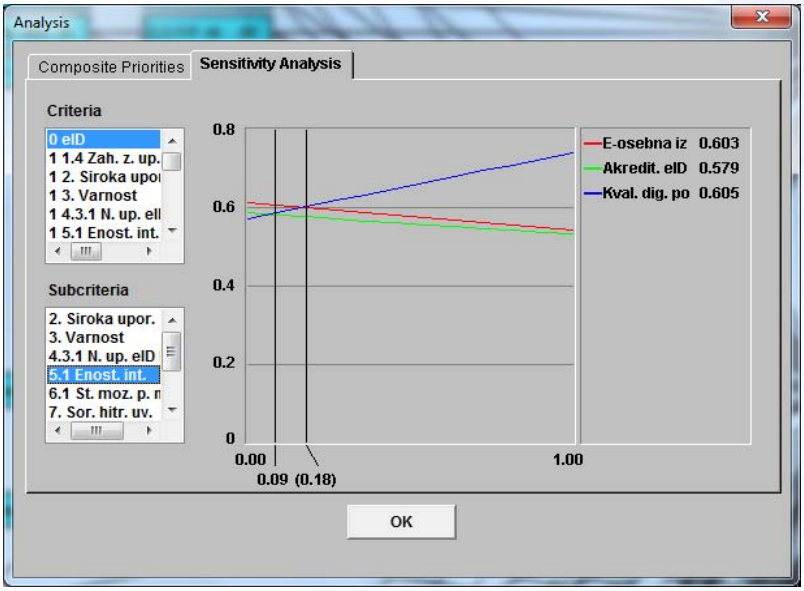
Občutljivostna analiza za pravne možnosti (Sklop 1)

Pri modelu z pravnimi možnostmi smo izvedli tri analize. Če utež za kriterij »Varstvo osebnih podatkov« iz 0,15 povečamo na 0,30, najboljši rezultat beleži Akreditirana e-identiteta, vrstni red ostalih dveh variant pa ostane nespremenjen:



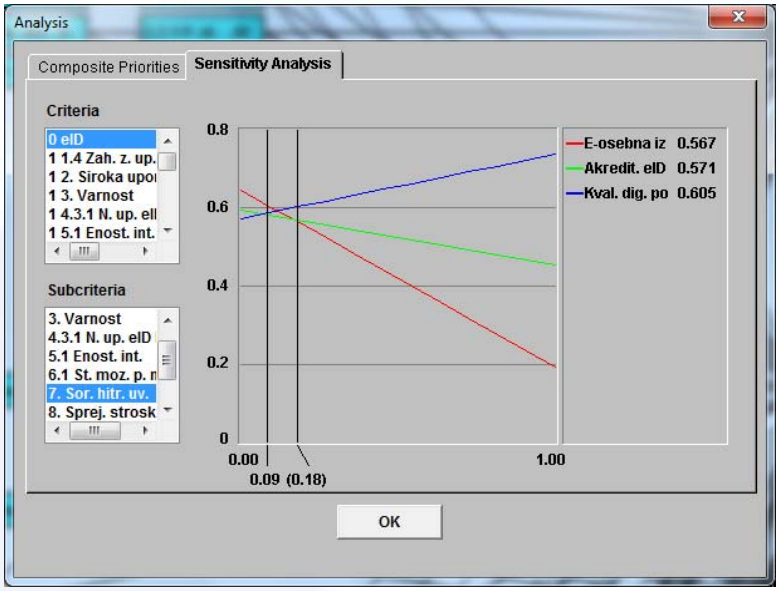
Slika 16 – Občutljivostna analiza za pravne možnosti - 1

Če utež za kriterij »Enostavnost integracije« iz 0,09 povečamo na 0,18, najboljši rezultat beleži Kvalificirano dig. potrdilo, vrstni red ostalih dveh variant pa ostane nespremenjen:



Slika 17 – Občutljivostna analiza za pravne možnosti - 2

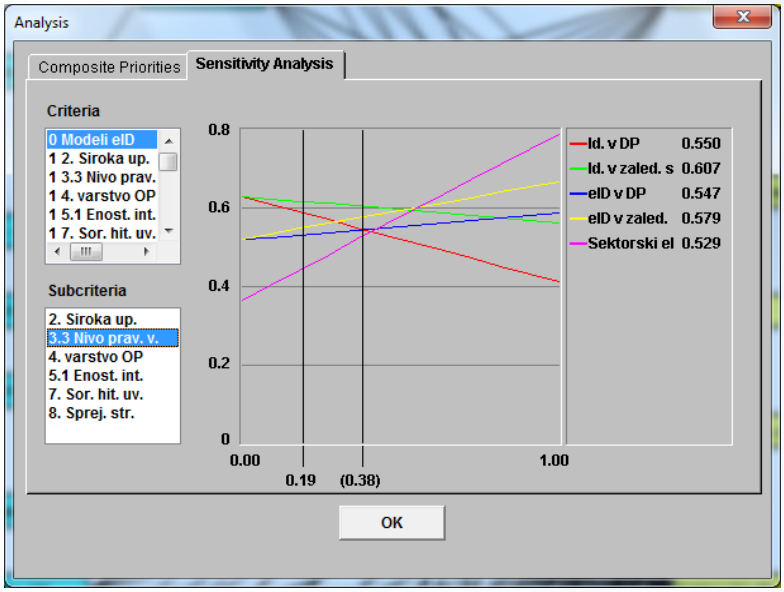
Če utež za kriterij »Sorazmerno hitra uvedba« iz 0,09 povečamo na 0,18, najboljši rezultat beleži Kvalificirano dig. potrdilo, ki mu sledi Akreditirana e-identiteta:



Slika 18 – Občutljivostna analiza za pravne možnosti - 3

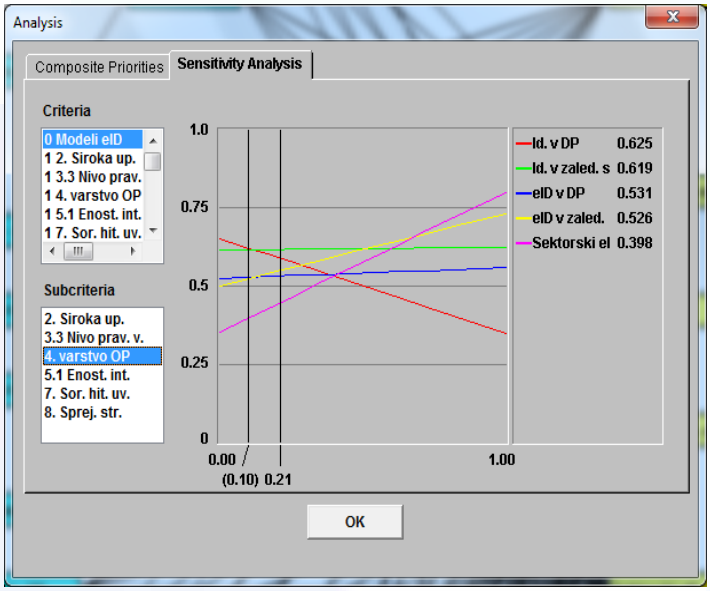
Občutljivostna analiza za modele identifikatorjev (Sklop 2)

Pri tem modelu smo izvedli štiri analize. Če utež za kriterij »Varnost« iz 0,19 povečamo na 0,38, drugi najboljši rezultat beleži E-identifikator v sistemu, rezultata za Identifikator v DP in E-identifikator v DP pa sta skoraj izenačena:



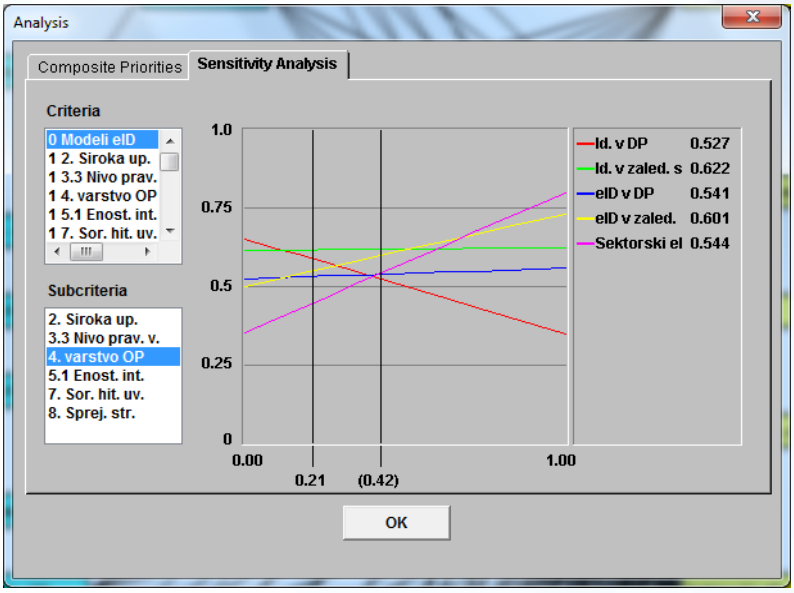
Slika 19 – Občutljivostna analiza za modele e-identitet - 1

Če utež za kriterij »Varstvo osebnih podatkov« iz 0,21 zmanjšamo na 0,10, najboljši rezultat beleži Identifikator v DP, ki mu z majhno razliko sledi Identifikator v sistemu, prav tako pa je majhna razlika med naslednjima dvema variantama, ki sta E-identifikator v DP in E-identifikator v sistemu:



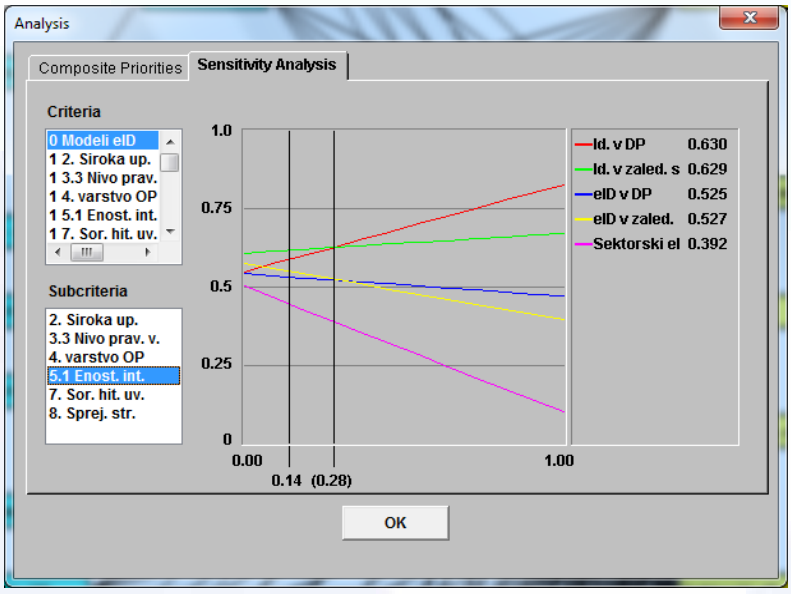
Slika 20 – Občutljivostna analiza za modele e-identitet - 2

Če utež za kriterij »Varstvo osebnih podatkov« iz 0,21 povečamo na 0,42, drugi najboljši rezultat beleži E-identifikator v sistemu, ki mu skoraj izenačena sledita Sektorski e-identifikator in E-identifikator v DP, najslabši pa postane rezultat za Identifikator v DP:



Slika 21 – Občutljivostna analiza za modele e-identitet - 3

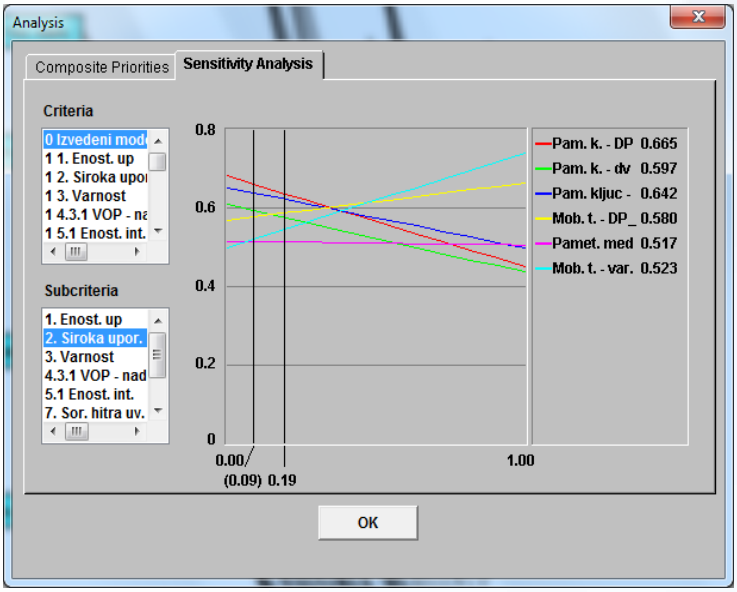
Če utež za kriterij »Enostavnost integracije« iz 0,14 povečamo na 0,28, najboljši rezultat beleži Identifikator v DP, ki mu z majhno razliko sledi Identifikator v sistemu, prav tako pa je majhna razlika med naslednjima dvema variantama, ki sta E-identifikator v sistemu in E-identifikator v DP:



Slika 22 – Občutljivostna analiza za modele e-identitet - 4

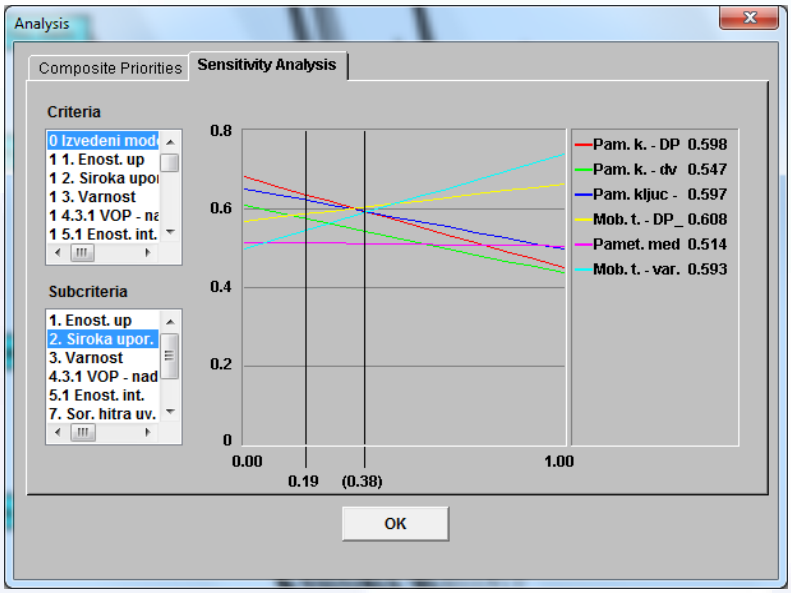
Občutljivostna analiza za izvedbene možnosti (Sklop 3)

Pri modelu za izvedbene možnosti smo izvedli tri analize. Če utež za kriterij »Široka uporabnost« iz 0,19 zmanjšamo na 0,09, tretji najboljši rezultat beleži Pametna kartica z dvojnim dostopom, obe varianti s potrdilom na varnostnem modulu pa sta precej bolj izenačeni:



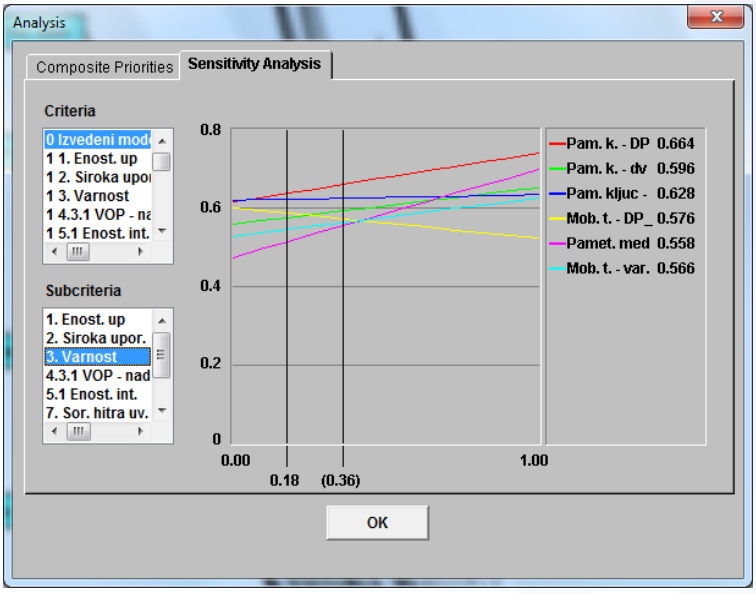
Slika 23 – Občutljivostna analiza za izvedbene možnosti - 1

Če utež za kriterij »Široka uporabnost« iz 0,19 povečamo na 0,38, so prve štiri variante (Mobilni telefon s potrdilom na SIM kartici, Pametna kartica, Pametni ključek in Mobilni telefon s potrdilom na varnostnem modulu) po rezultatih domala izenačene:



Slika 24 – Občutljivostna analiza za izvedbene možnosti - 2

Če utež za kriterij »Varnost« iz 0,18 povečamo na 0,36, tretji najboljši rezultat beleži Pametna kartica z dvojnim dostopom, variante z mobilnim telefonom oziroma s potrdilom na varnostnem modulu pa so precej bolj izenačene:



Slika 25 – Občutljivostna analiza za izvedbene možnosti - 3

6.2. Mnenje Zveze potrošnikov Slovenije

Zveza potrošnikov Slovenije poudarja (celotni dokument je v Prilogi E), da je s stališča uporabnosti storitev izjemno pomembno, da ima potrošnik za dostop do vseh javnih storitev (tako na državni kot občinski ravni) zgolj eno vstopno točko. ZPS predlaga, da se glede na vsebino elektronskih storitev omogočijo štiri ravni dostopa:

- povsem odprt dostop do osnovnih informacij, dokumentov, obrazcev,
- osnovna zaščita z uporabniškim imenom in geslom za dostop do večine obrazcev, pa tudi nekaterih osnovnih elektronskih storitev,
- varna zaščita s kvalificiranim digitalnim potrdilom za storitve, ki v realnem svetu zahtevajo osebno identifikacijo za okencem,
- varna zaščita z digitalnim podpisom za storitve, ki v realnem svetu zahtevajo osebno identifikacijo s podpisom.

