UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Diplomsko delo
univerzitetnega programa

POMEN UPRAVLJANJA IDENTITETE POSAMEZNIKA V POGOJIH ELEKTRONSKE UPRAVE

Mojca Subotić

Ljubljana, junij 2009

UNIVERZA V LJUBLJANI
FAKULTETA ZA UPRAVO

Diplomsko delo
univerzitetnega programa

POMEN UPRAVLJANJA IDENTITETE POSAMEZNIKA V POGOJIH ELEKTRONSKE UPRAVE

Kandidatka: Mojca Subotić
Številka indeksa: 04035128

Mentor: dr. Mirko Vintar

Ljubljana, junij 2009

POVZETEK

Diplomska naloga obravnava elektronsko upravo in z njo povezano področje upravljanja identitet posameznikov. Elektronska uprava prinaša hitrejši, enostavnejši in kakovostnejši način poslovanja v upravi. Temeljni cilj in pogoj za njeno uspešno delovanje je visoka stopnja varovanja tako uporabnikov elektronskih storitev kot samih dokumentov. Upravljanje identitet posameznikov je področje, ki ima ključni pomen pri odpravljanju napak, povezanih s sistemom varovanja pri samem nastanku in hrambi dokumentov in tudi pri procesu identifikacije uporabnikov. V diplomskem delu predstavljam področje upravljanja identitet posameznikov kot ključ do uspešnega elektronskega poslovanja v upravi in tehnološke rešitve na podlagi pametne kartice, elektronskega podpisa in z njim povezane infrastrukture javnih ključev ter biometrične podatke. Kot primer upravljana identitet posameznikov v pogojih elektronske uprave pa predstavljam projekte elektronske osebne izkaznice v izbranih državah: Španija, Italija, Estonija in Slovenija.

Ključne besede: E-uprava, upravljanje identitet posameznikov, elektronski podpis, infrastruktura javnega ključa, pametne kartice, biometrični podatki, elektronske osebne izkaznice.

SUMMARY

This graduation paper is addressing electronic government and with it related area of digital identitiy management. Electronic government brings on quicker, simpler and better type of management. Basic goal as well as condition for its success is a high level of security regarding both, users and documents involved in electronic services. Digital identity management is essential at rectification of errors connected to security system at origination and safe-keeping of documents and during the users' identification process. This paper is presenting the area of digital identity management as the key to successful electronic operations in government and thechnological solutions based on smart card, electronic signatures, public keys infrastructures and biometric data. As the examples of individuals' identities management in electronic government, projects of electronic identity card in chosen countries, being Spain, Italy, Estonia and Slovenia are presented.

Key words: E-goverment, digital identity management, electronic signature, public key infrastructure, smart cards, biometric data, electronic identity cards.

KAZALO

POVZETEK ii
SUMMARY III
1 UVOD 1
1.1 OPREDELITEV PROBLEMA 1
1.2 NAMEN IN CILJI 1
1.3 METODE RAZISKOVANJA 2
1.4 VSEBINA PO POGLAVJIH 2
2 ELEKTRONSKO POSLOVANJE 3
2.1 ELEKTRONSKA UPRAVA 3
2.2 ELEMENTI RAZVOJA ELEKTRONSKE UPRAVE V SLOVENIJI 5
2.2.1 Dosežki slovenske e-uprave v primerjavi z drugimi državami 7
2.3 E-UPRAVA V EVROPSKI UNIJI 8
2.3.1 Cilji e-uprave s strani Evropske unije 8
2.4 PODROČJE VARNOSTI 9
3 UPRAVLJANJE IDENTITET POSAMEZNIKA KOT KLJUČ DO USPEŠNEGA ELEKTRONSKEGA POSLOVANJA 10
3.1 POMEN UPRAVLJANJA Z IDENTITETAMI V ELEKTRONSKI UPRAVI 11
3.2 PREDSTAVITEV MOŽNOSTI TEHNOLOŠKIH REŠITEV NA PODLAGI PAMETNE KARTICE 12
3.3 ELEKTRONSKI PODPIS, TEMELJ ELEKTRONSKEGA POSLOVANJA 14
3.3.1 Infrastruktura javnih ključev 15
3.3.2 Sestavni deli infrastrukture javnih ključev 17
3.4 TEHNOLOŠKE REŠITVE NA BAZI BIOMETRIJE 19
3.4.1 Zakonodaja na področju biometrije 20
3.4.2 Biometrični podatki 21
3.5 UPRAVLJANJE IDENTITET, POGLED EVROPSKE UNIJE 24
3.5.1 Pojav velikega brata 26
4 PRIMERI UPRAVLJANJA IDENTITET POSAMEZNIKA V IZBRANIH DRŽAVAH 28
4.1 ELEKTRONSKA OSEBNA IZKAZNICA 28
4.2 PRIMERI ELEKTRONSKE OSEBNE IZKAZNICE V ŠPANIJI 29
4.2.1 Veljavnost izkaznice 30
4.2.2 Pravne podlage 30
4.2.3 Proces izdaje osebne izkaznice 30

4.2.4 Vrste mehanizmov, operacijskih sistemov in standardov, ki podpirajo elektronsko osebno izkaznico 31
4.3 PRIMER ELEKTRONSKE OSEBNE IZKAZNICE V ITALIJI 31
4.4 PRIMER ELEKTRONSKE OSEBNE IZKAZNICE V ESTONIJI 32
4.5 SLOVENSKA ELEKTRONSKA OSEBNA IZKAZNICA 33
5 ZAKLJUČEK 37
LITERATURA 39
VIRI 41
IZJAVA O AVTORSTVU IN NAVEDBA LEKTORJA 44

1 UVOD

Prehod na informacijsko družbo je spremenil način delovanja in poslovanja javne uprave. Pojav interneta, elektronske pošte in novih informacijsko-komunikacijskih tehnologij je povzročil proces reforme uprave. Reforma je usposobila upravo na način, ki ji omogoča izkoriščanje priložnosti, ponujenih s strani novo nastale družbe. S tem je razvila hitrejši in enostavnejši način poslovanja ter dostop do informacij in storitev.

1.1 OPREDELITEV PROBLEMA

Elektronsko poslovanje v upravi prinaša veliko prednosti in na splošno izboljšanje same uprave. Storitve so kakovostnejše, poslovanje hitrejše, sama odgovornost in učinkovitost pa sta zasnovani na višji stopnji. Skrajšajo se čakalne dobe, znižajo se stroški poslovanja in vzpostavi se povezanost med organi, ki predstavlja zmanjšanje obremenitev za uporabnike. Vendar pa neustrezna implementacija elektronske uprave v družbo s seboj prinaša veliko problemov.

Eden temeljnih problemov je varnost. Potreba po visoki stopnji varovanja je temeljni pogoj za uspešnost elektronske uprave. Sistem kot celoto in z njim povezane podatke, dokumente in identitete uporabnikov je treba zavarovati. Neustreznost in nerazvitost sistemov varovanja tako pri nastajanju kot pri obdelovanju, shranjevanju in prenosu podatkov prinaša nezaupanje v tak sistem. Možnost vdorov v sisteme in kraja identitet znižujeta povpraševanje po elektronskih storitvah. Strah in nezaupanje uporabnikov v nove tehnologije pomeni korak nazaj v industrijski družbi, zavira novosti in nadgraditve samega sistema elektronskega poslovanja.

Razvoj elektronske uprave je tudi eden temeljnih ciljev Evropske unije, saj pomeni povečanje stopnje konkurenčnosti storitev uprav in sposobnost prostega pretoka informacij, podatkov in dokumentov preko držav članic. Problem, ki nastaja, se nanaša na nesposobnost sistemov pri prepoznavanju podatkov in identitet uporabnikov, ki so nastali v eni državi, želijo pa se uporabljati tudi v drugih. Ni vzpostavljene dovolj dobre povezave med sistemi in to povzroča zaviranje razvoja e-uprave na nivoju Unije.

1.2 NAMEN IN CILJI

Namen diplomskega dela je predstavitev področja, imenovanega »digital identity management« oziroma elektronsko upravljanje identitet in njegovo povezavo z elektronskim poslovanjem v upravi.

Je področje, ki ima ključni pomen pri odpravljanju napak, povezanih s sistemi varovanja. Njegova implementacija in uporaba sta preprosti, a kljub temu omogoča zelo visoko stopnjo varovanja same identitete ter vseh podatkov in dokumentov povezanih z njo. Orodja, ki sestavljajo sistem upravljanja identitet, omogočajo kakovostno in unikatno identifikacijo lastnika identitete. Onemogočajo vdore vanjo in

posledično spreminjanje, brisanje ali uporabljanje podatkov in dokumentov. Ima sposobnost vgraditve varnostnega ventila v sisteme, preko katerih se posluje, tako da zavaruje vsakega uporabnika posebej in s tem onemogoča vdor nepooblaščenim osebam.

Je področje, na katerega daje Evropska unija veliko poudarka tako z vidika varovanja kot z vidika lažjega poslovanja med državami članicami. Povezavo med elektronskim poslovanjem uprave in »digital identity managementom« predstavlja elektronska osebna izkaznica kot identifikacijski dokument, preko katerega se lahko varno dostopa do storitev e-uprave. Elektronska osebna izkaznica je ena izmed možnosti, kako elektronsko poslovanje poenostaviti kljub visokemu varovanju uporabnikov in ponudnikov storitev, ki temelji na sistemu upravljanja z identitetami.

1.3 METODE RAZISKOVANJA

V diplomskem delu bom obravnavala področje upravljanja identitet v pogojih elektronske uprave. Prikazala bom elemente elektronske uprave in upravljanja identitet, povezave med njima in primer elektronske osebne izkaznice kot temeljnega projekta, ki povezuje obe področji: elektronsko poslovanje v upravi in upravljanje z identitetami. Uporabila bom metodo deskripcije, s pomočjo katere bom opisovala dejstva, procese in pojave, ki zajemajo elektronsko poslovanje in identitete. Metodi kompilacije in komparacije pa bosta uporabljeni na področjih upravljanja identitet v elektronskem poslovanju na stopnji Evropske unije ter pri opisovanju projektov elektronske osebne izkaznice v izbranih državah.

1.4 VSEBINA PO POGLAVJIH

V prvem poglavju je opisano področje elektronskega poslovanja in elektronske uprave v Sloveniji in Evropski uniji. Drugo poglavje opredeljuje upravljanje identitet posameznika kot ključ do uspešnega elektronskega poslovanja, s poudarkom na pomenu upravljanja identitet v elektronski upravi, orodjih, ki omogočajo upravljanje identitet, in na pogledih Evropske unije. Zadnje poglavje prikazuje primere upravljanja identitet posameznika v izbranih državah. Poudarek je na elektronski osebni izkaznici in na primerih elektronske izkaznice v izbranih državah, vključno s projektom nove osebne izkaznice, ki ga izpeljuje Slovenija.

2 ELEKTRONSKO POSLOVANJE

Elektronsko poslovanje je poslovanje v elektronski obliki, ki za svoje delovanje uporablja oziroma potrebuje informacijsko-komunikacijsko tehnologijo. Internet ima glavno vlogo, saj predstavlja temelj elektronskega poslovanja. Preko računalniškega omrežja lahko s pomočjo elektronskega poslovanja prodajamo, nabavljamo, izmenjujemo podatke, storitve in tudi izdelke. Lahko bi tudi rekli, da gre za brezpapirno poslovanje oziroma za različne oblike poslovnih transakcij, ki potekajo na elektronski način preko neosebnega stika. »Uspeh e-poslovanja je v tem, da ob nizkih stroških ustvarjamo dodatno vrednost, ki jo skozi nadaljnji proces čim bolj povečujemo (Center vlade za informatiko, 2001, str. 154).«

Taka oblika poslovanja se lahko uporablja na različnih področjih: v najrazličnejših poslovnih procesih in v javni upravi. Spekter delovanja elektronske uprave lahko širše opredelimo kot možnost sodelovanja in komuniciranja med poslovnimi partnerji, izvajanje raznovrstnih transakcij, trgovanje, vzpostavitev poslovnih procesov itd.

Cilj e-poslovanja je elektronsko izmenjevanje podatkov. Področja, na katerih se lahko razvija in uporablja, so zelo raznolika (storitve, blago, plačevanje, prodaja, delovanje državnih organov in javnih služb itd.). Udeleženci procesa izmenjave in posredovanja podatkov oziroma dokumentov so lahko podjetja, državne službe in tudi posamezniki.

Elektronsko poslovanje v Sloveniji opredeljuje Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP). Bistveni pomen zakona je, da elektronskemu podpisu daje enako veljavo kot lastnoročnemu. Temelji na naslednjih načelih: načelo varstva osebnih podatkov, načelo nediskriminacije elektronske oblike, načelo mednarodnega priznavanja, varstva potrošnikov in drugih. Zakon v celoti sledi evropskim usmeritvam.

2.1 ELEKTRONSKA UPRAVA

»E-uprava je uprava, katere celotno delovanje temelji na uporabi elektronskih dokumentov, e-poslovanja in interneta v njenem notranjem in zunanjem poslovanju, uvajanju novih sistemskih in organizacijskih rešitev ter novih modelov upravljanja.« (Vintar in Grad, 2004, str. 5). Glavni namen je izboljšava storitev na področju uprave preko uporabe interneta in elektronskega poslovanja. To pomeni, da bodo lahko občani, podjetja in ostali nevladni sektorji, ko bo elektronska uprava v resnici delovala, večino uradnih zadev, dovoljenj in dokumentov pridobili preko svojega računalnika oziroma interneta, interaktivnih kioskov, mobilnih telefonov in drugih naprav (glej Vintar, 2001, str. 177).

Elektronska uprava prispeva k odprtosti in preglednosti uprave. Lahko bi na kratko povedali, da zajema reformo uprave. Star način delovanja uprave ni bil več kos zahtevam državljanov. Današnja družba je informacijska družba, ki sloni na globalizaciji in informacijski tehnologiji in prav pomanjkanje teh elementov v upravi je privedlo do reforme. Storitve elektronske uprave prispevajo k posodobitvi javne uprave in k izboljšanju kakovosti storitev za uporabnike. Omogoča nam celo vrsto

storitev, kot so: oddaja davčne napovedi, pridobitev osebnih dokumentov, izpiskov iz matičnih knjig, lokacijskih dovoljenj itd. V prihodnosti naj bi se krog storitev razširil, saj je cilj kontinuirano izboljševanje in izpopolnjevanje uprave, približevanje uporabnikom in zvišanje zaupanja državljanov v storitve elektronske uprave.

Prednosti in slabosti

Dostopnost do storitev in informacij iz enega mesta, z možnostjo dostopa 24 ur na dan in sedem dni v tednu, prinaša skrajšanje čakalne dobe in pridobitev želenih informacij tudi izven delavnega časa uradov ter zvišanje obravnavanih zadev. Zaradi prejemanja in posredovanja podatkov preko spleta bodo cene storitev padle in znižali se bodo stroški poslovanja, poleg tega bomo priča nižji stopnji korupcije, saj elektronsko poslovanje temelji na strogo neosebnem stiku. Glede na to, da bo poslovanje temeljilo na elektronski obliki, bo lažje tudi pregledovanje uspešnosti poslovanja. Področje uprave si želi zlasti zvišati svoj ugled in vzpostaviti zaupanje njene storitve in institucije. Pričakovanja uporabnikov glede na področje uprave so zlasti zvišanje kakovosti storitev, hitrejše reševanje zadev z nižjimi cenami za storitve ter prijaznejši odnos uprave do strank.

Kljub najboljšemu namenu elektronske uprave pri zadovoljitvi pričakovanj uporabnikov v prihodnje in z vsemi prednosti, ki jih že uvaja, je treba omeniti tudi nekatere slabosti, ki spremljajo delovanje e-uprave.

Neosebni pristop sicer ima določene prednosti, vendar uporabnikom še vedno vzbuja strah pred zlorabo podatkov. Zato je slabost elektronskega poslovanja na sploh, torej ne samo v upravi, izločenost, povezana z nizkim računalniškim znanjem. Tukaj je treba zlasti omeniti starejše prebivalstvo, ki računalnikov ne uporablja in se zaradi svoje starosti tudi težje prilagaja nanje.

Poleg že omenjenih slabosti je skrb vzbujajoče tudi dejstvo, da se uporabniki neradi poslužujejo elektronskih storitev zaradi pomanjkanja zaupanja v varnost takih storitev in promocije storitev. Vintar meni (e-demokracija, 2007), da veliko ljudi pozna elektronsko poslovanje na področju uprave, če pa povprašamo po konkretnih storitvah oziroma katero od njih so že konkretno uporabili, pa pridemo do zaključka, da ljudje na splošno vedo, da e-uprava obstaja, vendar podrobnejših informacij o konkretnih storitvah ne poznajo in jih tudi ne uporabljajo.

Nevarnosti, ki zasledujejo področje e-uprave, so komponenta, na katero je treba dati veliko poudarka. V čim krajšem času je treba najti ustrezne rešitve na zgoraj navedene probleme. Poleg neznanja, povezanega z računalniki in z zvišanjem promocije, je področje zviševanja stopnje varnosti prvotnega pomena. Strah ljudi pred vdori v osebne podatke in uporaba le-teh so razlogi, zaradi katerih ljudje ne uporabljajo elektronskih storitev v tako visoki meri, kot je bilo pričakovano.

2.2 ELEMENTI RAZVOJA ELEKTRONSKE UPRAVE V SLOVENIJI

Prehod na informacijsko družbo je globalni proces, ki se mu ni mogoče izogniti in zajema vsa področja delovanja posamezne države. Eno izmed teh področji je tudi uprava. Njena reforma je tako kot večino evropskih držav zajela tudi Slovenijo.

»Uvajanje in razvoj e-uprave (v ožjem smislu) lahko analiziramo z več vidikov: z vidika zagotavljanja tehnološke infrastrukture (v upravi sami in pri uporabnikih), zagotavljanja ustreznih pravnih podlag ter ponudbe e-storitev in povpraševanja po njih, pri čemer so uporabniki storitev občani, podjetja in nevladne oziroma nepridobitne organizacije (Leben in Kunstelj, 2004, str. 7).«

Elektronske storitve na področju uprave se nanašajo na različne subjekte. Med seboj se razlikujejo glede na skupino uporabnikov, ki jih bo uporabljala. Razumljivo je, da se potrebe po storitvah e-uprave med skupinami uporabnikov razlikujejo. Obstajajo tri različne skupine uporabnikov in posledično trije različni odnosi uprave do njih. To so:

- G2C, e-storitve za državljane (government to citizen),
- G2B, e-storitve za poslovne subjekte (government to business) in
- G2G, e-storitve znotraj uprave (government to government).

V letu 2001 je bila v Sloveniji sprejeta strategija e-poslovanja v upravi, ki je predstavljala temelj za nadaljnji razvoj e-uprave, saj je vsebovala vse temeljne komponente, ki so potrebne za uvedbo dobrega sistema elektronskega poslovanja v upravi. Najpomembnejše med njimi so zagotovo e-podpis, e-poslovanje, zviševanje učinkovitosti in kakovosti upravnih storitev.

V Sloveniji je reforma vključila vse tri temeljne skupine uporabnikov. Reforma e-uprave je za posamezne uporabnike prinesla novosti na naslednjih področjih:

Za državljane:

- zemljiška knjiga,
- vpogled v lastne osebne podatke na podlagi digitalnega potrdila,
- sodni register,
- register predpisov,
- informacijski servis podatkov-ISPO itd.

Za poslovne subjekte:

- zemljiška knjiga in kataster,
- evidenca trga nepremičnin,
- sodni register,
- e-carina in e-davki za poslovne subjekte,
- e-letna poročila,
- e-zaposlitve za poslovne subjekte,
- elektronske storitve za notarje,

- portal e-Vem (državni portal za poslovne subjekte, ki omogoča registracijo samostojnega podjetnika na enem mestu).

Znotraj uprave:

- povezava med Zavodom za pokojninsko in invalidsko zavarovanje,
- centralnim registrom prebivalstva ZPIZ-CVI-CRP,
- povezava med evidencami Ministrstva za delo, družino in socialne zadeve.

Razvoj Slovenske e-uprave je po letu 2001 strmo naraščal, vidne izboljšave in novosti je mogoče videti na najrazličnejših področjih. Spodaj sem naštela le nekaj najpomembnejših novosti, ki jih je uvedla reforma uprave:

- uvedba portala e-uprave, ki ponuja informacije in storitve za državljane, pravne osebe in za samo poslovanje znotraj uprave,
- zanesljiva informacijsko-telekomunikacijska infrastruktura državne uprave,
- izvedba kompleksnih medresorskih projektov (vse na enem mestu e-VEM, centralni register prebivalstva e-CRP, povezovanje evidenc MDDSZ-CVI-CRP),
- vzpostavitev in delovanje infrastrukturnih gradnikov e-uprave (hitro komunikacijsko omrežje javne uprave – HKOM, podatkovni center – PDC, centralni moduli, centralne informacijske rešitve – CIS, centralni registri …),
- prihranki v javni upravi zaradi učinkov sodobnih e-storitev in medresorskih informacijskih projektov,
- vključevanje vseh resorskih organov v usklajevalno skupino e-uprave za boljšo informiranost in enostavnejši razvoj e-uprave (glej Ministrstvo za javno upravo, 2006, str. 8).

Za prihodnost e-uprave so poleg ciljev, vizij in usmeritev pomembni tudi pogoji, ki bodo omogočali razvoj in nadgradnjo e-uprave. Njihovo uresničevanje je ključnega pomena za uresničitev projektov v prihodnosti. Pogoji se nanašajo na devet področij:

- prenova poslovanja,
- reorganizacija,
- pravno-formalne osnove,
- menedžment,
- kadrovski viri,
- usposabljanje in znanje,
- finančna sredstva,
- promocija in
- informacijske rešitve (glej Ministrstvo za javno upravo, 2006, str. 19).

Ne glede na vse prednosti, ki jih prinaša elektronska uprava, pa imajo ljudje velike pomisleke glede uporabe le-te. Glavni dejavnik je strah, ki je povezan z zanesljivostjo take uprave, poleg tega pa nezaupanje v svoje znanje in sposobnosti glede uporabe novodobne uprave, ki temelji na elektronskih povezavah. Kljub temu, da je možno

uporabljati storitve preko spleta, veliko ljudi še vedno najraje uporablja star sistem, ki temelji na osebnem stiku.

Raziskava merjenja zadovoljstva uporabnikov e-uprave proučuje del, ki se nanaša na razloge za neuporabo e-uprave. Nekaj najosnovnejših rezultatov raziskave na področju neuporabe e-uprave oziroma razlogov za neuporabo:

- polovica anketirancev interneta sploh ne uporablja;
- 30 odstotkov uporabnikov interneta raje ureja zadeve na klasičen način, ker jih elektronski način ne zanima;
- 40 odstotkov uporabnikov interneta pozna obrazce za vloge, le-teh pa ni pridobilo, ker jih še niso potrebovali in ker menijo, da od njih nimajo koristi;
- 25 odstotkov poznavalcev elektronskih storitev teh še nikoli ni uporabljalo. Poudariti moramo, da je razkorak med poznavanjem in uporabo pri e-dohodnini kar 64 odstotkov, pri pridobitvi evropske kartice zdravstvenega zavarovanja pa le 29 odstotkov.

Glavni razlogi za neuporabo e-storitev so: nisem jih potreboval, raje zadeve urejam na klasičen način, nisem našel storitev, nimam digitalnega potrdila, drugi to opravijo zame (glej Vintar et al., 2006, str. 9).

Menim, da bi bilo treba graditi zlasti na promociji storitev e-uprave. Ljudem bi bilo treba predstaviti, kako je nov način urejanja zadev lažji in kakovostnejši od starega klasičnega sistema. Dostop do storitev je treba narediti bolj prepoznaven in enostavnejši, tako da bodo uporabniki že ob vstopu na spletno stran vedeli, kam se je treba prijaviti in kako dostopati do storitev, obrazcev in informacij. Strah pred napakami in nezaupanjem v varnost sistema onemogoča, da bi se uporabniki v višji meri posluževali storitev. To je treba v prihodnosti odpraviti, če želimo našo družbo napraviti informacijsko v pravem pomenu besede.

2.2.1 Dosežki slovenske e-uprave v primerjavi z drugimi državami

Meritve uspešnosti držav na področju e-uprave, ki jih opravlja neodvisna organizacija Capgemini, so leta 2005 Slovenijo uvrstile na 15. mesto v primerjavi s članicami EU in Norveško, Islandijo in Švico ter na drugo mesto v primerjavi z novimi članicami EU. Prehitela jo je samo Estonija (glej Ministrstvo za javno upravo, 2007).

V letu 2006 so meritve Slovenijo dvignile iz 15. na 7. mesto, prav tako glede na članice EU, Norveško, Islandijo in Švico (glej Capgemini, 2006).

V letu 2007 je Slovenija s projektom e-VEM prišla v finale tekmovanja za nagrado javnih storitev pod organizacijo združenih narodov. To pomeni, da se je uvrstila med deset najboljših držav na svetu. Na območju v EU pa je zasedla drugo mesto. V istem letu je Ministrstvo za javno upravo prejelo priznanje za primer oblikovanja programa za odpravo administrativnih ovir.
Glede na meritve Capgemini pa je Slovenija v letu 2007 zasedla drugo mesto, ki si jo deli z Malto (glej Capgemini, 2007).

Iz zgoraj navedenih podatkov je razviden hiter razvoj e-uprave v Sloveniji. Pomembno je, da naša uprava vsako leto zaseda visoka mesta. To pomeni, da uvajamo pravilno politiko oziroma gledamo na razvoj uprave s pravilnega zornega kota in se zavedamo, da so potrebne konstantne nadgradnje sistema. Te so pogoj za obstanek in uspešnost v današnji dinamični in spreminjajoči se informacijski družbi.

2.3 E-UPRAVA V EVROPSKI UNIJI

Področje elektronske uprave je trenutno ena glavnih tem v Evropski uniji na lokalni, regionalni, državni in globalni ravni. Predstavlja eno glavnih komponent reforme javnega sektorja, ki s seboj prinaša rast učinkovitosti, konkurenco in posodablja storitve. Uvajanje novih kompleksnih storitev, cenejši razvoj in vzdrževanje, povezovanje informacijskih sistemov in registrov, enotnost e-storitev, prilagodljivost poslovnim procesom, centralno obvladovanje e-storitev, transparentnost delovanja e-uprave so eni izmed ciljev, ki si jih je Evropska unija zastavila na področju uprave. Razlog, zakaj Evropska unija daje toliko poudarka na razvoj e-uprav v državah članicah, je predvsem v lažjem povezovanju uprav med državami, izmenjevanje podatkov in informacij, zagotavljanje varnosti na področju EU, povečanje konkurence ter zniževanje stroškov in zadovoljevanje zahtev državljanov po kakovostnejših storitvah (glej Heath, 2000, str. 11).

2.3.1 Cilji e-uprave s strani Evropske unije

Uprave vseh držav članic si želijo kakovostno, fleksibilno in uspešno upravo, ki bo zadovoljila potrebe uporabnikov in postopoma zmanjševala papirnato poslovanje. »Vse na enem mestu« je slogan, ki združuje vse uprave. Podprt je z varnim elektronskim poslovanjem, hitrimi odzivi in vključenostjo državljanov v proces odločanja. Pomembna komponenta je tudi finančna omejitev, ki predstavlja zniževanje stroškov poslovanja in posledično znižanje porabe javnih sredstev na področju uprave. Treba je uvesti razvite metodologije in orodja, ki bodo omogočali konstantno prilagajanje novim zahtevam in kompleksnemu okolju.

Znotraj političnih organov držav članic in tudi na evropskem nivoju je treba razviti strategije, ki bodo dolgoročno opredeljevale cilje in projekte za nadaljnji razvoj e-uprave, in prenehati s kratkoročnimi strategijami znotraj mandatov posameznih vlad. Cilj je izoblikovati uprave, ki bodo omogočile sodelovanje med različnimi nivoji na nivoju države kot tudi na nivoju unije, ter omogočiti standardizacijo storitev za skupne potrebe EU. Pomembno področje predstavlja zviševanje harmonizacije na področju prava med državami članicami, ki bo omogočala zviševanje stopnje varnosti in zasebnosti na področju opravljanja storitev ter uvedbo upravljanja identitet posameznika na področju celotne Unije.

2.4 PODROČJE VARNOSTI

Nizka uporaba elektronskih storitev je povezana s področjem varnosti. Ljudje so zaskrbljeni zaradi varnosti, zasebnosti, zaupnosti in dvomijo o pravilni uporabi podatkov. Kljub temu, da živimo v skrajno informacijski družbi in da se vsak dan neštetokrat srečujemo z izmenjavo podatkov preko spleta (na primer elektronska pošta), se ljudje, kar zadeva upravne storitve, še vedno raje poslužujejo starega sistema, ki temelji na osebnem stiku. Raziskava merjenja zadovoljstva uporabnikov e-uprave, ki so jo opravili na Fakulteti za upravo pod vodstvom dr. Mirka Vintarja, potrjuje dejstvo, da ljudje pričakujejo več na področju varnosti oziroma varovanju osebnosti, prav tako je bilo slabo ocenjeno zaupanje v samo e-upravo.

Človeško bitje se težko prilagaja na spremembe. V človeški naravi je, da se jim izogibamo do tistega trenutka, ko ugotovimo, da nam ne preostane nič drugega, kot da se z njimi sprijaznimo. Zanimivo je dejstvo, da se je večina uporabnikov javnih storitev nenehno pritoževala nad neustreznostjo in zastarelostjo sistema. Zdaj, ko pa imajo možnost uporabljati nove tehnologije, se le-tem množično izogibajo.

Kako uporabnike prepričati, da so e-storitve zanesljive in podprte z ustreznimi varnostnimi tehnologijami? Ali so res? Kaj lahko izboljšamo, na kakšen način? Kakšna tehnologija bo ustrezala vedno večjemu številu nevarnosti, ki ogrožajo elektronsko poslovanje? Kako napraviti povezavo tako varno, da bodo vdori vanjo in kraja identitet nemogoča? To so vprašanja, ki so si jih zastavile vse uprave držav članic in Evropska unija kot skupnost. Odgovor na zastavljena vprašanja ni enostaven, vendar pa je ena izmed možnosti sigurno upravljanje z identitetami posameznika.

3 UPRAVLJANJE IDENTITET POSAMEZNIKA KOT KLJUČ DO USPEŠNEGA ELEKTRONSKEGA POSLOVANJA

»Upravljanje identitete posameznika ali s tujko »identity management« bi lahko opisali kot celoto procesov, orodij in družbenih pogodb za ustvarjanje, vzdrževanje in omejevanje elektronske identitete ljudi ali splošneje sistemov in storitev, ki omogočajo varen dostop do raznolikih delov posameznih sistemov in aplikacij.« (Pato, 2003, str. 1). Je jedro varnostnega sistema, ki služi za vzdrževanje šifriranih informacij, katere omogočajo dostop do sistema oziroma njegovih posameznih delov. Je celota informacij in podatkov posameznika, ki enoznačno z najvišjo stopnjo zanesljivosti identificirajo posameznika.

V zadnjem desetletju je ta pojav pritegnil veliko pozornosti s strani elektronske industrije, saj gre za celoto, ki ne vsebuje samo tehnološke komponente, ampak tudi družbene in pravne. Vključuje pravne in fizične osebe, njegovo delovanje pa povezujemo z najrazličnejšimi podjetji in tudi z državnimi upravami. V današnjem e-svetu postane nenadomestljiv pojav povezan s poslovanjem, saj le-ta ob svojem delovanju opravlja identifikacijo vseh udeleženih identitet, z namenom uveljavitve zaupanja, spoštovanja zasebnosti in varovanja podatkov. S tega vidika je »identity management« ključ, ki aktivira e-poslovanje preko svoje sposobnosti prepoznavanja elektronskih identitet ter preko svojega znanja o njihovi pravilni uporabi. To pa je nujna komponenta, če želimo imeti sistem, ki ima sposobnost identifikacije vseh udeležencev in s tem zviševanje kakovosti njegovega delovanja (glej Casassa Mont et al., 2002, str. 1).

Pomen besede »identiteta« izhaja iz latinskega jezika, in sicer iz besednega korena »idem«. V angleškem jeziku se ta uporablja že od 16. stoletja. Ima tehnični pomen tako v algebri kot v filozofiji. V času Johna Locka so jo povezovali s telesnimi in mentalnimi trajnimi poškodbami. Identiteta je predstavljala dejstvo, da je oseba samosvoja in določljiva ter nenadomestljiva (glej Gleason, 1983, str. 911). Identiteta je ključni element zaščite pri e-poslovanju. Določa celoto podatkov, ki se nanašajo na posamezno osebo. Pomembna je za unikatno identifikacijo te osebe ter z njo povezane procese pri elektronskem poslovanju.