Tehnično zahtevnejše rešitve torej zahtevata le zadnji dve ravni dostopa, pri čemer bi po mnenju ZPS morali upoštevati tudi sedanje stanje in izhajati iz sistema kvalificiranih digitalnih potrdil. Zagotoviti pa bi morali preprosto uporabo ne samo v računalnikih, pač pa tudi na prenosnih napravah, kot so tablični računalniki in pametni telefoni.

ZPS kot najboljšo rešitev za avtentikacijo in e-podpisovanje **predlaga uporabo mobilnih telefonov s centralnim HSM**, s takšno rešitvijo bi namreč najhitreje in z najmanj zapleti omogočili uporabo kvalificiranih digitalnih potrdil kar najširši javnosti, kar je, skupaj s preprosto zasnovo rešitve za dostop do elektronskih storitev javne uprave, glavni predpogoj, da bodo potrošniki te storitve tudi uporabljali.

6.3. Mnenje Združenja bank Slovenije

Storitve e-bančništva zagotovo sodijo med najbolj uporabne e-storitve. Vsekakor je zato smiselno pri kakršnihkoli nadaljnjih korakih in odločitvah pomembno upoštevati ključne dejavnike uspeha teh storitev in pri prenovi najti rešitve, ki bi bile čim širše uporabne tudi za ta pomemben sektor.

Glavne konkretne izkušnje posameznih bank v zvezi z e-identiteto so povezane s pametnimi karticami, ki jih že več kot deset let podpirajo in jih zato tovrstne razvojne zamisli tudi zanimajo.

Odbor za IT pri ZBS tako v svojem stališču (celotni dokument je v Prilogi F) **predlaga uveljavitev ene pametne kartice na nivoju države**, ki bi morala vsebovati funkcionalnosti PKI (hranjenje digitalnega potrdila, e-podpis), ki bi omogočala več-uporabnost - za identifikacijo, avtentikacijo in avtorizacijo tako pri uporabi storitev javnega kot tudi zasebnega sektorja. Identifikator na kartici bi moral biti sprejemljiv za vse subjekte, izdajala pa bi ga samo ena institucija. Tako izvedena e-identiteta bi morala biti sprejemljiva za (skoraj) vse namene. S stališča varnosti jim je bližje kontaktna različica kartice in kot primer navajajo poenoten koncept univerzalne pametne kartice, ki se uveljavlja v skandinavskih državah.

Odbor za IT pri ZBS **kot drugo možnost navaja možnost uporabe mobilnih naprav**, glede na njihovo vsesplošno prisotnost. Pri tej možnosti izpostavljajo uporabo WPKI ali podobne tehnologije, kjer se uporablja SIM kartica kot nosilec e-identitete. Tovrstna rešitev bi morala biti sprejemljiva za čim širši krog uporabnikov. Tudi pri tej rešitvi poudarjajo pomembnost vidika varnosti. Po mnenju medresorske skupine so te možnosti sicer kontradiktorne, saj je za široko uporabnost bolj sprejemljiva rešitev s centralnim HSM.

V zaključku stališča še navajajo, da bi za uveljavitev navedenih praktičnih možnosti moral biti zagotovljen zadosten pogoj in to je splošna sprejemljivost.

7. SKLEPNE UGOTOVITVE

Namen pričujoče analize je omogočiti izbiro najustreznejše rešitve, s katero bi povečali varnost uporabnikove e-identitete, omogočili kreiranje kvalificiranega podpisa, poenostavili delo z digitalnimi potrdili ter s tem elektronsko poslovanje še bolj približali državljanom. Cilji, ki smo si jih pri tem zadali (***enostavnost uporabe, široka uporabnost, zagotovljen visok nivo varnosti, zagotovljeno varstvo osebnih podatkov, enostavnost integracije, poenoteno upravljanje, sorazmerno hitra uvedba, sprejemljivi stroški***), sledijo namenu izboljšanja tega področja v Sloveniji in temeljijo tudi na trendih njegovega razvoja, saj se e-identiteta pogosto navaja kot temelj vseh e-storitev, tako v zasebnem kot tudi v javnem sektorju. Poleg tega mora razvoj tega področja v Sloveniji upoštevati tudi zahteve EU, kajti nemoteno opravljanje storitev med državami EU postaja eden poglavitnih ciljev vseh strateških dokumentov, sprejetih na ravni EU. V času priprave analize se je oblikoval tudi predlog za novo ureditev na ravni EU za področje različnih storitev, povezanih z e-podpisom in e-identifikacijo (»trust services«), ki jo bo potrebno upoštevati pri vpeljavi novih rešitev za upravljanje z e-identitetami.

Za pomoč pri analizi je bil pripravljen odločitveni model, ki je podrobno predstavljen v razd. 6.1.1., in na osnovi katerega so različne fokusne skupine ocenjevale posamezne rešitve v treh ločenih sklopih. Rezultati v nekaterih primerih odražajo pomanjkanje poznavanja področja s strani posameznih fokusnih skupin (predvsem s strani končnih uporabnikov in celo ponudnikov e-storitev), kar je posledica zahtevnosti področja in preslabega poznavanja posameznih rešitev, predvsem tistih, ki še niso v uporabi oz. razširjene v slovenskem prostoru npr. akreditirana e-identiteta, sektorski e-identifikator, rešitve s potrdilom na varnostnem modulu (podrobno o tem v razd. 6.1.2). Pri končnih usmeritvah je tako potrebno upoštevati tudi druge podlage, zunanja mnenja, mnenje strokovnjakov in trende, ki jih z odločitvenim modelom ni moč ovrednotiti.

Zaključek analize temelji na različnih podlagah, in sicer upošteva:

- 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 (ZPS),
- mnenje predstavnikov ponudnikov e-storitev iz zasebnega sektorja (ZBS),
- zunanje pravno mnenje,
- mnenje medresorske delovne skupine,
- predlog nove uredbe v zvezi z e-podpisom, e-identifikacijo in e-avtentikacijo in drugih tovrstnih storitev na ravni EU,
- najnovejše usmeritve v drugih državah (Švedska, Avstrija) in
- izsledke izvajanja EU projekta STORK.

V nadaljevanju so podani zaključki za vse tri sklope analize.

Sklop 1: pravne možnosti e-identitet

Za prvi sklop se bile identificirane tri možnosti (podrobno so predstavljene v poglavju 3), in sicer:

1. e-osebna izkaznica
2. akreditirana e-identiteta
3. kvalificirana digitalna potrdila

Osebna izkaznica, kot jo poznamo danes, omogoča državljanom, da jo uporabljajo za izkazovanje svoje istovetnosti doma in v tujini. Državljani imajo do osebne izkaznice spoštljiv odnos, saj predstavlja vsakega posameznika in njegovo pripadnost državi. Državljani pri postopkih hranjenja in obdelave osebnih podatkov običajno svoji državi zaupajo bolj kot komercialnim ponudnikom storitev na trgu. E-osebna izkaznica v smislu kombinacije klasičnega osebnega identifikacijskega dokumenta opremljenega tudi z ustreznimi sredstvi za možnost varne e-avtentikacije in e-podpisa bi tako bila le dodana vrednost obstoječi osebni izkaznici, saj se državljani z njo ne bi identificirali le v fizičnem svetu temveč tudi v elektronskem. Uporabo e-osebne izkaznice bi po vzoru nekaterih drugih držav lahko razširili tudi na njeno uporabo v vsakodnevnih postopkih, kot npr. e-bančno poslovanje, evidentiranje prihoda v službo, avtomatsko izpolnjevanje obrazcev na uradniških okencih, izposoja mestnega kolesa, vožnja z mestnim avtobusom, možnost nakupa alkoholnih in tobačnih izdelkov na avtomatih, kjer je pogoj polnoletnost idr.

Glede na rezultate vrednotenja odločitvenega modela se kot **najprimernejša izbira izkaže prav e-osebna izkaznica. Dosega najboljše rezultate predvsem pri fokusnih skupinah iz javnega sektorja, medtem ko se predstavniki zasebnega sektorja bolj nagibajo k trenutni situaciji, kjer imamo na voljo različne ponudnike kvalificiranih digitalnih potrdil. Ta rešitev ne prinaša nobenih novosti glede prenove e-identitet v smislu večje pravne urejenosti, zato odločitev zanjo ni smotrna** in sta v nadaljevanju podrobneje obravnavani samo možnosti e-osebne izkaznice in akreditirane e-identitete.

E-osebna izkaznica bi v naše poslovanje prinesla številne prednosti in bi izpolnila veliko zastavljenih ciljev:

- ne bi bilo potrebe po večjih prilagoditvah aplikacij, saj gre za poznan koncept, ki temelji na kvalificiranih digitalnih potrdilih,
- povečalo bi se zavedanje in zaupanje uporabnika, saj bi bila e-identifikacija na uradnem identifikacijskem dokumentu,
- za uporabnika predstavlja razumljivo in sprejemljivo rešitev (isti dokument se uporablja za identifikacijo v fizičnem in elektronskem svetu),
- ob izvedeni predhodni presoji vplivov na varstvo osebnih podatkov in ustrezni izvedbi zagotavlja visok nivo varnosti e-identitete,
- omogoča uporabo standardizirane naprave za varno tvorjenje podpisa.

Ker bi e-osebna izkaznica vključevala le potrdila enega overitelja, bi njena uvedba postopno lahko povzročila izločitev drugih overiteljev, zato s tega vidika e-osebna izkaznica ni najbolj priporočljiva rešitev. Tudi po stroškovni, zakonodajni in nenazadnje organizacijski plati je njena

uvedba najbolj zahtevna. Primer Finske, ki je bila ena izmed prvih držav z e-osebno izkaznico, nas opozarja tudi na nevarnost, da je uvedba in uporaba e-osebne izkaznice neuspešna, če se le-ta ne uporablja tudi na drugih področjih e-storitev, ki jih državljani najpogosteje potrebujejo, kot je npr. e-bančništvo ipd. Združenje bank Slovenije sicer podpira uvedbo ene same pametne kartice in kot eno izmed možnosti navaja prav e-osebno izkaznico.

Na uspešnost uvedbe e-osebne izkaznice vsekakor vpliva tudi način in premišljenost same uvedbe. Uvedba e-osebne izkaznice je bila v slovenskem prostoru že večkrat neuspešno pričet projekt, v večini primerov je bil razlog za zaustavitev politične narave (povezano sicer tudi z visokimi stroški uvedbe), zadnji poskus iz leta 2008 pa je bil zaustavljen tudi zaradi načrtov za vzpostavitev multifunkcijske kartice in posledičnega združevanja različnih identifikacijskih številk na enem mestu brez izvedene predhodne presoje vplivov na varstvo osebnih podatkov, kar je povzročilo številne pomisleke z vidika varstva osebnih podatkov. Kot smo izpostavili v poglavju 4, pa je s pravočasno izvedbo predhodne presoje vplivov na varstvo osebnih podatkov mogoče doseči tudi višjo raven varstva osebnih podatkov.