V današnjem svetu ima vsaka oseba podatke, ki ji dajejo identiteto, in preko njih dokazuje svojo verodostojnost. Najpogostejše so ime, priimek, naslov, enotna matična številka občana (EMŠO) in davčna številka. Ti podatki dokazujejo, da kot osebe z vsemi pravicami in dolžnostmi, ki so nam bile dodeljene, res obstajamo. Enak postopek velja v virtualnem svetu. Uporabniki morajo imeti podatke, ki dokazujejo njihovo identiteto oziroma zagotavljajo, da je uporabnik res tista oseba, za katero se predstavlja. Lahko bi tudi rekli, da je »identity management« glavna komponenta sistema varovanja, ki je namenjen za preverjanje identitete posameznikov, ki želijo vstopiti v elektronski svet in v njem opravljati različne transakcije oziroma se poslužujejo storitev na spletu. Ko je identiteta potrjena in sistem preveri in potrdi verodostojnost podatkov, lahko začne uporabnik poslovati, tj. opravljati transakcije preko elektronskega sistema, saj je sistem preveril vse podatke in s tem zagotovil najvišjo varnost.

3.1 POMEN UPRAVLJANJA Z IDENTITETAMI V ELEKTRONSKI UPRAVI

Marca leta 2000 so se v Lizboni sestali vsi glavni predstavniki držav članic z namenom narediti ekonomijo Evropske unije najbolj dinamično in konkurenčno na svetu. Za dosego Lizbonske strategije je eden ključnih področij e-uprava kot pomemben faktor evropske politike na področju informatizacije. Zvišanje kakovosti javnih storitev, zvišanje odgovornosti, informatizacija javne uprave so področja, ki jih dojemamo kot temelj za dosego ugodnosti, ki jih ponuja informacijska družba in posledično za dosego Lizbonske strategije (glej Stefanova et al., 2006, str. 24).

Področje upravljanja identitet in izbor ustreznih tehnologij za določitev in overitev državljanov in podjetij sta dve izmed najpomembnejših vsebin za oblikovanje napredne informacijske družbe, ki bo kot cilj imela varovanje identitet, podatkov, dokumentov fizičnih in pravnih oseb. Zajema področja, kot so zasebnost in varovanje podatkov subjektov na eni strani, na drugi pa pravilno zagotavljanje izvajanja prava, zakonodajne ureditve, nacionalne varnosti in na splošno učinkovitosti na področju pravne ureditve, ki ureja področje varovanja osebnih podatkov in pravilno uporabo le-teh. Upravljanje identitet posameznika v e-upravi pomeni kombinacijo tehnologije, ekonomije, družbe, varnosti in zasebnosti osebnih podatkov ter zaupanje in sprejemanje takega sistema. E-uprava na nivoju EU potrebuje povezane dostope do informacij za ureditev medsebojnih odnosov in za iskanje najustreznejših rešitev.

Uprave so vedno upravljale z identitetami, razlika je le v tem, da se sedaj soočajo z edinstvenim izzivom, ki še vedno zajema področje upravljanja identitet, ampak v novi obliki, in sicer elektronski. Upravljanje identitet in podatkov fizičnih in pravnih oseb je največji del uprave v smislu njenega delovanja. Odnos med upravo, državljani in podjetji je edinstven in kot tak bo tudi vedno ostal. Sprememba je samo v tem, da se je odnos iz starega osebnega sistema prenesel v elektronski. Sprememba prinaša velika pričakovanja s strani posameznikov in podjetij. Pričakovanja in zahteve do uprave so visoke, saj za svoje delovanje uporablja občutljive podatke, ki jih mora ustrezno zavarovati in hraniti.

Danes se uprave soočajo s kompleksnim in spreminjajočim se okoljem. Od njih se zahteva, da naredijo ravnotežje med potrebami po varnosti, zasebnosti, zahtevami državljanov in podjetij po varnih spletnih storitvah ter vprašanjem pravilnega in varnega upravljanja identitet. Vprašanje ravnotežja in uskladitve ni enostavno, zato mora biti projekt podprt tudi s strani politike, tehnologije in zakonodaje. »Identity management« v e-upravi ponuja rešitev za upravljanje z identitetami na področju javnega in zasebnega poslovanja. Omogoča sodelovanje med različnimi delovnimi področji in harmonizira e-upravo na nivoju Evropske unije.

Potrebno pa je poudariti, da sam sistem »identity managementa« ni dovolj za uspeh, potrebno ga je povezati z normativnimi in tehnološkimi rešitvami. Glede normativnega področja je situacija slednja; zelo pomembno je, da vsaka država sprejme ustrezne zakone oz. norme, ki bodo sistemu »identity managemanta« dajali ustrezna pooblastila, okvirje, v katerih se lahko giblje, pravice in dolžnosti ter varstvo in zaščito. Poleg same države pa imajo tudi vsa podjetja oz. vsi pravni subjekti, ki za svoje delovanje uporabljajo sistem upravljanja identitet posameznikov, pravico in

dolžnost, da za svoje delovanje uredijo pravilnike, ki bodo zaščitili njihove interese in interese uporabnikov. Glavni elementi tehnoloških rešitev pa so: pametne kartice, elektronski podpis, infrastruktura javnega ključa, digitalna potrdila ter področje biometrije.

3.2 PREDSTAVITEV MOŽNOSTI TEHNOLOŠKIH REŠITEV NA PODLAGI PAMETNE KARTICE

Pametna kartica je pomembna tehnološka rešitev v svetu informacijske družbe. Po velikosti je enaka današnjim plastičnim plačilnim karticam, s to razliko, da ima vgrajen mikročip, ki se različno odziva na sisteme, torej se obnaša pametno. »Vse skupaj bazira na mikroprocesorju, ki je običajno manjši računalnik, ki lahko sprejema, shranjuje in procesira podatke ter omogoča uporabo različnih aplikacij.« (Zadel, 2003, str. 549). Prav visoke zmogljivosti mikroprocesorja in njegova sposobnost varnega in dolgotrajnega shranjevanja podatkov ter možnost izvajanja raznih kriptografskih funkcij predstavljajo temeljno povezavo s sistemom upravljanja identitet posameznikov.

Sestavni deli mikroprocesorja pa so naslednji:

- mikročip: tisti, ki dejansko naredi kartico »pametno«; ima dve osnovni funkciji, in sicer obdeluje in prikazuje podatke;
- pomnilnik: pametna kartica mora imeti obstojen pomnilnik, ki hrani podatke, kot so ime nosilca in uporabniške programe. Imeti pa mora tudi pomnilnik, kamor se vpisujejo sprotne informacije, kot je na primer stanje po opravljeni transakciji. Na splošno ima pametna kartica tri vrste pomnilnika, in sicer so to bralni, bralno-pisalni in programobilni bralni pomnilnik,
- vhodno-izhodna enota (glej Jurišič, 1997, str. 37).

Pametna kartica poleg shranjevanja in obdelovanja podatkov omogoča tudi avtentikacijo in prepoznavanje njenega imetnika, nadomestilo za denar in varno plačilno poslovanje. S pomočjo kartice poteka varen prenos podpisanih dokumentov med različnimi med seboj neodvisnimi partnerji. Varovanje podatkov in varnost njihovega prenosa zagotavlja PIN številka, ki je shranjena v posebnem delu pomnilnika. Ko lastnik kartice želi vstopiti v sistem, mora najprej vstaviti kartico v vhodno-izhodno enoto in nato vtipkati PIN številko oziroma kodo. Če pametna kartica potrdi ujemanje vtipkane kode s tisto, ki je shranjena na pomnilniku, lahko imetnik kartice vstopi v računalniški sistem. Kljub visoki stopnji varovanja podatkov preko PIN kode pa se v zadnjem obdobju veliko govori o dodatnem preverjanju avtentičnosti imetnika kartice. Največ pozornosti je namenjene področju biometrije, ki se v zadnjem desetletju naglo razvija in omogoča skoraj nezmotljivo preverjanje avtentičnosti. Poleg mikročipa, PIN kode oz. biometričnih podatkov pa je pomemben faktor pametne kartice tudi njen format. »Format pametnih kartic določa ISO standard, določa pa tako fizične karakteristike kartic, kot tudi dimenzije, lokacije kontaktov, tipe označevanja, protokole komunikacij s svetom, priporočila za operacijski sistem, organizacijo podatkov na kartici in varnostne mehanizme.« (Pehani, 1999, str. 16)

Na vprašanje, kje lahko pametne kartice uporabljamo, lahko odgovorimo, da povsod. V današnjem času se njihova uporaba širi na vedno več področij, najbolj aktualna pa so slednja:

- telekomunikacije; pametne kartice na področju telefonije so praktično edini obstoječi sistem; telefonije, ki temelji na starem sistemu, skoraj več ni. V mobilni telefoniji so prisotne od vsega začetka, prvotno le zaradi identifikacije, kasneje tudi zaradi varnosti;
- zdravstvo; glavni motivi za uvajanje pametnih kartic na področju zdravstva so pregled in nadzor stroškov ter dokazovanje zdravstvenega zavarovanja. Za zdaj na kartici še ni vsebovano zdravstveno stanje lastnika;
- bančništvo; pojav pametnih kartic kot način uvedbe elektronske denarnice. Potreba po pametnih karticah se kaže tudi na področju varnosti, zlasti pri transakcijah (glej Jurišič in Tonejc, 2001, str. 70).

Poleg navedenih treh področij se pametne kartice lahko uporablja tudi na področjih e-uprave, vojske, televizije, transporta, šolstva itd. Lahko bi rekli, da si danes ne moremo več predstavljati življenja brez pametnih kartic, saj omogočajo brezgotovinsko poslovanje, dostop do baz osebnih podatkov ter zaščito le-teh, predvsem pa poenostavlja administracijo in onemogoča zlorabo in kriminal.

Uporaba pametne kartice poteka tako, da se izvedejo naslednji koraki:

- preveri se verodostojnost operaterja;
- preveri se verodostojnost uporabnika preko vizualne primerjave podatkov natisnjenih na kartici ali preko elektronskega dostopa do podatkov, ki so shranjeni na kartici;
- v podatkovni bazi se poišče zahtevane podatke;
- preko najdenih podatkov se kreira dokument;
- podpiše se dokument z operaterjevim zasebnim ključem;
- na pametno kartico se shrani podpisani dokument (glej Trampuš et al., 2002, str. 2).

Pojav pametnih kartic na državnem nivoju (primer osebne izkaznice) s seboj prinese mnogo vprašanj in skrbi s strani državljanov, zlasti na področju nadzora ljudi. Čip na kartici si vsako identifikacijo zapomni in jo posreduje v centralni sistem za zbrane podatke. To lahko pomaga policiji pri izdelavi natančnega profila vsakega človeka, ki ima v lasti osebno izkaznico. To bi bilo zelo močno orožje v boju proti terorizmu, nezakonitemu prestopu meja in boju proti organiziranemu kriminalu. Po drugi strani pa bi lahko privedlo do totalnega nadzora nad ljudmi in s tem do kršenja pravice do zasebnosti. Ljudje se ob takemu načinu identifikacije počutijo ogroženi in prisoten je strah pred zlorabami. Velik poudarek je zlasti na izgubi anonimnosti in zasebnosti. Potrebno pa je poudariti, da je pametna kartica najbolj ustrezen način zadovoljitve visoke stopnje varnosti v sodobnih informacijskih sistemih in je poleg tega ključen instrument za izgradnjo sistema tehničnega varovanja, ki se bo najbolje prilagajal potrebam določenega okolja.

3.3 ELEKTRONSKI PODPIS, TEMELJ ELEKTRONSKEGA POSLOVANJA

Elektronski podpis je nadomestek lastnoročnega podpisa v elektronskem poslovanju. Lahko pa ga predstavimo tudi kot skupek podatkov v elektronski obliki, ki je povezan z drugimi podatki in je namenjen preverjanju teh podatkov in identifikaciji podpisnika. Zagotavlja identiteto posameznika in onemogoča naknadno zanikanje lastništva podpisanih dokumentov. Zagotavlja njihovo verodostojnost. To pomeni, da jih ni mogoče spremeniti ali popraviti. Lahko bi rekli, da predstavlja temelj elektronskega poslovanja, ki zagotavlja dokumentu v elektronski obliki pravno veljavo. Izvedba samega elektronskega podpisa je zaradi svojih tehnoloških zmogljivosti s seboj prinesla številne pozitivne učinke, ki jih lastnoročni podpis prej ni poznal. To so predvsem tajnost sporočila, neokrnjenost vsebine sporočila, potrjevanje časa nastanka sporočila in zanesljiv sprejem sporočila. Vsi navedeni učinki dajejo elektronskemu sporočilu višjo veljavo in učinkovitost kot papirnatemu sporočilu oziroma dokumentu (glej Toplišek, 1996, str. 295). Uporablja se lahko za najrazličnejša elektronska pravna dejanja, in sicer od sklepanja elektronskih pogodb, oddajanja in sprejemanja ponudb, vlaganja zahtevkov, potrjevanja sprejemanja elektronskih dokumentov do izdajanja e-računov.

Prva država, ki je uzakonila elektronski podpis, je bila ameriška zvezna država Utah. Republika Slovenija je to naredila leta 2000, ko je slovenski parlament sprejel zakon o elektronskem poslovanju in elektronskem podpisu. S to potezo je Slovenija postala enakopravna z ostalimi državami glede elektronskega načina transakcije dokumentov.

Zavedati se moramo, da elektronski in digitalni podpis nista enaka pojma. Elektronski podpis je splošen pojem, ki je definiran kot skupek vseh oznak, narejenih z elektronskimi mediji, z namenom označevanja dokumentov in datotek. Digitalni podpis je sicer elektronski podpis, ampak samo tisti, ki za svoje delovanje uporablja asimetrično kriptografijo, ki temelji na paru ključev. Omeniti je treba še varen elektronski podpis, ki predstavlja vrsto digitalnega podpisa, vendar je overjen s kvalificiranim potrdilom. Njegove značilnosti so:

- da je povezan izključno s podpisnikom;
- da je iz njega mogoče zanesljivo ugotoviti podpisnika;
- da je ustvarjen s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom;
- da je povezan s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave z njimi (glej ZEPEP, 2. člen).

Pri elektronskem poslovanju sta sporočilo in podpis neločljivo povezana, zato je elektronsko poslovanje bolj verodostojno od lastnoročnega in predvsem ga je nemogoče ponarediti, kar za lastnoročni podpis ne velja. Zato lahko trdimo, da je elektronsko poslovanje preko elektronskega podpisovanja, ki temelji na infrastrukturi javnih ključev, na splošno varnejše kot papirnato poslovanje, ki temelji na lastnoročnem podpisu.

Pravna podlaga

Temeljna podlaga v Sloveniji za to področje je Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP), ki je bil izdan leta 2000. Predstavlja temeljni element slovenske pravne ureditve na tem področju. Ureja vprašanje elektronskega poslovanja in določa pogoje za elektronske transakcije in sisteme, na katerih se izvajajo. Njegov namen je pravno izenačiti elektronsko obliko poslovanja s klasičnim papirnatim poslovanjem, kar posledično daje enako veljavo elektronskemu podpisu kot lastnoročnemu. Slovenija je s tem zakonom usklajena s pravili Evropske unije o elektronskem poslovanju.

Poleg ZEPEP imamo v Sloveniji še naslednje pravne podlage:

- Zakon o elektronskem poslovanju na trgu (Ur .l. RS, št. 57/2000),
- Zakon o splošnem upravnem postopku (Ur .l. RS, št. 52/2002),
- Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Ur. l. RS, št. 77/200),
- Pravilnik o prijavi overiteljev in vodenju registra overiteljev Republike Slovenije (Ur .l. RS, št. 99/2001).

Pravni viri Evropske unije:

- Direktiva EU o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (1995/46/EC),
- Direktiva o elektronskem odpisu (1999/93/EC),
- Direktiva o elektronskem poslovanju (2000/317EC),
- Direktiva o pravnem varstvu baz podatkov (96/9/EC).

3.3.1 Infrastruktura javnih ključev

Za varno elektronsko poslovanje uporabljamo elektronski podpis ali bolje rečeno digitalni elektronski podpis, saj omogoča identifikacijo oseb v elektronskem svetu. Vendar pa za njegovo izpeljavo potrebujemo infrastrukturo javnih ključev, ki omogoča, da je podpis verodostojen, pravilno izpeljan in avtentičen.

Infrastruktura javnih ključev (ang. Public key infrastructures-PKI) postaja temeljni element za zagotavljanje varne izmenjave podatkov preko spleta. »PKI nudi uporabnikom svetovnega spleta zaupnost, celovitost, avtentikacijo, neponovljivost, kar posledično pomeni trdno osnovo za zagotovitev varnega izmenjavanja podatkov v elektronski obliki (Saksida, 2006, str. 104).« Sestavljajo jo strojna in programska oprema, varnostna politika, kriptografski sistemi ter nazadnje tudi uporabniki. Vse komponente skupaj pa pripomorejo k varni e-komunikaciji z uporabo javnih ključev za digitalno podpisovanje. Predstavlja enega najučinkovitejših sredstev za identifikacijo oseb, kar ji tudi omogoči status tehnologije z visoko ravnjo varovanja.

Infrastruktura javnih ključev sestoji iz štirih ključnih elementov:

- overitelja, ki skrbi za generiranje javnih in zasebnih ključev ter digitalnih potrdil in za njihovo hranjenje in objavo;
- prijavne službe, ki skrbi za registracijo in avtentikacijo oseb, ki zaprosijo za digitalno potrdilo;
- imenika, v katerem so na dostopnejših mestih shranjena digitalna potrdila;
- uporabnika, ki se poslužujejo PKI, za opravljanje varnih elektronskih komunikacij in e-poslovanje (glej Saksida, 2006, str. 104).

Je mehanizem, pri katerem zaupanje temelji na sistemu kriptologije v kombinaciji z javnim in zasebni ključem. Sistem kriptologije temelji na dveh elementih, in sicer na javnem in zasebnem ključu. Vsak uporabnik ima v lasti javni in zasebni ključ. Pošiljatelj sporočilo zakodira in pošlje sporočilo prejemniku s svojim zasebnim in prejemnikovim javnim ključem. Prejemnik sporočilo odkodira s svojim zasebnim in pošiljateljevim javnim ključem. Zasebni ključ je vedno v lasti lastnika, nikoli si ga ne deli z ostalimi. Na žalost pa kriptiranje podatkov ni dovolj za zagotavljanje visoke stopnje varovanja izmenjave podatkov, saj so mogoči napadi nepooblaščenih oseb, ki zasedejo položaj med pošiljateljem in prejemnikom. Za take vrste napadov pa imamo že razvito dodatno varovalno funkcijo, ki jo izvedejo overitelji in jo imenujemo digitalno potrdilo oziroma certifikat. Javni ključ z digitalnim potrdilom mora biti znotraj PKI hranjen tako, da je dostopen vsem uporabnikov, medtem ko je zasebni ključ dostopen samo lastniku. Le tako je omogočeno pravilno upravljanje digitalnih potrdil in javnih ključev, ki omogočajo varno uporabo elektronskega podpisa in šifriranja. Temelj PKI je skupno zaupanje vseh uporabnikov v celotno infrastrukturo. Preko PKI si uporabniki med seboj zaupajo in poslujejo, vendar je sistem zaupanja med njimi neposreden, saj vsi zaupajo isti agenciji za izdajanje digitalnih potrdil.

PKI omogoča, da so izdajanje, obnavljanje in uporaba javnih ključev čim bolj transparentni in avtomatizirani. Njen namen je zlasti:

- generiranje, hranjenje in izdajanje ključev,
- izdajanje digitalnih potrdil,
- objavljanje digitalnih potrdil v imenikih,
- preklicevanja digitalnih potrdil (glej Frelih, 2003, str. 40).

Infrastruktura javnih ključev je potrebna, ker uporabniki v virtualnem svetu ne poslujejo preko osebnega stika in fizično ne moremo prepoznati, kdo dejansko je na drugi strani povezave in ali je to res tista oseba, za katero se predstavlja. Nikoli ne moremo natančno vedeti ali je oseba s katero poslujemo in kateri posredujemo naše podatke, res tista, za katero se izdaja. Iz teh razlogov potrebujemo sistem za identifikacijo, ki nam bo to zagotovil. Eden izmed boljših sistemov za identifikacijo oseb je metoda kriptiranja, na kateri temelji PKI. Zato lahko s pomočjo infrastrukture javnih ključev oziroma preko njegove uporabe z visoko stopnjo varnosti in sigurnosti poslujemo preko spleta. Mehanizmi javnih ključev omogočajo, da vedno vemo s kom poslujemo in mu zato lahko brez zadržkov posredujemo naše podatke in dokumente.

3.3.2 Sestavni deli infrastrukture javnih ključev

PKI je sestavljen iz asimetrične kriptografije in digitalnega potrdila.

Asimetrična kriptografija

Sama beseda kriptografija izhaja iz dveh grških besed, in sicer kryptos, ki pomeni skrivati, in graphia, ki pomeni pisanje. Lahko bi rekli, da gre za tajno pisanje. Danes pa beseda kriptografija predstavlja predvsem znanost za varno shranjevanje in izmenjavo podatkov. V današnjem času je zlasti pomembna v povezavi z vprašanjem varnosti na spletu, predvsem zaradi postopka šifriranja in dešifriranja podatkov oziroma sporočil. V postopku šifriranja oziroma dešifriranja pa predstavljata glavni dve vlogi algoritem, ki predstavlja standardni postopek in ključ, ki naredi šifriranje unikatno. Pri asimetrični kriptografiji govorimo o sistemu dvojnega ključa; vsak pošiljatelj ima v lasti svoj zasebni ključ, ki je znan le njemu in ga lahko še dodatno zavaruje z geslom. Da bi prejemnik lahko sporočilo dešifriral, mu mora biti znan drugi pošiljateljev ključ, ki se imenuje javni ključ. Zasebni in javni ključ sta med seboj v zahtevnem matematičnem razmerju, vendar pa je iz javnega ključa dejansko nemogoče izpeljati zasebni ključ. »Sama uporaba asimetrične kriptografije v infrastrukturi javnih ključev nam zagotavlja celovitost, zaupnost, nezmotljivost sporočila in preverjanje identitete pošiljatelja (Toplišek, 1996, str. 293).«

Digitalno potrdilo

»Gre za potrdilo v elektronski obliki, ki povezuje podatke elektronskega podpisa z določeno osebo, ter nedvoumno potrjuje njeno istovetnost (Žoher in Urlep, 2007, str. 97).« Njegov namen je povezovanje podatkov, z namenom preverjanja digitalnega podpisa in s tem potrditev identitete osebe. Predstavljen je kot računalniški zapis, ki vsebuje naslednje podatke:

- različico formata,
- enolično številčno oznako potrdila v okviru izdanih potrdil posameznega overitelja,
- identifikator algoritma, s katerim je bil narejen elektronski podpis overitelja,
- ime overitelja, ki je potrdilo izdal,
- obdobje veljavnosti potrdila,
- ime lastnika javnega ključa,
- javni ključ in identifikator algoritma, v katerem se ključ uporablja,
- neobvezni polji, ki omogočata ponovno uporabo že dodeljenih razločevalnih imen overitelja ali lastnika javnega ključa (danes se ne uporablja več),
- neobvezne razširitve, ki vsebujejo dodatne informacije o javnem ključu in politikah v skladu s katerimi je bilo potrdilo izdano, o imetniku in izdajatelju potrdila ter različnih omejitvah (glej Pavliha in Blažič, 2002, str. 42).

Vedno ko želimo vstopiti v elektronske storitve ali v notranjost določenega omrežja, se od nas zahteva digitalno potrdilo. Dokazati je treba tudi, da imamo v lasti zasebni ključ, ki je povezan z javnim ključem v digitalnem potrdilu. Hramba digitalnega potrdila in zasebnega ključa se ponavadi nahaja v datoteki ali brskalniku našega

računalnika, najpogosteje je zavarovan z geslom. Vedno bolj aktualno je hranjenje digitalnega potrdila in zasebnega ključa na pametnih karticah ali ključih USB. Pametna kartica in ključ USB podpisujeta dokumente z zasebnim ključem, vendar pa zasebnega ključa ne izdata niti kriptografskemu programu. Za uporabo pametnih kartic in ključev USB je treba na operacijske sisteme najprej namestiti gonilnike. Na mediju je tako shranjeno digitalno potrdilo, za dostop do njega je potrebno geslo ali PIN-koda. V primeru napačnega vnosa gesla ali kode se kartica oziroma ključ zaklene.

Digitalno potrdilo zagotavlja naslednje:

- pošiljatelj in prejemnik sporočila sta res tista, za katera trdita, da sta;
- podatke pošilja pooblaščena oseba;
- nadzor nad dostopom; preko avtentikacije uporabnika se zagotovi avtoriziran dostop do podatkov;
- verodostojnost sporočila;
- onemogoča naknadno zanikanje lastništva sporočila;
- preko postopka šifriranja lahko samo upravičeni uporabniki preberejo sporočila.

Za elektronsko poslovanje je treba imeti spletno kvalificirano digitalno potrdilo, ki ga izdajajo registrirani overitelji. Digitalni podpis je veljaven in ima enako moč kot lastnoročni podpis samo, če je overjen s tako imenovanim kvalificiranim digitalnim potrdilom. Zagotavlja identiteto imetnika potrdila in celovitost vseh podatkov, ker le-teh ni mogoče spreminjati brez potrditve lastnika. Pomembno je, da se storitve, ki se opravljajo po elektronski poti, opravljajo po najvišji stopnji varnosti. Varnost digitalnih podpisov ne sme biti vprašljiva. »Za izvedbo e-storitev v okviru državne uprave je pomembno, da ima uporabnik poleg ustreznega znanja in dostopa do omrežja še digitalno potrdilo (Drobnjak in Jereb, 2007, str. 58).«

Kvalificirano digitalno potrdilo

Je potrdilo, ki je izdelano in izdano na podlagi zahtev, ki jih določa Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP). Njegova lastnost je varna uporaba elektronskega podpisa, drugi pomembni dejavnik pa je, da se ponudnik sam odloči, katera kvalificirana potrdila in katerega izdajatelja bo podprl. Iz kvalificiranega digitalnega potrdila mora biti ugotovljivo naslednje:

- ime in država stalnega prebivališča overitelja,
- ime imetnika potrdila,
- dodatni podatki o imetniku potrdila, ki so predpisani za namen, za katerega se bo potrdilo uporabljalo,
- podatki za preverjanje elektronskega podpisa,
- začetek in konec veljavnosti potrdila,
- identifikacijska oznaka potrdila,
- varen elektronski podpis overitelja, ki je potrdilo izdal,
- morebitne omejitve v zvezi z uporabo potrdila,

- morebitne omejitve transakcijskih vrednosti, za katere se potrdilo uporablja (glej ZEPEP, člen 28.).

V Sloveniji imamo register overiteljev digitalnih potrdil. V njem so trenutno vpisani štirje, ki delujejo v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP), Uredbo o pogojih za elektronsko poslovanje in elektronsko podpisovanje, evropskimi direktivami in drugimi veljavnimi predpisi. Overitelji so podjetja, ki skrbijo za generiranje, hranjenje, objavljanje in preklicevanje javnih in zasebnih ključev in digitalnih potrdil.

V Sloveniji so registrirani naslednji overitelji kvalificiranih digitalnih potrdil

Ministrstvo za javno upravo:

- digitalna potrdila SIGOV-CA so namenjena institucijam javne uprave za potrebe javne uprave;
- digitalna potrdila SIGEN-CA so namenjena fizičnim in pravnim osebam za potrebe e-poslovanja z javno upravo in med seboj.

HALCOM informatika, d. o. o:

- digitalna potrdila HALCOM-CA so namenjena pravnim in fizičnim osebam, registriranim za opravljanje dejavnosti.

AC NLB:

- digitalna potrdila AC NLB delujejo v okviru Nove Ljubljanske banke. Namenjena so fizičnim in pravnim osebam za e-poslovanje z NLB.

POŠTA CA:

- digitalna potrdila POŠTA CA delujejo v okviru Pošte Slovenije za fizične in pravne osebe (glej Vintar in Grad, 2004, str. 231).

Digitalna potrdila so namenjena upravljanju, dostopu in izmenjavi podatkov. Zato je zelo pomembno, da je izdajanje digitalnih potrdil s strani overiteljev točno določeno. Jasno mora biti določen namen, delovanje, upravljanje s kvalificiranimi digitalnimi potrdili, odgovornost overitelja ter varnostne zahteve.

3.4 TEHNOLOŠKE REŠITVE NA BAZI BIOMETRIJE

Visoka stopnja varovanja je danes ena najbolj iskanih dobrin. Pomemben dejavnik pri varovanju je identifikacija, ki mora biti hitra, učinkovita in zanesljiva. Glede na to, da živimo v skrajno konkurenčni družbi, mora biti tudi cenovno ugodna. Biometrija predstavlja eno, mogoče celo najboljšo rešitev za problem identifikacije in z njo povezane varnosti. Beseda biometrija izhaja iz starogrških besed »bios«, ki pomeni življenje, in »metron«, ki pomeni meritev. Enostavneje lahko besedo biometrija

opišemo kot vedo o prepoznavanju ljudi na podlagi telesnih, fizioloških in vedenjskih značilnosti. Najpomembnejše je, da gre za značilnosti, ki so unikatne pri vsakem človeškem bitju.

Ugotavljanje identitet posameznikov temelji na podlagi treh vprašanj, in sicer:

- kar oseba ima; primer je pametna kartica,
- kar oseba ve; sem spadajo gesla in PIN-kode,
- kar oseba je; pod to vprašanje spada biometrija.

Problem v prvem primeru je ta, da se kartica lahko izgubi, geslo ali PIN-koda pa pozabita. V tem kontekstu so biometrične značilnosti v veliki prednosti, saj se ne morejo izgubiti, pozabiti, skriti ali spremeniti. To predstavlja enega glavnih razlogov, zakaj je biometrija tako pomembna v povezavi z upravljanjem identitet oziroma z njihovo identifikacijo in avtentikacijo.

Človeške značilnosti, ki se najpogosteje uporabljajo v biometriji, so:

- prstni odtis,
- podoba obraza,
- šarenica in
- DNK.

Biometrija lahko temelji tudi na naslednjih značilnostih:

- dlani,
- vonju,
- barvi glasu,
- gibanju,
- prepletu ven na roki,
- lastnoročnem podpisovanju in
- tipkanju.

Zgoraj navedene značilnosti so unikatne, neprenosljive, nezamenljive in njihova ponaredba je izredno zahtevna. Poleg tega se lahko uporabljajo z ali brez uporabnikove vednosti. Med vsemi naštetimi sta najbolj verodostojna in unikatna DNK in šarenica. Nemogoče ju je spremeniti. Možnosti, da bi dve osebi imeli enak DNK ali šarenico, so tako zelo majhne, da postanejo že zanemarljive. Glede na to, da pri identifikaciji osebe ne uporabljamo samo biometrične značilnosti, ampak tudi druge elemente, je možnost, da bi napačno identificirali osebo, dejansko skoraj nična.

3.4.1 Zakonodaja na področju biometrije

Vsaka država mora področje osebnih podatkov zakonsko urediti. Področje biometrije je v Sloveniji urejeno z Zakonom o varstvu osebnih podatkov (Ur. l. RS, št. 84/2004). Biometrijo kot obliko obdelave osebnih podatkov obravnavajo štirje členi v tretjem

poglavju. Razlog, zakaj je obravnavana v Zakonu o varstvu osebnih podatkov, je naslednji: prstni odtis, podoba obraza, šarenica, očesna mrena, DNK in drugi biometrični podatki so istočasno tudi osebni podatki, saj se od človeka do človeka razlikujejo. Na njihovi podlagi je mogoče identificirati osebo. Vsakršno zbiranje, shranjevanje, uničevanje, posredovanje teh podatkov se šteje za obdelavo osebnih podatkov. Iz tega razloga zanje veljajo določbe o varovanju osebnih podatkov. Zakon določa, da se biometrične značilnosti lahko obdelujejo za identifikacijo posamezne osebe oziroma za preverjanje identitete osebe. Identifikacija osebe pomeni ugotavljanje same identitete osebe, preverjanje identitete pa pomeni ugotavljanje, ali je oseba res tista, za katero se izdaja. Zakon dovoljuje uporabo biometrije v javnem in zasebnem sektorju, vendar le v določenih primerih.

V javnem sektorju se biometrija lahko uporablja le za varovanje ljudi in njihovega premoženja oziroma za varovanje tajnih podatkov in njihovih poslovnih skrivnosti. Temeljni pogoj je, da se namena ne da doseči z drugimi sredstvi. Kljub vsemu pa se lahko biometrične ukrepe določi z zakonom, če gre za izpolnjevanje obveznosti iz obvezujoče mednarodne pogodbe ali za identifikacijo posameznikov pri prehajanju državnih meja (glej ZVOP-1, 79. člen).