Uvedba akreditirane e-identitete bi poenostavila vzpostavitev višjega nivoja urejanja e-identitet in omogočila akreditacijo tudi drugih, z e-identitetami povezanih storitev. Čeprav ta možnost v odločitvenem modelu ni najbolje ocenjena (razlike so sicer zelo majhne, v fokusih skupinah iz javnega sektorja se je celo skoraj izenačila z rezultati, ki jih je dosegla e-osebna izkaznica), **po mnenju medresorske delovne skupine omogoča bistveno boljšo pravno urejenost področja e-identitet kot kvalificirana digitalna potrdila in bolje sledi trendom in nenazadnje pravnim zahtevam, ki se nam obetajo na ravni EU**. Že v odločitvenem modelu je dosegla najboljše rezultate prav pri doseganju cilja glede varstva osebnih podatkov. Razlog za njeno slabšo uvrstitev gre v splošnem pripisati odsotnosti instrumenta akreditacije v slovenskem prostoru, kot ga predvideva ZEPEP za namene e-podpisa. Po mnenju medresorske delovne skupine pa ta oblika ni edina možna oblika akreditacije oz. bi bilo potrebno njene pristojnosti razširiti tudi na druga področja, povezana z e-identifikatorji za potrebe e-storitev. Razširjene pristojnosti akreditacije predvideva tudi predlog nove uredbe na tem področju na ravni EU, ki postavlja zahteve glede medsebojnega priznavanja in sprejemanja e-identitet med državami EU ter uvaja naslednje t.i. »zanesljive storitve« (»trust services«), ki bodo s to dodatno regulativo dobile pravno veljavnost in ureditev: elektronski žigi (»e-seals«), časovni žigi, varno e-vročanje, e-dokumenti, avtentikacija spletnih mest.

V Sloveniji tudi nimamo vzpostavljenih ustreznih organizacij in postopkov za presojanje ustreznosti naprav za varno e-podpisovanje, kar pa je pomembno z vidika zagotavljanja kvalificiranih e-podpisov. Nadalje bo nova regulativa uredila tudi različne nivoje zaupanja, kar je za področje e-avtentikacije na podlagi obstoječih rešitev po državah članic uvedel projekt STORK (glej razd. 2.4.1). Različnim nivojem so naklonjeni tudi na Zvezi potrošnikov Slovenije, kjer predlagajo štiri različne nivoje glede na vsebino e-storitev. Naštete vidike najenostavneje uredi oblika predlagane akreditirane e-identitete.

Če primerjamo e-osebno izkaznico in akreditirano e-identiteto, je slednja primernejša oblika prenove tega področja v slovenskem prostoru. Bistvene prednosti, ki jih prinaša v primerjavi z e-osebno izkaznico, so sledeče:

- manjša je odvisnost od politične podpore,
- odločitev za e-osebno izkaznico precej omeji nabor primernih izvedbenih možnosti (npr. ni možnosti izvedbe z mobilnimi napravami)
- z akreditacijo se lahko uvede in uredi različne nivoje zaupanja, e-osebna izkaznica pa omogoča zgolj samo najvišji nivo varnosti,
- nediskriminatornost do overiteljev na trgu,
- manj posega v obstoječe rešitve, kjer lahko uporabniki tudi za storitve e-uprave uporabljajo e-identitete, izdane s strani zasebnega sektorja,
- akreditirana e-identiteta ne ovira oz. izključuje morebitne kasnejše uvedbe e-osebne izkaznice.

Ne glede na to, katera izmed rešitev bo izbrana, pa bo v obeh primerih treba načrtovati različne ukrepe, ki jih bo potrebno izvesti pri sami implementaciji rešitve. Potrebni ukrepi so sledeči:

- ureditev pravnega okolja (sprememba ustrezne zakonodaje),
- organizacijski ukrepi (vzpostavitev instrumenta akreditacije v primeru akreditirane e-identitete, vzpostavitev in stalno tesno sodelovanje med različnimi institucijami v primeru e-osebne izkaznice),
- usklajenost konkretne izvedbe z različnimi možnostmi Sklopa 2 in Sklopa 3,
- izvedba presoje vplivov na varstvo osebnih podatkov,
- izvedba presoje informacijske varnosti,
- prilagoditev in upoštevanje smernic na ravni EU, dognanj projekta STORK ipd.

Sklop 2: modeli identifikatorjev

Za drugi sklop je bilo identificiranih pet različnih možnosti (podrobnosti v poglavju 4), pri čemer je potrebno poudariti, da za posamezno možnost obstaja več različnih izvedb, zato je pred uveljavitvijo kakršnekoli rešitve potrebno podrobneje proučiti in ovrednotiti njeno konkretno izvedbeno različico:

1. uradni osebni identifikator v digitalnem potrdilu,
2. uradni osebni identifikator v zalednem sistemu overitelja,
3. e-identifikator osebe v digitalnem potrdilu,
4. e-identifikator osebe v zalednem sistemu overitelja,
5. sektorski e-identifikatorji.

Prva dva modela odražata obstoječe stanje v Sloveniji. **Nekateri overitelji v skladu s prvim modelom namreč v digitalno potrdilo vključijo davčno številko imetnika.** Po rezultatih vrednotenja na podlagi odločitvenega modela je ta rešitev pričakovano tudi najbolj zaželena na strani ponudnikov storitev, saj predstavlja najenostavnejšo uporabo e-identitet pri avtentikaciji. Je pa z vidika varstva osebnih podatkov in varnosti najmanj zaželena. V nekaterih obstoječih rešitvah so digitalna potrdila celo javno objavljena v imenikih digitalnih potrdil, kar pomeni tudi javno objavo enoličnih identifikatorjev, v tem primeru davčne številke imetnika, kar gotovo ni prijazno z vidika varstva osebnih podatkov. Poleg tega je v tem primeru davčna

številka imetnika razvidna tudi iz vsakega elektronsko podpisanega dokumenta, saj je zaradi enostavnejše verifikacije podpisa digitalno potrdilo običajno dodano samemu elektronskemu podpisu. Zaradi vsega zgoraj navedenega **te možnosti tako ni mogoče predlagati kot priporočljive rešitve za potrebe identifikacije imetnika digitalnega potrdila oz. e-identitete in je izločena iz nadaljnje obravnave.** Drugi model se uporablja pri digitalnih potrdilih, ki jih izdaja overitelj na MPJU, saj vključujejo dodatno serijsko številko, ki je v namenski prevajalni tabeli povezana s pripadajočimi obstoječimi identifikatorji imetnika (EMŠO, davčna številka). Taka rešitev je prijaznejša z vidika varstva osebnih podatkov in same varnosti, je pa njena uporaba nekoliko zahtevnejša za ponudnike storitev, zahteva pa tudi določene pravne, organizacijske in tehnične ukrepe, ki omogočajo dostop do prevajalne tabele za potrebe avtentikacije imetnikov potrdil tako za ponudnike storitev v javnem kot tudi v zasebnem sektorju.