V zasebnem sektorju pa se lahko biometrične ukrepe izvaja le, če je to potrebno za opravljanje dejavnosti oziroma varovanje premoženja, tajnih podatkov in poslovnih skrivnosti. Vse skupaj pa je mogoče le ob pogoju, da so predhodno obveščeni vsi zaposleni (glej ZVOP-1, 80. člen).

3.4.2 Biometrični podatki

Prstni odtis

Prstni odtis sodi med najzanesljivejše načine ugotavljanja človekove identitete. Je tudi najstarejši način identifikacije med biometričnimi podatki. Znano je, da ima vsak človek unikaten prstni odtis, celo dvojčka nimata enakega. Začetek uporabe prstnega odtisa sega v čas, ko še ni bila razvita informacijska družba. V preteklosti se je prstni odtis uporabljal za preverjanje identitete na področju kriminalitete, danes pa vzorec uporabljamo za preverjanje identitete posameznika, brez povezave s kriminalnimi dejanji. Kljub temu ljudje še vedno povezujejo prstni odtis s kriminalom in se ob odvzetju vzorca prstnega odtisa počutijo nelagodno in ogroženo.

Prstni odtis nastane že pri zarodku in se skozi življenjsko dobo človeka ne spreminja. Prav tako se v primeru poškodbe ponovno vrne v izvorno obliko, brez kakršnih koli sprememb. Prstni odtis sestavljajo grebeni s porami obdani z votlinami, nahajajo se na ožilju tik pod kožo, izoblikujejo se v prvih sedmih mesecih od nastanka fetusa (glej Jain et al., 2001, str. 9). Za ugotovitev značilnosti prstnega odtisa je najpogosteje uporabljena metoda, ki temelji na prepoznavanju vzorca. Prstni odtis sestavljajo loki, oboki, zasuki, razdelitve in združitve grebenov. Vsak prstni odtis ima okoli trideset vzorcev, ki se med seboj razlikujejo po položaju, sestavi in usmerjenosti. Skupek vseh vzorcev nam prikaže predlog prstnega odtisa.

Za določitev vzorca prstnega odtisa obstajajo različne tehnologije:

- optična,
- termična,
- kapacitivna,
- tehnologija električnega polja,
- senzor brez dotika.

Optična tehnologija uporablja digitalne kamere; prst položimo na stekleno ploščo, preko katere se preslika naš prstni odtis. Je najpogosteje uporabljena tehnologija za preverjanje prstnega odtisa. Termična tehnologija meri temperaturo med vzorci prstnega odtisa in na podlagi teh, naredi celoten prstni odtis. Kapacitivna tehnologija preko električne napetosti in odziva vzorcev na električni tok ustvari sliko prstnega odtisa. Tehnologija električnega polja uporablja meritev električnega polja pod kožo, torej na samih vzorcih. Tehnologija senzorja brez dotika deluje tako, da se prstna blazinica položi na določeno mesto senzorja, kjer se nahaja odprtina, in preko leče se preslika prstni odtis. Sistem zaznavanja prstnega odtisa v tehnologiji brez dotika je zelo podoben tistemu v optični (glej Bača et al., 2006, str. 5).

Prstni odtis kot identifikacijsko orodje za ugotavljanje ali preverjanje identitete se lahko vpelje v vse vrste pametnih kartic. S tem je identifikacija lastnika kartice lažja in zanesljivejša, možnost zlorabe prstnega odtisa kot identifikacijskega orodja pa je zelo nizka.

Podoba obraza

Osnova sistema identifikacije osebe na podlagi obraza je slika obraza. Oblika obraza je jedro človeške identifikacije. Ljudje smo zmožni prepoznati druge obraze kljub spremembam osvetlitve, ozadja, pozicije obraza (profil), velikosti z razdalje, obraznih razpoloženj, pričeske, ličil, barve polti, starosti, nošenju očal. Sistem prepoznavanja obraza, ki temelji na digitalni fotografiji, lokalizira obraz, normalizira njegov izraz in določi značilnosti obraza, preko značilnosti pa odloči o identiteti posameznika.

Mednarodni standardi za biometrične fotografije

Biometrična fotografija vsebuje celoten obraz človeka, del ramena, vrat in lase. Izdelana mora biti na tankem sijajnem fotografskem papirju v velikosti 35 x 45 mm, lahko je v črno-beli ali barvni tehniki. Slika mora pokazati pravo podobo osebe in nikakor ne sme biti retuširana. Fotografirana oseba mora imeti odkrito čelo in obraz, ni dovoljenih nikakršnih pokrival, ki bi oteževala identifikacijo osebe na fotografiji. Poteze obraza morajo biti jasno prikazane, in sicer od konice brade do lasišča, velikost obraza mora zajemati okoli 80 odstotkov površine fotografije. Obraz mora biti enakomerno osvetljen, na sliki ne sme biti nikakršnih senc ali odsevov. Barva in oblika oči morata biti jasno določeni, v primeru rdečih oči je slika ne uporabna. Ozadje mora biti srednje sive barve. V primeru, da ima oseba na sliki svetel odtenek las ali da ima slikana oseba temne lase, mora biti ozadje svetlo sive barve. Ozadje mora biti vedno enobarvno in ne sme vsebovati nikakršnih vzorcev. Pozicija glave mora biti ravna, ne nagnjena, obrnjena ali povešena. Oseba mora biti fotografirana

od spredaj, nos pa se mora nahajati natanko na sredini fotografije. Pogled mora biti usmerjen v fotoaparat naravnost, oči morajo biti odprte in jasno vidne. V primeru da oseba nosi očala, je pomembno, da rob očal in okvirji ne prekrivajo oči (glej Ministrstvo za notranje zadeve, 2006).

Uporaba biometrične slike se je v 21. stoletju povečala, zlasti na področju osebnih dokumentov. Biometrične slike se vse pogosteje vgrajujejo v potne liste in osebne izkaznice. Dogodek 11. septembra 2001 v Združenih državah Amerike je pomenil veliko prelomnico za razvoj osebnih dokumentov, zlasti tistih, ki nam omogočajo potovanja oziroma prehod meja tujih držav. ZDA so po terorističnih napadih razvile program Visa Waiver. Glavni cilj tega programa je, da državam, ki so do zdaj lahko vstopale v ZDA samo s potnim listom in brez vize, v prihodnje ne bo več dovoljevala vstopa z navadnim potnim listom, ampak samo s potnimi listi, ki bodo vsebovali biometrične podatke. Veliko držav po svetu je začelo s projektom vgrajevanja biometrične slike v potne liste ne samo zaradi programa, ki so ga predstavile ZDA, ampak tudi zaradi borbe proti terorizmu, zaradi zvišanja varnosti na mejnih prehodih in letališčih, težjega ponarejevanja dokumentov ter lažjega in hitrejšega identificiranja oseb. Slovenija je avgusta 2006 začela z izdajanjem biometričnih potnih listov, ki imajo vgrajeno biometrično sliko.

Izdaja novih potnih listov je skladna z Uredbo Sveta EU št. 2252/2004 (z dne 13. 12. 2004, v veljavi z 18. 1. 2005) o standardih za varnostne značilnosti in biometrične podatke v potnih listih in potovalnih dokumentih, ki jih izdajo države članice.

Slika šarenice

Prepoznava temelji na unikatnih lastnostih človeške šarenice. Je barven del očesa, ki obkroža črno zenico. Največkrat je metoda uporabljena za identifikacijo, lahko pa tudi za verifikacijo. Prepoznavanje poteka pri vidni ali infrardeči svetlobi. Analizirajo se radialni vzorci, pegice in brazde v šarenici. Šarenica se razlikuje od človeka do človeka in je unikatna pri vsakem človeškem bitju, ni mogoče najti dve osebi z enakim vzorcem šarenice. Zelo pomemben podatek je, da šarenice kirurško ne moremo spremeniti, ne da bi poškodovali oko. Ljudje z umetnim očesom so hitro prepoznavni, saj se njihova šarenica ne odziva na spremembe svetlobe.

Šarenico v biometriji uporabljamo tako, da jo slikamo s kamero z razdalje enega metra. Sistem za preverjanje identitete je preprost; oseba približa oko kameri, ki v nekaj trenutkih odčita sliko šarenice oziroma njene spremembe ob reakciji, ki jo povzroči količina svetlobe, ki ji je šarenica izpostavljena. Vzorec očesne šarenice vsebuje vrsto različnih podrobnosti, ki so celo bolj precizne in edinstvene od prstnih odtisov. Tkivo šarenice sestavljajo naključno porazdeljene točke, kot so: brazde, tvorbe raz, kolagenska tkiva, obroči in pege. Ob povezavi vseh točk, ki tvorijo tkivo šarenice, dobimo edinstven prepoznaven vzorec (glej Wildes, 1997, str. 1349). Šarenica kot biometrični podatek ni zelo razširjena pri identifikaciji in avtentifikaciji oseb. Veliko bolj sta aktualna prstni odtis in biometrična slika. Kljub temu, da obstajajo trditve, ki šarenici dajejo višjo stopnjo verodostojnosti in nezmotljivosti kot prstnemu odtisu, pa predstavlja glavni problem visoka cena tehnologije, ki omogoča ugotavljanje vzorcev šarenice in njeno obdelovanje. Glede na to, da se vedno bolj

izpostavlja pomen vzorca šarenice za zvišanje kakovosti identifikacije oseb, lahko pričakujemo, da bodo v prihodnosti cene padle in bo vzorec šarenice postal eden glavnih biometričnih sredstev za identifikacijo.

Molekula, imenovana deoksiribonukleinska kislina

Bolj poznana kot DNK se največ uporablja v forenzične namene. Za identifikacijo in avtentikacijo osebe v elektronskem poslovanju se še ne uporablja in se najverjetneje tudi v prihodnje ne bo prav kmalu. Spada v področje biometrije in jo lahko označimo kot biometričen podatek.

DNK je okrajšava za deoksiribonukleinsko kislino, ki predstavlja eno-dimenzijsko edinstveno šifrirno kodo vsakega posameznika, izjema sta samo enojajčna dvojčka, ki imata enak DNK (glej Jain et al., 2001, str. 8). Je nosilka genetske informacije v vseh živih bitjih. Glavna naloga DNK je shranjevanje bistvenih informacij. Njegova oblika je dvojna vijačnica, pri čemer se dve verigi ovijeta druga proti drugi. Nahaja se v krvi, slini, tkivih in lasišču. Vzorec DNK lahko pridobimo iz vseh prej omenjenih delov oziroma sestavin človeškega telesa. To je bistvena prednost pred ostalimi biometričnimi podatki, ki se nahajajo samo na enem delu človeškega telesa. Analiza DNK poda identiteto osebe, ki ji je bil odvzet vzorec. Možnost, da bi dve osebi imeli enako sestavo DNK, je praktično nemogoča. Poleg šarenice je najbolj unikaten del človekovega telesa, zato naj bi bila identifikacija na njegovi podlagi nezmotljiva.

DNK se uporablja kot identifikacijski podatek samo v medicini. Problem je v tem, da je potrebno laboratorijsko obdelovanje podatkov in to zahteva čas, čas pa predstavlja dodaten strošek. Problem predstavlja tudi visoka cena laboratorijskega preverjanja značilnosti in ujemanja odvzetega vzorca DNK. V bližnji prihodnosti si le težko predstavljamo uporabo DNK za identifikacijo oseb na področju elektronskega poslovanja. Nedvomno pa je DNK podatek, ki spada v biometrijo, saj je unikaten in preko njega je mogoča identifikacija osebe.

3.5 UPRAVLJANJE IDENTITET, POGLED EVROPSKE UNIJE

Državljani Evropske unije in tudi ostali po svetu živimo v času globalizacije, ki pomeni povezovanje držav in ljudi, ukinitev mej, uvajanje skupnih politik in združevanje celotnega sveta. Ni več mogoče pričakovati, da bomo sami brez povezanosti z drugimi državami lahko konkurirali v svetovnem gospodarstvu in se borili proti nevarnostim. Stopnja varnosti je prišla do najnižje točke. Ljudje se ne počutijo več varni, nevarnosti, ki nas obkrožajo, je vedno več: teroristični napadi, nelegalni prestopi mej, vdori in kraje identitet, vdori v informacijske sisteme gospodarskih družb in podjetij itd. Vsemu temu je treba narediti konec. Povezati je treba moči in narediti pomemben korak naprej v boju proti tem nevarnostim. Kaj je treba narediti, da bo mogoče istočasno povezati gospodarstva in vzpostaviti visoko stopnjo varovanja ljudi in njihovih osebnih podatkov, elementov identifikacije in avtentikacije v elektronskem svetu? Odgovor na to vprašanje postaja vse bolj jasen in potrjen s strani držav v Evropski uniji in tudi ostalih po svetu. Potrebno je upravljanje z identitetami posameznikov na varen, kakovosten in učinkovit način.

Evropska unija želi v čim krajšem času postati najkonkurenčnejša država na svetu z najvišjo stopnjo varovanja svojih državljanov. Vse države članice morajo biti med seboj povezane, politično, gospodarsko, socialno kot tudi na področju informacijsko-komunikacijske tehnologije. Za njeno uvedbo in vzpostavitev je potrebno predhodno povezati vse države članice na ostalih področjih in s skupnimi močmi vpeljati tako informacijsko tehnologijo, ki bo povezovala vse članice na vseh področjih: od uprave in zdravstva do vseh ostalih strok, ki bodo omogočali elektronsko poslovanje.

Spletno poslovanje ne bo več omogočeno samo znotraj države, ampak bodo vpeljani sistemi, ki bodo preverjali identitete vseh državljanov EU. Podatki o državljanih bodo potovali iz ene države v drugo brez oviranja s strani informacijske tehnologije. Na področju uprave bo upravljanje identitet posameznikov temeljilo na tehnologiji, ki bo podpirala identifikacijo vseh državljanov EU, omogočila posredovanje osebnih podatkov v vse države članice in s tem zvišala stopnjo varnosti in omogočila e-upravo ne samo na državni stopnji posamezne članice, ampak tudi na stopnji celotne Evropske unije. Poleg posredovanja osebnih podatkov, zvišanja stopnje varnosti in možnosti uporabe e-uprave na stopnji EU bo tudi znižala stroške, naredila upravo kakovostnejšo, prijaznejšo in odgovornejšo.

Potrebna je uvedba odprtega sistema upravljanja z identitetami, saj bo le tako mogoče vzpostaviti sodelovanje med različnimi resorji in harmonizacijo e-uprav na nivoju unije. Vsaka država uvaja sebi najprimernejše sisteme in tehnologije za upravljanje identitet in osebne dokumente, ki bodo vsebovali elektronske podpise in biometrične podatke. Vendar pa nastane problem, ko želi državljan neke države s svojim identifikacijskim dokumentov opravljati transakcije oziroma poslovati v drugi državi. Problem je v tem, da tehnologija ene članice ne podpira in ne zaznava identitete državljanov drugih članic.

Interoperabilnost

»Pri interoperabilnosti informacijskih in organizacijskih sistemov gre za kompleksnejšo težnjo, da bi bili vsi evropski sistemi med seboj primerljivi, združljivi in povezljivi po tehnični, organizacijski in semantični strani (Petrič, 2008, str. 2).« Nepovezanost je problem, ki se vse pogosteje povezuje z javno upravo. Predstavlja glavno oviro pri vzpostavitvi e-uprave, ki bo obvladovala celotno področje uprave na stopnji države in na stopnji EU. Interoperabilnost je sposobnost informacijsko-komunikacijske tehnologije in poslovnih procesov za podpiranje prenosa in izmenjav podatkov ter prenašanja informacij in znanja. Na področju Evropske unije obstoja projekt, imenovan evropski interoperabilnostni okvir (skrajšano EIO), ki ima postavljen cilj doseči dobro povezavo med različnimi informacijskimi sistemi, postopki in organizacijami. To bi hkrati privedlo tudi k višji preglednosti nad sistemi, podatkovnimi bazami in storitvami.

»Združeni v raznolikosti« je slogan Evropske unije, ki ga je uporabila ob razširitvi iz 15 na 25 članic, z namenom poudariti zavest o edinstvenosti vsake države članice ob hkratnemu povezovanju v Unijo. Ukinitev meja na področju trgovanja je bila prva točka v povezavi EU. Trenutno pa področje ukinitve meja zajema posredovanje in izmenjavo informacij in podatkov državljanov. To pomeni, da različni programi

uporabljajo enake protokole za branje in zapisovanje enakih datotek (glej Frech, 2005, str. 5). Interoperabilnost ne pomeni samo sodelovanje med vladami za olajšanje transakcij fizičnih oseb in izboljševanje razmerij med podjetji, ampak pomeni tudi zniževanje stroškov in skrajšanje časa pri identifikaciji in verifikaciji identitet. Posredovanje podatkov in informacij preko informacijske tehnologije ne predstavlja stroškov glede časovnega razmerja, saj je podatek posredovan v enem samem trenutku. Pomembna je tudi za reorganizacijo delovnega procesa in zvišanje kompatibilnosti. Pomembno je, da je smisel informacij in podatkov, ki se izmenjujejo, razumljiv v vseh sistemih in aplikacijah, ne samo v tistih, v katerih je bil podatek prvotno ustvarjen. S tehničnega pogleda je treba imeti sisteme, ki bodo znali prebrati podatke o identitetah posameznikov, ki se nanašajo na vse državljane Evropske unije, kljub temu da so nastali v eni državi članici, obdelujejo pa se v drugi.

Cilj Evropske unije glede upravljanja identitet je jasen. Zavedamo se, da je upravljanje identitet ključni faktor za: izboljšanje področja gospodarstva in konkurence, uvajanje stopnje varovanja državljanov in njihovih osebnih podatkov ter istočasno izvajanje reforme e-uprave tako na nivoju vsake države članice kot na nivoju celotne Unije. Možnosti posredovanja osebnih podatkov državljanov iz ene države v drugo se še ne realizira, medtem ko se na stopnji posameznih članic znotraj njihovega ozemlja to že uvaja, oziroma imajo že pripravljene projekte, kako bodo to izpeljale. Cilj bo dokončno uresničen šele takrat, ko bo celoten proces upravljanja identitet deloval enotno na stopnji Evropske unije.

3.5.1 Pojav velikega brata

Antiutopičen roman pisatelja Georga Orwella z naslovom »1984« je v petdesetih letih prejšnjega stoletja opisoval mračen prikaz družbe v prihodnosti. Glavni koncept romana, ki ga v današnjem času uporabljamo v povezavi z elektronskim poslovanjem, razvojem informacijske tehnologije in današnjo družbo, ki temelji na internetu, je tako imenovan pojav Big brotherja (velikega brata), ki nas opazuje in sledi vsakemu našemu koraku.

Vprašanje zasebnosti v tako imenovani informacijski družbi in specifično vprašanje pooblastil državnih varnostnih in obveščevalnih organov pri zatiranju terorizma, organiziranega kriminala in kriminala, povezanega z računalniki, predstavlja enega ključnih pravno-sociološko-etničnih vprašanj. Hkrati pa ta ista tehnologija prinaša s sabo veliko nevarnost, in sicer ožanje življenjskega prostora ene najbolj temeljnih človekovih pravic, tj. pravice zasebnosti (glej Klemenčič, 2001, str. 11). Zasebnost in pojav velikega brata se vse pogosteje pojavljata v povezavi z upravljanjem identitet posameznika, saj utemeljujeta strah ljudi pred vohunjenjem državnih organov v njihove zasebne podatke.

Zmanjševanje zasebnosti in svobode bosta, če nekaj ne naredimo, postopoma zasenčile vse pozitivne komponente sistema upravljanja identitet. Kritiki se vse bolj opirajo na ti dve točki in zanemarjajo vse ostale prednosti, ki jih tak sistem prinaša. Povečanje stopnje varnosti, izboljšanje elektronskih storitev in lažji dostop vanje, skrajšanje čakalnih vrst, zniževanje stroškov, zvišanje konkurence je le nekaj prednosti, ki jih sistem upravljanja identitet prinaša s seboj. Če dobro analiziramo

situacijo, pridemo do dvoreznega meča. Na eni strani imamo zvišanje stopnje varnosti in konkurenčnosti, na drugi pa vprašanje zasebnosti človeka in njegove pravice do nedotakljivosti njegovih osebnih podatkov. Kaj je pomembnejše, čemu se v 21. stoletju ne moremo izogniti in kaj bo za nas koristnejše, so vprašanja, na katera je težko odgovoriti oziroma je odgovor odvisen od vsakega posameznika. Dejstvo pa je, da je nemogoče doseči visoko stopnjo varovanja podatkov ob nedotakljivosti človekove zasebnosti. Hkrati pa nihče ne more zagotovo trditi, da programi in sistemi za identifikacijo posameznikov ne bodo privedli do zlorabe tajnih podatkov.

»Veliki brat« pa v sistemu upravljanja identitet poleg vdora v osebne podatke lahko pomeni tudi samo krajo identitete in možnost uporabe denarnih sredstev. Obstaja pa tudi možnost, da bi sami državni organi oziroma vsi, ki bi imeli dostop do elektronske identitete posameznika, lahko pridobivali informacije, ne samo o finančnem stanju državljana, ampak tudi o njegovih zdravstvenih, spolnih in družinskih značilnostih.

V primeru, da bi prišlo do zlorabe takih podatkov, je za zaščito zasebnosti in dostojanstva osebe potrebno izoblikovati zakonske okvirje, ki bi tako zlorabo ustrezno kaznovali in izničili katere koli odločitve, ki bi bile sprejete na podlagi podatkov, ki so bili nezakonito pridobljeni. Strah ljudi pred pojavom »nekdo vas vedno opazuje« povzroča nezaupanje in negativni pristop do novih tehnologij in sistemov, ki upravljajo identitete, ter samim pojavom identificiranja ljudi preko kartic, čipov, identifikacijskih številk, elektronskih podpisov ali biometričnih podatkov. Sistemi bi morali delovati tako, da identificirajo, ne pa tudi izdajajo samo identiteto. Zato je treba ustvariti take sisteme, ki bodo preprečevali prenos podatkov iz enega sistema v drugega, razen v primerih, ki so določeni z zakonodajo. Treba je strogo določiti mejo med sistemi, tako da se ne bodo mogli pomešati podatki s strani zdravstva, uprave, poslovnega področja itd. Zakonsko in tehnološko je treba onemogočiti tak pojav in vpeljati tako zanesljive sisteme, ki bodo zagotavljali varnost osebnih podatkov na najvišji možni ravni. »Pomembno je da postanemo pozorni na možnost zbiranja podatkov in vdora v zasebnost, še sploh s strani države. Ker če njenemu delovanju na tem področju niso postavljene nobene meje, lahko slednje predstavlja potencialno grožnjo za demokracijo in svobodo (Ficko, 2007, str. 172).«

Moj osebni pogled na omenjeno situacijo glede zbiranja podatkov je sledeč: Osebno me ne skrbi samo zbiranje podatkov, sama se ob tem celo počutim varnejša. Skrbi pa me, ali so podatki dovolj dobro zavarovani in ali se z njimi upravlja dovolj profesionalno in nepristransko. Temeljno vprašanje je torej, kdo, kdaj in zakaj bo dostopal do mojih tajnih podatkov in ali se bodo uporabljali za namen, zaradi katerega so se prvotno zbirali. Prav zato je to poglavje potrebno zelo poglobljeno pravno urediti in zaščititi, »saj nadzor že dolgo ni več vprašanje tehnologije, temveč predvsem zakonodaje (Ocvirk, 2003, str. 49).«

4 PRIMERI UPRAVLJANJA IDENTITET POSAMEZNIKA V IZBRANIH DRŽAVAH

4.1 ELEKTRONSKA OSEBNA IZKAZNICA

Možnost dostopa do elektronskih storitev kadar koli in kjer koli je predhodna zahteva za vzpostavitev konkurenčno-dinamičnega okolja, ki temelji na znanju in sposobnosti obvladovanja. Taka družba prinese s seboj tveganja na področju varnosti. Za zmanjšanje tveganj je treba ustvariti dovolj sposobno in močno metodo avtentikacije in identifikacije, ki bo lahko onemogočila in zmanjšala stopnjo tveganja na področju varnosti.

Pomembno povezavo med informatizirano družbo in elektronsko identifikacijo in avtentifikacijo državljanov predstavlja elektronska osebna izkaznica. To je pametna kartica, ki vsebuje zasebni ključ, ta pa podpira javni ključ, digitalni certifikat in biometrične podatke lastnika. Omogoča elektronsko podpisovanje dokumentov preko elektronskega podpisa in njena uporaba se ne navezuje samo na področje e-uprave, ampak tudi na e-plačila, e-zdravstvo, e-transport. Preko nje pa je tudi možno voliti in oddajati napoved za dohodnino. Predstavlja rešitev za e-identifikacijo posameznika in jamči istovetnost osebe pri dostopanju do e-storitev, omogoča varen prenos podatkov in e-transakcije ter digitalni podpis in varovanje vseh sodelujočih strank pri elektronskem poslovanju. V kakšnem obsegu se lahko elektronsko osebno izkaznico uporablja oziroma kolikšna je njena sposobnost, je odvisno od vsake države posebej. Predvsem glede na to, koliko od zgoraj navedenih področij je v posamezni državi informatiziranih, koliko storitev je mogoče opraviti preko spleta in koliko državljani sploh uporabljajo tak način poslovanja. Večina držav je projekt uvedbe elektronske osebne kartice že razvila ali ga razvija in ga poskuša realizirati. Nekatere države ga že imajo, nekatere pa niso izrazile zanimanja na tem področju.

Države, ki že imajo e-ID (okrajšava za elektronsko osebno izkaznico), so: Finska, Belgija, Italija, Avstrija, Španija, Estonija in Švedska. Tri evropske države so sprejele odločitev o uvedbi take osebne izkaznice, in sicer Nizozemska, Francija in Slovenija. Malta se je odločila, da bo izkaznico uvedla, ampak ne v obliki pametne kartice. Zakaj ostale države nimajo interesa v tem projektu, ni povsem znano, lahko pa so razlogi naslednji: zadržanost oziroma nezaupljivost državljanov do uporabe elektronske izkaznice, visoki stroški implementacije infrastrukture javnega ključa (PKI) ali nizka valorizacija njene uporabe s strani uprave.

Fizične in pravne osebe (podjetja) je treba poučiti in prepričati o prednostih, ki jih prinaša uporaba elektronske izkaznice, kot so: varnejše in bolj legitimno poslovanje, 24-urna dostopnost do storitev, varnejša e-komunikacija in enostavnejše izdajanje tega dokumenta ter spreminjanje vsebovanih osebnih podatkov. Zvišanje povpraševanja po elektronskih osebnih izkaznicah s strani državljanov in s strani pravnih subjektov bi za posledico imelo vlaganje držav v ta projekt. Razlog bi bil istočasno informatiziranje družbe ob pokritju stroškov razvoja zaradi visokega povpraševanja.

4.2 PRIMERI ELEKTRONSKE OSEBNE IZKAZNICE V ŠPANIJI

Decembra leta 2003 je španski parlament sprejel novi zakon o elektronskem podpisu, s katerim so želeli razširiti uporabo digitalnih podpisov za e-trgovino in e-upravo. Zakon predstavlja legalni okvir za prihodnji razvoj nacionalne elektronske osebne izkaznice. Španski ministrski svet je februarja 2004 uradno odobril kreiranje in distribucijo novih elektronskih izkaznic z biometričnimi identifikacijskimi elementi, ki zagotavljajo varno identifikacijo in avtentičnost podatkov na dokumentu in s tem varen dostop državljanov do transakcij elektronskih storitev.

Vlada je leta 2006 predstavila nove izkaznice z biometričnimi identifikatorji in elektronskim podpisom. Projekt je vodilo Ministrstvo za notranje zadeve v sodelovanju z Ministrstvom za javno upravo in nacionalno policijo. Nova izkaznica omogoča digitalno podpisovanje dokumentov in pogodb, identifikacijo in dokazovanje državljanov v varnem digitalnem okolju in enostaven, hiter in ugoden dostop do e-storitev. Elektronska osebna izkaznica pa poleg tega, da služi kot identifikacijski dokument v virtualnem svetu, služi tudi kot identifikacijski dokument državljana v realnem svetu. To sposobnost ji dajejo na obeh straneh izkaznice natisnjeni podatki, ki omogočajo identifikacijo imetnika že na prvi pogled. Na sprednji strani so natisnjeni naslednji podatki:

- ime lastnika,
- prvi in drugi priimek,
- spol,
- državljanstvo,
- rojstni datum,
- številka osebne izkaznice,
- datum poteka,
- čas, v katerem je osebna izkaznica veljavna,
- identifikacijska številka državljana.

Na hrbtni strani pa naslednji:

- kraj rojstva, pokrajino in državo,
- imena staršev,
- naslov stalnega bivališča,
- mesto prebivanja,
- številka pisarne, v kateri so izkaznico izdali ali informacija OCR-B za elektronsko branje o identiteti državljana preko normative OACI za potovalne dokumente (glej Comision tecnica de la implementacion del DNI eletronico, 2006, str. 5).

Po zaključku začetnega testiranja leta 2006 so začeli redno izdajati kartice in do marca 2007 so jih izdali več kot 420.000. Izdaja kartic se je postopoma razširila, tako da so zdaj na voljo po vsej Španiji. Nekatere institucije, kot je na primer davčni urad, so uvedle storitve, ki so kompatibilne s kartico, kot na primer davčna napoved zasebnikov. Do februarja 2007 je bilo razvitih 260 storitev na vseh nivojih uprave, do

katerih je mogoče dostopati z elektronsko osebno izkaznico (glej Ministrstvo za notranje zadeve, Španija - pokazatelji rasti elektronske osebne izkaznice).

4.2.1 Veljavnost izkaznice

Veljavnost izkaznice je odvisna od starosti podpisnika:

- 5 let, ampak le v primeru, ko podpisnik ni star 30 let v trenutku, ko je izdana,
- 10 let v primeru, ko je podpisnik starejši od 30 let in mlajši kot 70 let,
- nedoločen čas, ko je podpisnik starejši od 70 let (glej Zakon o osebni izkaznici in certifikatu elektronskega podpisa v Španiji, 6. člen).

Paziti je treba na veljavnost potrdila znotraj čipa, ki ga vsebuje elektronska osebna izkaznica, saj so veljavna 30 mesecev (po preteku tega roka je treba kartico potrditi na avtomatu).

4.2.2 Pravne podlage

V Španiji so temeljne pravne podlage za področje elektronske osebne izkaznice naslednje:

- Direktiva 1999/93/CE evropskega parlamenta in komisije, preko te se je vzpostavil okvir za vse evropske države ob uveljavitvi elektronske osebne izkaznice,
- Zakon 59/2003, 19. december, Elektronski podpis,
- Zakon 15/1999, 13. december, Varovanje podatkov,
- Dekret 1553/2005, 23 december, elektronska osebna izkaznica in elektronski podpis dobijo pravno veljavo (glej Ministrstvo za notranje zadeve Španija − Funkcije in pravna podlaga elektronske izkaznice).

4.2.3 Proces izdaje osebne izkaznice

V Španiji se osebne izkaznice ne izdajajo na upravnih enotah, kot se to izvaja pri nas. Za to so odgovorne policijske postaje, v katerih so posamezni oddelki, ki pokrivajo upravna področja.

Pogoj za izdajo izkaznice pri prvi izdaji je osebna navzočnost. S seboj je treba imeti rojstni ali potni list ter izpisek iz matične knjige, ki vsebuje naslov prebivališča. Predpogoj je, da nobeden od zgoraj naštetih dokumentov ni starejši od treh mesecev. S seboj je treba prinesti dve digitalni sliki obraza v barvah v velikosti 32 x 26 mm. Oseba na sliki mora gledati v fotoaparat brez dodatkov na lasišču ali temnih stekel oziroma kakršnih koli drugih lepotnih dodatkov, ki bi lahko onemogočali prepoznavnost osebe na sliki (glej Ministrstvo za notranje zadeve Španija − Postopek izdaje elektronske izkaznice).

4.2.4 Vrste mehanizmov, operacijskih sistemov in standardov, ki podpirajo elektronsko osebno izkaznico

Za uporabo elektronske osebne izkaznice moramo imeti nekatere računalniške aparate in programe, ki bodo dovolili dostop do čipa in s tem dostop do informacij oziroma podatkov, ki se nahajajo v čipu. Osebni računalnik in čitalec pametnih kartic, ki podpira standard ISO-7816, sta osnovna pogoja.

Za pravilno delovanje elektronskih osebnih izkaznic mora biti računalniška oprema opremljena z ustreznimi programi, ki se imenujejo kriptografski modeli. V Microsoft sistemu mora oprema imeti funkcijo, ki se imenuje Cryptographic service provider (CSP). V Unixu, Linexu in Macu pa lahko uporabljamo izkaznico preko kriptografskega modela, ki se imenuje PKCS#11 in določa standarde za uporabo pametnih kartic in izvajanje kriptografskih operacij.