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 (deloma in za potrebe osebnih dokumentov to pravno podlago že omogoča 28. člen ZEPEP) in njegovo umestitev v primeren obstoječ register (predvidoma Centralni register prebivalstva) ter vzpostavitev ustrezne prevajalne tabele v primeru odločitve za izvedbo modela 4, ki predvideva shranjevanje novega identifikatorja v zalednem sistemu. **Uvedba kateregakoli izmed obeh modelov bi močno vplivala na ponudnike obstoječih e-storitev, saj bi zahtevala prilagoditev le-teh na nov način avtentikacije**. Uvedba novega e-identifikatorja bi povzročila nekaj sprememb tudi pri overiteljih, saj bi zahtevala vzpostavitev organizacijskih in tehničnih pogojev za dostop do e-identifikatorja osebe pri izdaji digitalnega potrdila, potrebne pa bi bile tudi spremembe politik delovanja overiteljev z namenom izdajanja novih vrst digitalnih potrdil. Uvedbo novega e-identifikatorja v svojem mnenju sicer ne izključuje tudi Združenje bank Slovenije.

Največ sprememb bi vnesla odločitev za sektorske e-identifikatorje, ki so sicer zgled dobre prakse pri spoštovanju varstva osebnih podatkov pri e-poslovanju. Gre za koncept, ki ga so ga uvedli in uspešno implementirali v Avstriji. Model preprečuje kakršnokoli povezovanje identifikatorjev med različnimi sektorji uporabe, kljub temu, da se v njihovem primeru za vse storitve uporablja enotna rešitev e-identitete, t.i. »Burgerkarte«. **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 je izbira te možnosti nesmotrna in je izločena iz nadaljnje obravnave.** Uvedba bi namreč povzročila precejšnje spremembe v načinu avtentikacije in zahtevala obsežne organizacijske, pravne in tehnične spremembe.

Po rezultatih vrednotenja na podlagi odločitvenega modela je bila najvišje ocenjena možnost, ki predvideva uporabo obstoječega osebnega identifikatorja v zalednem sistemu, medresorska delovna skupina pa je še nekoliko bolje ocenila možnost z namenskim e-identifikatorjem, prav tako v zalednem sistemu overitelja. Kljub temu, da je ta rešitev ugodnejša z vidika varnosti in varstva osebnih podatkov, pa se pri primerjavi obeh variant, ki se zanašata na zaledni sistem, kot primernejša izkaže rešitev z obstoječim identifikatorjem, saj uvedba dodatnega e-identifikatorja pomeni preveč novih zahtev tako na strani overiteljev kot in predvsem na strani

ponudnikov storitev, ki bi morali svoje informacijske sisteme prilagoditi, tako da bi namesto na obstoječih identifikatorjih (npr. davčni številki) temeljili na novem e-identifikatorju. 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**.

Sklop 3: izvedbeni modeli e-identitet

Izvedbene možnosti za naprave za varno tvorjenje e-podpisa zaradi hitrega razvoja tega področja poleg že znanih možnosti prinašajo tudi precej novosti. V analizi smo zajeli tako uveljavljene rešitve (npr. pametna kartica s kontaktnim čipom) kot tudi rešitve, ki so manj razširjene oziroma so se pojavile v zadnjem času (npr. pametna kartica z dvojnim dostopom, mobilne rešitve, rešitve s potrdilom na varnostnem modulu). Medsebojno smo primerjali naslednje možnosti, ki so podrobneje predstavljene v poglavju 5:

1. pametna kartica:
    - pametna kartica s kontaktnim čipom,
    - pametna kartica z brezkontaktnim čipom,
    - pametna kartica s čipom z dvojnim dostopom (kontaktni in brezkontaktni),
    - pametna kartica z brezkontaktnim in kontaktnim čipom,
2. pametni ključek,
3. centralni HSM z močno avtentikacijo,
4. uporaba mobilnih telefonov:
    - model WPKI,
    - model s centralnim HSM.

Rešitev s pametnimi karticami je najstarejši in gotovo najbolj uveljavljen način za zagotavljanje zanesljive avtentikacije uporabnikov in kvalificiranih digitalnih podpisov. Na voljo so v različnih izvedbah, ki so lahko bolj ali manj primerne, odvisno od zahtev in potreb v konkretnem primeru. Najbolj so razširjene pametne kartice s kontaktnim čipom, za uporabo katerih potrebujemo ustrezen čitalnik in programsko opremo (medprogramje). Na voljo in v zadnjem času vedno bolj razširjene so tudi brezkontaktne pametne kartice, ki v primerjavi s kontaktnimi ne zahtevajo vstavljanja kartice v čitalnik, saj zadostuje že, če kartico dovolj približamo čitalniku. To po eni strani predstavlja lažjo uporabo za imetnike, po drugi strani pa je uporaba tovrstnega načina načeloma manj varna, saj zahteva izvedbo dodatnih varnostnih ukrepov z namenom preprečevanja nepooblaščenega dostopa. Enako kot pri kontaktni različici tudi pri brezkontaktni potrebujemo ustrezno programsko opremo in čitalnik brezkontaktnih kartic, ki zaradi svoje višje cene to možnost prikaže kot manj primerno za zasebno rabo. Poleg tega je ta tehnologija zaenkrat še manj razširjena, v večjem obsegu se uveljavlja npr. v Nemčiji, kjer so l. 2010 pričeli z izdajanjem e-osebnih izkaznic na kartici z brezkontaktnim čipom, v letu 2011 pa so s podobnim projektom pričeli tudi na Poljskem. Poleg kartic z zgolj kontaktnim in brezkontaktim čipom obstajajo tudi izvedbe z obema čipoma oziroma z dvojnim dostopom do enega čipa. Njihova prednost je predvsem ta, da omogočajo uporabo obeh tipov čitalnikov. Na tržišču so na voljo tudi pametni ključki, katerih prednost je v tem, da vsebujejo že integriran

čitalnik, za uporabo katerega pa je še vedno potrebno zagotoviti ustrezno programsko podporo.

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.