4.3 PRIMER ELEKTRONSKE OSEBNE IZKAZNICE V ITALIJI

Italijanska elektronska osebna izkaznica je pametna kartica, ki vsebuje osebne in biometrične podatke državljana. Ima enake funkcije kot stara osebna izkaznica. Sicer služi kot dokazni dokument identitete državljana. Njene nove funkcije pa so možnost identifikacije v virtualnem, spletnem svetu.

Državljani lahko uporabljajo svojo novo izkaznico za dostop do spletnih strani, na katerih bodo lahko imeli dostop do vseh podatkov in informacij, ki so na spletu in je do njih mogoče priti le preko spletne identifikacije, ki temelji na osebni izkaznici. Vsa podjetja, ki bodo želela imeti dostop do svojih storitev preko spleta, se morajo registrirati pri Ministrstvu za notranje zadeve. Na ta način je mogoče zavarovati tako pravice državljanov kot tistih, ki zagotavljajo storitve (glej Arcieri et al., 2004, str. 1).

V Italiji imajo dve vrsti pametnih kartic: že zgoraj omenjene elektronske osebne izkaznice in nacionalno kartico za storitve (carta nacionale dei servizi – CNS). Obe se lahko uporabljata za dostop do elektronskih storitev. Razlika med njim je v tem, da prva služi tudi kot identifikacijski dokument identitete državljana. Glede na to, da elektronska osebna izkaznica služi kot identifikacijski dokument, ima na sprednji strani natisnjene podatke o imetniku. Podatki, ki so natisnjeni na izkaznici, so naslednji:

- ime in priimek lastnika,
- datum in kraj rojstva,
- spol,
- višina,
- naslov stalnega prebivališča,
- slika,
- prstni odtis obeh kazalcev,
- občina, v kateri je bila izkaznica izdana,
- številka dokumenta,
- datum izdaje izkaznice in preteka,

- državljanstvo,
- podpis,
- v predelih, kjer je uradnih več jezikov, to je na severu, morajo biti podatki zapisani tudi v nemškem oziroma francoskem jeziku (glej Wikipedia, 4. 9. 2008).

V izkaznici je vgraviran mikročip, ki vsebuje infrastrukturo javnega ključa (PKI). Mikročip omogoča višjo stopnjo varovanja zasebnega ključa in vseh ostalih podatkov, ki se navezujejo na identiteto posameznika. Italija si prizadeva, da bi v prihodnje na izkaznici lahko bili dodani podatki, povezani z zdravstvenim stanjem, zavarovanjem, pokojnino itd. Mikročip omogoča, da se v njega lahko dodajajo, brišejo ali spreminjajo podatki, ne da bi bilo treba kartico menjati.

Leta 2001 je Italija začela izdajati elektronske osebne izkaznice, ki imajo za osnovo infrastrukturo javnega ključa (PKI). Da bi državljani uporabljali elektronske osebne izkaznice in se nanje navadili, so bile na začetku brezplačne. Izdajo se lahko osebam, starejšim od 15 let, potreben pa je podpis staršev. Za razliko od potnega lista se jo dovoli izdati tudi nedržavljanom Italije, ki morajo imeti prijavljeno stalno prebivališče v Italiji. Veljavnost osebne izkaznice v Italiji se izteče po petih letih (glej Wikipedia, 11. 9. 2008).

Kabelska televizija je v Italiji zelo popularna. Ima jo velika večina gospodinjstev. Zato želijo v prihodnje omogočiti dostop do javnih storitev ne samo preko interneta, ampak tudi preko kabelske televizije in mobilne telefonije, ampak o tem ni še zgrajenih nobenih temeljnih predpostavk oziroma projektov.

4.4 PRIMER ELEKTRONSKE OSEBNE IZKAZNICE V ESTONIJI

Estonija je začela s projektom elektronske osebne izkaznice v letu 2000, izdajati pa so jih začeli v letu 2002. Za razliko od ostalih držav je elektronska izkaznica dokument, za katerega lahko zaprosijo vsi državljani Estonije, ki so starejši od 15 let.

Uporaba izkaznice temelji na čitalcu pametne kartice, ki se namesti na domačem računalniku, druga možnost pa je preko infotočk. Izkaznica je primarni dokument identifikacije državljanov. Uporabna je lahko na različnih področjih, tako v zasebnem, kot v javnem sektorju. Poleg sposobnosti fizične identifikacije njenega lastnika ima še elektronske funkcije za enostavno in varno avtentikacijo.

V izkaznico je vgrajen mikročip, ki vsebuje osebne podatke, digitalno potrdilo o avtentičnosti, edinstven elektronski naslov in potrdilo o elektronskem podpisu. Elektronski naslov, ki je zapisan v mikročipu, je sestavljen iz imena, priimka in štirih številk, ki zagotavljajo unikatno identifikacijo osebe. Štiri številke zagotavljajo unikatno identifikacijo osebe v primeru, ko obstaja več ljudi z enakim imenom in priimkov (glej The estonian ID card and Digital signature concept, 2003, str. 7). Elektronski naslov se s potekom izkaznice in menjavo potrdil ne spreminja, njegova veljava ni povezana s časovnim obdobjem. Podatki o imetniku izkaznice imajo veljavnost deset let. V primeru, da so se podatki spremenili, na primer sprememba

priimka pri ženskah, je treba podatek na izkaznici ustrezno spremeniti, medtem ko je treba potrdila oziroma certifikate po treh letih obvezno obnoviti.

Podatki o njenem imetniku pa se ne nahajajo samo v mikročipu, ampak tudi na sami izkaznici**.** Na sprednji strani so natisnjeni naslednji podatki:

- ime in priimek lastnika,
- lastnoročni podpis,
- slika,
- datum rojstva,
- naslov stalnega prebivališča,
- številka izkaznice in koda državljana (national ID code),
- spol,
- datum poteka izkaznice.

Na hrbtni stran pa naslednji:

- mesto rojstva,
- datum izdaje izkaznice,
- številka kartice in kodo državljana v šifrantih (glej Wikipedia, 3. 9. 2008).

Estonija sodi na najvišja mesta na lestvici razvitosti e-poslovanja na vseh področjih. Več kot polovica prebivalstva ima elektronske osebne izkaznice in preko njih dostopa do vseh elektronskih storitev. Državljani so osveščeni glede informacijske tehnologije in prednosti, ki jih ta nudi. Pilotni projekt elektronske osebne izkaznice, ki ga je izvedla leta 2002, je zgradil trde temelje in državljane vpeljal v svet elektronskega poslovanja in elektronskih identitet. Papirnato poslovanje se umika in vse bolj se uporablja elektronska povezava. Poleg tega so skrajšali čakalne dobe in znižali stroške poslovanja. Delež ljudi, ki uporabljajo ta sistem, je jasno razviden že po podatku, da več kot 70 odstotkov davčnih zavezancev odda dohodninsko napoved v elektronski obliki, kar je izjemno visoka številka v primerjavi z ostalimi državami. Potrebno pa je tudi poudariti, da je bila Estonija prva država, ki je uvedla volilni sistem preko interneta, in sicer za volitve na lokalni ravni leta 2005 (glej E-government in Estonia, 2007, str. 4). Estonija mora biti za vzgled in primerjavo glede razvoja elektronskega poslovanja, števila izdanih elektronskih izkaznic in glede stopnje informatiziranja družbe in osveščanja njenih državljanov.

4.5 SLOVENSKA ELEKTRONSKA OSEBNA IZKAZNICA

Vedno večje število storitev e-uprave, ki se nahajajo na portalu e-uprave, je razvilo zanimanje za vgraditev kvalificiranega digitalnega potrdila v osebno izkaznico. Tako bi jo iz navadne spremenila v elektronsko. Osebna izkaznica je tako kot v drugih državah tudi v Sloveniji najbolj razširjen identifikacijski dokument. Z vgrajenim potrdilom bo postala dokument za identifikacijo tudi v virtualnem svetu.

Za izdelavo nove osebne izkaznice bodo lahko zaprosili vsi državljani, starejši od 15 let, tudi tisti, ki imajo prijavljeno stalno prebivališče v tujini. Nova osebna izkaznica se

bo izdala po želji in tudi v prihodnje ne bo obvezen dokument. Ob izdaji novih izkaznic bodo stare veljale do preteka roka njihove veljavnosti.

Zakon o spremembah in dopolnitvah osebne izkaznice (Uradni list RS. Št. 44/2008, ZOIzk-B) bo elektronsko osebno izkaznico z digitalnim potrdilom razširil tudi na uporabo na področju zdravstva, za uveljavljanje zdravstvenih storitev. S tem bomo zmanjšali število dokumentov, znižali stroške in zvišali stopnjo varnosti. Saj zdravstvena kartica, ki jo zdaj uporabljamo nima slike, medtem ko elektronska osebna izkaznica vsebuje sliko njenega imetnika.

Ob vložitvi vloge za izdajo osebne izkaznice bo imel vsak državljan prosto izbiro pri odločitvi o tem, ali bo izkaznica vsebovala mikročip ali ne. V primeru, da bo mikročip vgraviran, bo odločal še o tem, kakšna potrdila naj mikročip vsebuje. Možne so tri opcije:

- osebna izkaznica, ki vsebuje kvalificirano potrdilo za opravljanje storitev e-uprave,
- osebna izkaznica, ki vsebuje dostop do podatkov zdravstvenega zavarovanja,
- osebna izkaznica, ki vsebuje oboje (glej Ministrstvo za notranje zadeve, 2008).

Register o osebnih izkaznicah in register o zdravstvenem zavarovanju bosta povezana med seboj, vendar le v taki meri, da bo mogoče preveriti, ali je oseba zdravstveni zavarovanec ali ne, ne bo pa možnosti dostopa do številke zdravstvenega zavarovanja.

Veliko polemike je bilo glede vprašanja izdelave ene izkaznice, ki bi služila kot osebna izkaznica, kakor tudi kot zdravstvena izkaznica. Delikatno področje predstavljajo zdravstveni podatki imetnika izkaznice in z njimi povezana bojazen, da bi lahko s pomočjo elektronske osebne izkaznice prišli do podatkov povezanih z zdravstvenim stanjem njenega imetnika. Mnenja strokovnjakov so deljena. Na primer: Nataša Pirc Musar meni (Dnevnik, 2008), da bi v primeru fotokopiranja osebne izkaznice nekomu dali tudi našo številko zdravstvenega zavarovanja (ta bo namreč natisnjena na izkaznici, a le v primeru, ko bo to imetnik sam želel), kljub temu da jo upravljavec zbirke ne potrebuje. Negativno se je prav tako odzval profesor Bojan Bugarič, ki meni (Dnevnik, 2008), da gre za nedomišljen projekt, ki opira številne polemike, zlasti glede povezave baz podatkov, ki dodatno povečujejo moč oblasti, ki s tem širi področje nadzora nad posameznikovo zasebnostjo. Ministrstvo za notranje zadeve pa se brani z argumentom, da bodo vsi trije registri (osebnih izkaznic, zdravstvenih zavarovanj in izdanih kvalificiranih potrdil) ostali avtonomni in med seboj ločeni. Poleg tega pa na ministrstvu trdijo, da bo vsak dostop zabeležen in bo sama uporaba osebne izkaznice mogoča le ob vnosu PIN kode.

Nove osebne izkaznice se bodo začele izdajati po uskladitvi pravilnika o izvrševanju Zakona o osebni izkaznici. Poleg tega še ni določeno, kdo bo nove osebne izkaznice izdeloval. »Na področju zdravstva se bodo lahko začele uporabljati takoj, ko bodo to omogočali predpisi s področja zdravstva in ko bo uveden ustrezen informacijski sistem (Wikipedia, 12. 9. 2008).«

Veljavnost izkaznice polnoletnim osebam ostane enaka, in sicer deset let, za mladoletne pa bo veljavnost naslednja: otrokom do treh let se bo izkaznica izdala samo za tri leta. Mladoletnim osebam med tretjim in petnajstim letom pa za pet let. V primeru da državljan v petih letih izgubi ali pogreša dve ali več izkaznic, se mu izda listina le za obdobje enega leta.

Podatki na osebni izkaznici

Elektronska osebna izkaznica bo vsebovala naslednje podatke:

- ime in priimek,
- EMŠO,
- sliko,
- rojstni datum,
- spol,
- državljanstvo,
- stalno prebivališče,
- datum izdaje in veljavnosti izkaznice,
- serijsko številko osebne izkaznice,
- pristojni organ,
- lastnoročni podpis.

V primeru, da imetnik ne sme prestopiti državne meje, mora biti to označeno na izkaznici.

Državljanu, starejšemu od 15 let, se lahko izda izkaznico z mikročipom, na katerem je kvalificirano digitalno potrdilo državnega overitelja. V potrdilu so poleg podatkov, ki jih določa zakon o elektronskem podpisu, zapisani še ime in priimek, serijska oziroma registrska številka osebne izkaznice ter EMŠO in davčna številka. Zadnja dva podatka sta zapisana v kriptografsko zaščiteni obliki, ki onemogoča nepooblaščeni dostop (glej ZOIzk-B, 6. člen). Na dvojezičnih območjih (Primorska in Prekmurje), bodo vsi podatki zapisani tudi v italijanskem oziroma madžarskem jeziku .

Slovenija bo z uvedbo elektronske osebne izkaznice odprla vrata v elektronsko poslovanje na področju javnega in zasebnega sektorja. Za uresničitev takega projekta je potrebna podpora s strani vseh državnih institucij. Najprej je treba uskladiti vso zakonodajo, da bo lahko elektronsko poslovanje uspešno delovalo, poleg tega pa mora biti nova osebna izkaznica usklajena s standardi, ki veljajo za vse države (polikarbonat, digitalna potrdila, čip, aplikacije, ki podpirajo uporabo digitalnega potrdila ...). Uporaba bo mogoča preko infotočk, ki bodo lahko v lasti tako zasebnega kot javnega sektorja, druga opcija pa je preko osebnega računalnika, z namestitvijo čitalca pametnih kartic.

V prihodnje bo omogočeno imetnikom elektronske osebne izkaznice opravljati celo vrsto elektronskih storitev s področja javnega in zasebnega sektorja. Možen bo tudi dostop do zdravstvenih in finančnih podatkov. Z razvojem e-registrov bo mogoč tudi dostop do njih in preko njih opravljati storitve, ki so vezane na podatke iz e-registra. Omenja se tudi možnost e-demokracije, ki omogoča elektronske volitve. V prihodnje

lahko torej pričakujemo, da bo elektronska osebna izkaznica služila tudi kot zdravstvena, bančna, kreditna kartica in izkaznica socialnega zavarovanja, po sistemu »ena za vse«.

Članice Evropske unije, ki že imajo elektronske osebne izkaznica, in tiste, ki projekt šele izvajajo, med njimi je tudi Slovenija, poskušajo med seboj vzpostaviti medsebojno sodelovanje, ki temelji na priznavanju različnih nacionalnih shem na področju elektronske identifikacije. Cilj projekta je zmanjšanje in postopna ukinitev tehnoloških meja in postopno priznavanje elektronskih identitet drugih držav. To bo omogočilo poslovanje preko elektronskih osebnih izkaznic tudi v drugih državah članicah in ne samo v državi, kjer je bila izkaznice izdana.

Potreba po elektronskih osebnih izkaznicah je vsak dan večja. Glede na to, da so nekatere države projekt elektronskih izkaznic že uresničile, nekatere med njimi uspešneje, druge manj, imamo mi priložnost, da se izognemo njihovim napakam. Pred samo izvedbo projekta pa je potrebno temeljno razmisliti, kako bomo hkrati uspešno izvedli projekt in zaščitili pravice državljanov, povezane z varstvom osebnih podatkov.