Razvoj in množična uporaba mobilnih telefonov, tabličnih računalnikov in drugih mobilnih naprav nas po drugi strani usmerja k vpeljavi postopkov elektronskega poslovanja, ki vključujejo tovrstne naprave bodisi kot nosilce zasebnih ključev bodisi kot naprave, ki omogočajo dostop do zasebnih ključev na centralnem varnostnem modulu. **Mobilne naprave bi 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.** Uporabo teh medijev za tovrstne storitve spodbujata tudi Zveza potrošnikov Slovenije in Združenje bank Slovenije. Tovrstna uporaba mobilnih telefonov se uspešno uveljavlja npr. v Estoniji in Avstriji, ki sta sicer zgleden primer držav z uveljavljenimi enotnimi e-identitetami, v primeru Estonije klasične e-osebne izkaznice v povezavi z mobilnimi e-identitetami in v primeru Avstrije enotne »Burgerkarte«. Po izkušnjah obeh držav je razmah uporabe mobilnih naprav v porastu, v Avstriji pa ta način uporabe celo vzpodbujajo pred klasičnim, torej s pametnimi karticami. O omogočanju e-avtentikacije in kvalificiranih e-podpisov razmišljajo tudi druge države, kot npr. Švedska, Moldavija, Romunija. Po podatkih analize iz programa IDABC iz l. 2009 je takrat v EU že 6 držav uporabljalo mobilne telefone za e-podpis in e-avtentikacijo.

Pri analizi rezultatov vrednotenja smo ugotovili, da lahko **z vidika ciljev različne rešitve v grobem združimo v dve skupini in sicer na rešitve z dig. potrdilom na pametnem mediju ter na rešitvi z dig. potrdilom na varnostnem modulu**, saj je taka delitev bolj ali manj očitna pri večini zastavljenih ciljev. Če upoštevamo predstavljene prednosti in slabosti posameznih izvedb, **se izmed rešitev z dig. potrdilom na pametnem mediju kot najbolj primerna izbira izkaže pametna kartica s kontaktnim čipom**. Nenazadnje je bila ta rešitev najbolje ocenjena pri vrednotenju na podlagi odločitvenega modela, kot najbolj primerno možnost pa jo je izbrala tudi medresorska delovna skupina. Morebitna odločitev za pametno kartico z dvojnim dostopom ali dvojnim čipom je smiselna le v primeru konkretnih potreb, povezanih z brezkontaktnim dostopom, in če ta dodatna funkcionalnost odtehta pomisleke v zvezi z varnostjo in varstvom osebnih podatkov pri tej rešitvi.

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 dig. potrdilom na pametnem mediju**, zahteva pa podrobnejšo analizo potrebnih ukrepov za njeno morebitno vzpostavitev. Poleg tega je pri analizi rezultatov potrebno upoštevati tudi dejstvo, da so sorazmerno nizke ocene za mobilne rešitve in rešitve z varnostnim modulom, podane s strani fokusnih skupin, gotovo tudi posledica novosti in nepoznavanja teh rešitev, predvsem v primeru ocenjevanja s strani končnih uporabnikov. Kot je razvidno iz zunanjega pravnega mnenja o ustreznosti modelov s centralnim HSM (glej razd.

5.2), je z vidika pravne veljavnosti ta rešitev enakovredna rešitvam z dig. potrdilom na pametnem mediju, kar dokazuje tudi uporaba tovrstne rešitve v Avstriji, kjer imajo, za razliko od Slovenije, vzpostavljen tudi institut za presojanje ustreznosti naprav za varno e-podpisovanje, v okviru katerega je bila potrjena ustreznost uporabljene mobilne rešitve z varnostnim modulom. Ta rešitev je kot najprimernejša predstavljena tudi v mnenju ZPS, saj ne zahteva menjave kartic SIM ter sodelovanja med operaterji mobilne telefonije, kot je to potrebno v primeru sistema WPKI, s takšno rešitvijo pa bi po njihovem mnenju najhitreje in z najmanj zapleti omogočili uporabo kvalificiranih digitalnih potrdil kar najširši javnosti.

Uporaba mobilnega telefona z varnostnim modulom omogoča tudi nadgradnjo rešitve v povezavi z vzpostavitvijo centralne storitve avtentikacije, ki je kot skupni gradnik predvidena v Akcijskem načrtu elektronskega poslovanja javne uprave**.** Na nivoju te centralne storitve bo namreč 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.** V tem primeru je uporabniška izkušnja povsem primerljiva tisti, pri kateri uporabnik dejansko podpisuje z uporabo svoje pametne kartice. Podoben pristop bodo v kratkem implementirali na Švedskem, tovrstna razširitev pa je zanimiva tudi v primeru vzpostavitve akreditirane e-identitete z različnimi nivoji zaupanja, kjer bi bilo možno poleg rešitev za kvalificirano podpisovanje (mobilni telefoni, pametne kartice) podpreti tudi v Sloveniji trenutno najbolj uporabljeno rešitev za avtentikacijo t.j. uporabo kvalificiranega digitalnega potrdila v spletnem brskalniku. Takšna avtentikacija bi omogočala elektronsko podpisovanje na nekoliko nižjem nivoju (napreden elektronski podpis, overjen s kvalificiranim dig. potrdilom), ki se v Sloveniji zaenkrat daleč najpogosteje uporablja.

SEZNAM PRILOG

A. Pravna ureditev varnih e-identitet; Inštitut za ekonomijo, pravo in informatiko; avgust 2011

B. Skladnost hrambe zasebnih ključev na strojnem varnostnem modulu z direktivo 1999/93/ES in slovensko zakonodajo; Inštitut za ekonomijo, pravo in informatiko; avgust 2011

C. Razvoj odločitvenih modelov za vrednotenje različnih možnosti uvedbe e-identitet; Fakulteta za upravo; maj 2012

D. Rezultati vrednotenja odločitvenih modelov; Ministrstvo za pravosodje in javno upravo, junij 2012

E. Mnenje ZPS o primernem načinu prenove e-identitet; Zveza potrošnikov Slovenije; januar 2012

F. Stališče Odbora za IT pri Združenju bank Slovenije do prihodnjega razvoja e-identitet; Združenje bank Slovenije; februar 2012