5 ZAKLJUČEK

Spremembe v družbi so v devetdesetih letih prejšnjega stoletja povzročile spremembe v načinu poslovanja javne uprave. V Sloveniji je bilo na omenjenem področju prelomno leto 2001, ko smo dobili prvi elektronski portal v upravi. Internet, nove tehnologije, elektronska pošta, elektronski portali in hitrejši ritem življenja so povzročili spremembe tudi na področju zahtev uporabnikov. Zahtevane so hitre in kakovostne storitve, podprte z visoko stopnjo varnosti. Vse mora temeljiti na visoki tehnologiji, s čim nižjimi stroški poslovanja. Zahtev in pričakovanj ni lahko uresničiti, potrebna je sestava strategije, ki bo na dolgi rok omogočila sistem delovanja uprave, ki bo uresničevala zahteve in jih sproti nadgrajevala in dopolnjevala. Živimo v skrajno dinamični in spreminjajoči se družbi. Za uspešno delovanje sistema, v našem primeru sistema elektronskega poslovanja v upravi, je treba osnovati sistem, ki bo prilagodljiv na spremembe v družbi in se hkrati s spremembami spreminjal tudi sam. Znal bo slediti toku življenja v družbi. Področje varovanja je temeljni pogoj za uspešnost in kakovost elektronskega poslovanja v upravi. Predstavlja sestavni del, brez katerega sistem ne more delovati, kaj šele prilagajati in odzivati se na vse spremembe in nevarnosti, ki mu prihajajo naproti.

V svojem delu sem kot rešitev problema varnosti pri elektronskem poslovanju v upravi predstavila področje upravljanja z identitetami posameznikov, z možnostjo uvajanja zelo visoke stopnje varovanja, ki hkrati daje sistemu veliko fleksibilnost za prilagajanje na spremembe. Menim, da projekti pametnih kartic, ki temeljijo na infrastrukturi javnih ključev in vsebujejo biometrične podatke, predstavljajo svetlejšo prihodnost v e-upravi tako z globalnega vidika kot z vidika posamezne države. Enostavna uporaba, zelo visoka stopnja varovanja in tehnološka izpopolnjenost predstavljajo ključ za nadgradnjo poslovanja e-uprave. Z istočasno sposobnostjo varovanja občutljivih podatkov uporabnikov in posledično zviševanja zaupanja v elektronske storitve uprave bo takšna uporaba pripomogla k rasti povpraševanja po omenjenih storitvah. Dejstvo je, da se večina držav, ki imajo elektronske uprave s storitvami na spletu, soočajo z nizkim povpraševanjem državljanov po taki vrsti storitev in visok delež prebivalstva ne zaupa v tako vrsto poslovanja, predvsem zaradi strahu pred neustreznim varovanjem njihovih podatkov in prepričanjem, da je star sistem varnejši in enostavnejši.

V zadnjem delu diplomske naloge sem kot primer pametne kartice, ki omogoča varno elektronsko identifikacijo, predstavila projekte elektronskih osebnih izkaznic v izbranih državah. Izbrane države so: Španija, Italija, Estonija in Slovenija. Elektronska osebna izkaznica je osebni dokument, ki omogoča identifikacijo njegovega imetnika v elektronskem svetu in predstavlja primer povezave z elektronskim poslovanjem preko upravljanja identitet. Digitalna potrdila, ki jih vsebuje elektronska osebna izkaznica, omogočajo elektronski podpis in s tem možnost podpisovanja elektronskih dokumentov, hkrati pa infrastruktura javnega ključa zagotavlja zelo visoko stopnjo varovanja. Ob vgraditvi biometričnih podatkov v mikročip, ki se nahaja na kartici, bi bila možnost zlorabe kartice in njenih podatkov skoraj nemogoča.

Elektronska osebna izkaznica je projekt, ki ga pospešeno uresničuje večina članic Evropske unije, saj varna e-identifikacija predstavlja osnovni pogoj za kakovostno in varno e-poslovanje v upravi. Projekt elektronske osebne izkaznice se izvaja tudi v Sloveniji, vendar se izkaznice še ne izdajajo. Treba je narediti zelo kakovosten projekt, kako osebne izkaznice realizirati, do katerih storitev bomo z identifikacijo preko osebne izkaznice lahko dostopali in ali bo služila tudi kot zdravstvena kartica, v kateri bodo naši podatki v zvezi z zdravstvenim zavarovanjem. Poleg kakovostne sestave in izvedbe projekta je potrebna tudi podpora s strani vseh vej oblasti. Stimulacija in promocija takega projekta sta ključnega pomena. Uporabnike teh storitev je treba prepričati, da je prav v upravljanju identitet skrit ključ do uspešne e-uprave, ki bo prinesla veliko pozitivnega za uporabnike in za samo državo.

Ob koncu pisanja diplomskega dela sem prišla do spoznanja, da tak sistem predstavlja rešitev glede varnosti in lažje povezanosti upravnih področij znotraj samih držav, pa tudi področij znotraj Evropske unije. Vendar pa so za ustrezno zvišanje povpraševanja po storitvah in stopnje zaupanja potrebne še druge dopolnitve in spremembe. Preko upravljanja identitet lahko zgradimo stabilen, kakovosten in dinamičen sistem elektronskega poslovanja na področju uprave. Prav takšnega namreč nujno potrebujemo tako z vidika gospodarstva, konkurence, globalizacije kot z vidika potreb uporabnikov.

Dejstvo je, da prihodnost temelji na informacijski tehnologiji in svetovnem spletu. Moramo se zavedati, da živimo v času sprememb, na katere se je treba prej ali slej prilagoditi. Manj ko se bomo upirali dejstvom, katerim se ni mogoče izogniti, prej bomo lahko naš sistem delovanja dogradili, izpopolnili in ga naredili konkurenčnega v primerjavi z ostalimi, kar pa bo pozitivno vplivalo na celotno državo in ne samo na področje javne uprave.

LITERATURA

MONOGRAFIJE:

PAVLIHA, M. in JERMAN BLAŽIČ, B. Zakon o elektronskem poslovanju in elektronskem podpisu s komentarjem. GV založba, Ljubljana, 2002.

VINTAR, M. in GRAD J. E-uprava: Izbrane razvojne perspektive. Fakulteta za upravo, Ljubljana, 2004.

ČLANKI:

BAČA. M. et al. Prstom otključaj vrata. Zaštita, časopis o zaščititi i sigurnosti osebe i imovine. Zagreb, 2006, let. 2, št. 2, str. 5.

CASASSA MONT, M. et al. Identity management: a Key e-Bussines Enabler. L' Aquila. 2002, let. 16 , št. 8 str. 1. URL=«http://www.hpl.hp.com/techreports/ 2002/HPL-2002-164.pdf«. 10. November 2008.

DROBNJAK, S. in JEREB E. Ali nas čaka življenje na daljavo?. Organizacija. Ljubljana, 2007, let. 40, št. 1, str. 58.

FICKO, A. Vdor v zasebnost z uporabo novodobnih informacijskih in komunikacijskih sredstev. Javna uprava. Ljubljana, 2007, let. 43, št. ¾, str.172.

FRELIH, T. Ena oseba, ena kartica, dva namena ali Ena kartica za fizični in logični dostop. Avtomatika. Ljubljana, 2003, št. 34, str. 40.

GLEASON, P. Identifying identity. A semantic history. Journal of american history. 1983, let. 68, št. 4, str. 911. URL=«http://bscw.avmz.uni-siegen.de /pub/bscw.cgi/d1038023/Gleason.pdf«. 3. september 2008.

HEATH, W. Europe's readiness for e-government. Report. 2000, let. 6, št. 39, str. 11. URL=«http://www.egov.vic.gov.au/pdfs/e-readiness.pdf«. 2. september 2008.

JAIN, A. et al. An introduction to biometric recogniton. IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video-Based Biometrics. 2004, let. 14, št. 1, str. 8 in 9. URL=«http://www2.citer. wvu.edu/members/publications/files/RossBioIntro-CSVT2004.pdf«.

JURIŠIČ, A. Pametne kartice. Uporabna informatika. Ljubljana, 1997, let. 5, št. 1, str. 37.

JURIŠIČ, A. in TONEJC J. Pametne kartice in varnost. Monitor. Ljubljana, 2001, let. 11, št. 6, str. 70.

KLEMENČIČ, G. Veliki brat na vašem računalniku. Pravna praksa. Ljubljana, 2001, let. 20, št. 32-33, str. 11.

OCVIRK, V. Veliki brat-da ali ne? Moj mikro. Ljubljana, 2003, let. 19, št. 3, str. 49.

PATO, J. Identity Management: Setting context. Tecnical report. 2003, št. 72, str. 1. URL=«http://zoo.cs.yale.edu/classes/cs155/spr03/idmgmt-tr.pdf«.
2. september 2008.

PEHANI, P. Mikroprocesorska kartica kartični operacijski sistem. Uporabna informatika. Ljubljana, 1999, let. 7, št. 2, str. 16.

SAKSIDA, M. Infrastruktura javnih ključev v Sloveniji. Varstvoslovje. Ljubljana, 2006, let. 9, št. ½, str. 104.

STEFANOVA, K. et al. Innovative approach to identity management solutiondevelopment for e-government at EU level. Journal of Telecommunication and Information technology. 2006, let. 2, št. 2, str. 24. URL=«http://www.itl.waw.pl/ czasopisma/JTIT/2006/2/24.pdf«. 7. september 2008.

TOPLIŠEK, J. Elektronski podpis-usklajevanje tehnoloških in pravnih rešitev pri elektronskem poslovanju. Organizacija. Ljubljana, 1996, let. 29, št. 5, str. 293, 295.

VINTAR, M. E-uprava deset milisekund po velikem poku. Uporabna informatika. Ljubljana, 2001, let. 9, št. 4, str. 177.

WILDES, R. Iris recognition: An emerging Biometric Tehnology. Proc. of the IEEE. 1997, let. 85, št. 9, str. 1349. URL=«http://disys.korea.ac.kr/~mbsong /technical_notes/Iris_paper.pdf«. 11. september 2008.

ZADEL, L. Uporaba pametnih kartic v sodobnem načinu poslovanja. V: FLORIANČIČ, Jože (ur.): Zbornik 22. mednarodne konference o razvoju organizacijskih ved. Moderna organizacija, Kranj, 2003, str. 549.

ŽOHER, B. in URLEP, I. Profesionalna kartica in infrastruktura javnih ključev. Bilten. Ljubljana, 2007, let. 23, št. 3, str. 97.

RAZISKAVE:

LEBEN, A. in KUNSTELJ M. Trendi razvoja e-uprave. Uprava. Ljubljana, 2007, let. 2, št. 2, str. 7.

VINTAR, M. et al. Merjenje zadovoljstva uporabnikov e-uprave. Ljubljana, 2006, str. 9. URL=«http://www.fu.uni-lj.si/iiu/Clanki/MZS-eUprave-RazsirjeniPovzetek ZaSplet - 06(4).pdf«. 15. september 2008.

VIRI

ARCIERI, F. et al. The Italian electronic identity card. The national conference of digital national research. 2004. URL=«http://dgrc.org/dgo2004/disc/posters/tuesposters/rp_arcieri.pdf«. 3. september 2008.

Cagemini. On-line public services are increasingly mature, »intelligent« users centric inclusive services are the next frontier , says new e-Government report. 2006. URL=«http://www.capgemini.com/resources/news/online_public_services_are_ncreasingly _mature«. 6. november 2008.

Capgemini. The users challenge benchmarking the suplly of online public services. 2007. URL=«http://ec.europa.eu/information_society/eeurope/i2010«docs/Bench_marking/egov_benchmark_2007.pdf«. 30. oktober 2008.

Comision tecnica de la implementacion del DNI eletronico. Dni eletronico guia de referencia basica, version 1.0. 2006. URL=«http://www.alfabetizaciontecnologica.es/index.php?option=com_phocadownload&view=category&id=2:.&download=40:&«. 21. september 2008.

CVI-Center vlade za informatiko. Strategija e-poslovanja v javni upravi. 2001. URL=«sehttp://www.vlada.si/data/e-poslovanje.pdf«. 20. september 2008.

Dnevnik. Nove osebne izkaznice-nova tehnologija: na enem mestu bo zbranih preveč podatkov. 2008. URL=«http://www.dnevnik.si/novice/slovenija/314429«. 20. januar 2009.

E-demokracija, intervju s prof. dr. Mirkom Vintarjem. 2007. URL=«http://www.e-demokracija.si/2007/06/25/dr-mirko-vintar-nasa-elektronska-uprava-je-prevec-vezana-na-trenutno-politicno-garnituro/«. 3. september 2008.

E-government in Estonia. 2007. URL=«http://www.epractice.eu/ resource/731«. 27. januar 2009.

FRECH, S., A. Analysis of Global eID projects with focus on Interoperability by using the TFI model. 2005. URL=«http://freh.eu/doc/LSE/ArticleID_Interoperability. pdf«. 7. september 2008.

Ministrstvo za javno upravo. Novinarska konferenca, predstavitev rezultatov meritve uprave s strani Evropske unije ter aktualnih storitev e-uprave. 2007. URL=«www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/mju_dokumenti/ppt/Tiskovka_-_gradivo_-_razultati_-_28_-_09_-_07.ppt«. 1. september 2008.

Ministrstvo za javno upravo. Strategija e-uprave Republike Slovenije za obdobje 2006-2010 (SEP-2010). 2006. URL=«http://e-uprava.gov.si/eud/e-uprava/sep2010_200406_1.doc«. 1. september 2008.

Ministrstvo za notranje zadeve. Biometrična fotografija; priporočila in navodila. 2006. URL=«http://www.mnz.gov.si/fileadmin/mnz.gov.si/pageuploads/SOJ/pdf/0813506 _zlozenka2.pdf«. 7. september 2008.

Ministrstvo za notranje zadeve. Z novo osebno izkaznico si bomo prihranili stroške, varna je tudi pred zlorabo. 2008. URL=«http://www.mnz.gov.si/nc/si/splosno/ cns/novica/article/12027/5746/«. 2. september 2008.

Ministrstvo za notranje zadeve Španija, funkcije in pravna podlaga elektronske izkaznice. URL=«http://www.dnielectronico.es/Guia_Basica/descripcion.html«. 3. september 2008.

Ministrstvo za notranje zadeve Španija, pokazatelji rasti elektronske osebne izkaznice. URL=«http://www.dnielectronico.es/oficina_prensa/noticia_destacada/ mapa_ provin_desp_dnie.html«. 6. november 2008.

Ministrstvo za notranje zadeve Španija, postopek izdaje elektronske osebne izkaznice. URL=«http://www.dnielectronico.es/Guia_Basica/proceso_expedicion. html«. 7. september 2008.

PETRIČ, K. Dnevi slovenske informatike in interoperabilnost. 2008. URL=«http://www.mnz.gov.si/fileadmin/mnz.gov.si/pageuploads/SK/slike/2008/E_pub likacije_2008/InteroperPredav_javna_uprava.pdf«. 24. januar 2009.

TRAMPUŠ, M. et. al. Uporaba pametnih kartic za varno shranjevanje dokumentov. Fakulteta za računalništvo in informatiko. 2002. URL=«http://marvin.fri.uni-lj.si/ papers/Trampus_inf_druzba03.pdf«. 2. september 2008.

The Estonian ID card and digital signature concept. Whitepaper, version 3. 2003. URL=«http://www.epractice.eu/files/upload/gpc/document/191-1126603983.pdf« 7. september 2008.

Wikipedia. Spletna stran evropske komisije. URL=«http://ec.europa.eu/idabc/en/ document/4487/5584«. 3. september 2008.

Wikipedija. Portal upravne enote Avellino. URL=«http://www.comune.avellino.it/ progetti/cartadidentita.php«. 4. september 2008.

Wikipedia. Spletna stran o elektronski osebni izkaznici v Italiji. URL=«http://www.cartadidentita.it/«. 11. september 2009.

Wikipedia. Portal upravne enote Ilirska Bistrica. URL=«http://upravneenote.gov.si/ ilirska_bistrica/splosno/novice/novica/ article/4561/ 3910/?cHash=ad87fa6829« . 12. september 2008.

Zakon o elektronskem poslovanju in elektronskem podpisu. Ur. list RS, št. 57/00, 30/01, 25/04, 73/04 in 61/06.

Zakon o osebni izkaznici in certifikatu elektronskega podpisa v Španiji. Real decreto, 1553/2005, 6. člen – veljavnost osebne izkaznice URL=«http://www.belt.es/legislacion/reciente/pdf/RD_24_dic_05.pdf«. 3. september 2008.

Zakon o spremembah in dopolnitvah zakona o osebni izkaznici. Ur. list RS, št. 44/08.

Zakon o varstvu osebnih podatkov. Ur. list RS, št. 84/04, 113/05, 51/07, 67/07 in 94/07.

.

IZJAVA O AVTORSTVU IN NAVEDBA LEKTORJA

Študentka Mojca Subotić izjavljam, da sem avtorica tega diplomskega dela, ki sem ga napisala pod mentorstvom prof. dr. Mirka Vintarja, in soglašam z objavo diplomskega dela na spletni strani Fakultete za upravo.

Lektorica diplomskega dela je prof. Nataša Koražija.

Ljubljana, junij 2009 Podpis: