UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

PRENOVA INFORMACIJSKEGA SISTEMA KARTICE ZDRAVSTVENEGA ZAVAROVANJA

Ljubljana, september 2006 Robert Romšak

IZJAVA

Študent Robert Romšak izjavljam, da sem avtor tega magistrskega dela, ki sem ga napisal pod mentorstvom prof. dr. Mirota Gradišarja in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, 12. oktober 2006 Podpis: _____

Kazalo vsebine

Kazalo slik

Kazalo tabel

1 Uvod

Leto 1995 je bilo prelomno za Zavod za zdravstveno zavarovanje Slovenije, saj se je z začetkom projekta uvedbo kartice zdravstvenega zavarovanja (KZZ) začelo obdobje intenzivnega razvoja informacijskega sistema kartice zdravstvenega zavarovanja. Ob uvedbi sistema KZZ je bil slovenski sistem med tehnološko najsodobnejšimi z vidika varovanja podatkov in med najbolj izkoriščenimi. Razvite so bile številne aplikacije in rešitev celovito uvedena v celotnem zdravstvenem in zdravstveno-zavarovalniškem sistemu.

Kartica je dokument, s katerim zavarovana oseba izkazuje veljavnost zdravstvenega zavarovanja. Kartica je tudi prenosni mini zdravstveni karton, saj vsebuje nekatere osebne in zdravstvene podatke, pomembne za zdravnika in farmacevta.

Podobne kartice so v istih letih, ko se je uvajala slovenska kartica, široko uvedle tudi nekatere druge evropske države (Nemčija, Belgija, Francija).

V teh letih je tehnologija zelo napredovala in bolj kot kadarkoli prej v zgodovini vpliva na družbo v kateri živimo. Najdemo jo povsod, ustvarja nove skupine ljudi in poslov in je vzrok družbene evolucije. Izum, ki simbolizira navedene spremembe je računalnik, ki se je iz velikosti računalnika iz ene cele sobe zmanjšal na površino nekaj kvadratnih milimetrov.

S pojavom interneta, ki kot medij in kot komunikacijsko sredstvo ponuja vrsto možnosti, tudi državna uprava dobiva močno orodje, ki ga lahko uporabi pri uresničevanju svojih globalnih ciljev (Črešnar, 2002, str. 7-9). Predvsem je to očitno pri komuniciranju z zunanjim svetom, pa tudi pri notranjih procesih razvoja, organizacije, racionalizacije in optimizacije.

Razvoj računalniških omrežij in dostopnost komunikacij pri subjektih zdravstvenega varstva sedaj omogoča sodobnejše rešitve, ki temeljijo na pametnih karticah, ki se uporabljajo predvsem za namen identifikacije zavarovane osebe oziroma pacienta in zdravstvenega delavca v sistemu. Podatki pa se namesto na karticah vodijo na strežnikih, do katerih uporabniki v sistemu na varen način dostopijo skozi računalniška omrežja.

Pri razvoju novega informacijskega sistema moramo najprej definirati poslovne zahteve. Cilj procesa je izdelati kakovostne, celovite in pravilno definirane poslovne zahteve, kajti v nasprotnem primeru lahko to postane glavni razlog neuspeha projektov izgradnje novega informacijskega sistema (Vallabhaneni, 1996, str. 803).

Primarna naloga informacijskega sistema je optimalna uporaba informacijske tehnologije za učinkovito in kvalitetno podporo poslovnega sistema. Pri prenovi informacijskega sistema je potrebno upoštevati, da so poslovni procesi ustrezno urejeni in organizirani (Clarke, 2001, str. 127).

Današnji način uporabe moderne tehnologije je predvsem v tem, da imamo boljše evidence, lepše in hitrejše izpise in lažji dostop do potrebnih informacij. Gre skratka za vsebinsko nespremenjene procese, ki pa se odvijajo hitreje in zanesljiveje. Vse premalo pa je takih načinov uporabe moderne tehnologije, ki bi pomenili tudi bistvene spremembe v delovnem procesu. Brez takih korenitejših sprememb bo državnih uradnikov zmeraj premalo, dela pa zmeraj preveč.

Pri elektronskem poslovanju je velik poudarek na zagotavljanju ustrezne varnosti pri dostopu do podatkov oziroma ob uvedbi takšne infrastrukture, ki bo nudila zaupnost elektronskih storitev in s tem varno elektronsko poslovanje (varni protokoli, varna infrastruktura, varnostna politika vseh vpletenih, itd.).

Najvišji nivo varnosti lahko zagotovimo z uporabo kvalificiranih digitalnih potrdil na pametnih karticah ter postavitvijo infrastrukture javnih ključev (IJK), ob tem pa moramo upoštevati veljavne mednarodne standarde in Zakon o elektronskem poslovanju in elektronskem podpisu (ZEPEP).

V nalogi bom odgovoril na vprašanje, ali je z ekonomskega, organizacijskega, pravnega in tehnološkega vidika v slovenskih razmerah smotrno spremeniti obstoječ sistem kartice zdravstvenega zavarovanja tako, da bo večji del podatkov neposredno dostopen izvajalcem zdravstvenih storitev v bazi podatkov na Zavodu in drugih zavarovalnicah. Del podatkov vezanih na zavarovane osebe se bo shranjeval na strežnikih (npr. elektronski recept).

Glavni poudarek v nalogi bo povezan s prenovo personalizacije kartic in vzpostavitvijo infrastrukture javnih ključev (IJK), saj bo to prvi korak k prenovi informacijskega sistema KZZ, ki ga bo Zavod moral izvesti v naslednjih dveh letih.

V prvem delu naloge sem naredil analizo sedanjega sistema KZZ. Sledi kratek pregled pametnih kartic in obstoječe rešitve infrastrukture javnih ključev v Sloveniji in izven naših meja. V drugem delu naloge je predstavljena prenova personalizacije KZZ ter vzpostavitev infrastrukture javnih ključev z uporabo digitalnih potrdil. Navedel sem prednosti, ki jih bomo zavarovane osebe, izvajalci zdravstvenih storitev in Zavod, pridobili s prenovo informacijskega sistema kartice zdravstvenega zavarovanja. V zadnjem delu naloge sem opisal možnosti uporabe nove KZZ tudi v druge namene ter v sklepu opisal glavne poudarke naloge.

1.1 Opredelitev problema

Sistem kartice zdravstvenega zavarovanja v Sloveniji vse od nacionalne uvedbe leta 2000 sodi med boljše v evropskem prostoru, kar je prispevalo tudi k večjemu številu obiskov tujih predstavništev s področja zdravstva v Sloveniji.

Kljub temu pa trenutni sistem KZZ ni popoln in se Zavod sooča s številnimi problemi, ki bi jih v naslednjih letih rad odpravil s prenovo informacijskega sistema KZZ.

V nadaljevanju bom opisal probleme, zaradi katerih se je Zavod odločil za prenovo informacijskega sistema kartice zdravstvenega zavarovanja.

Dobavitelj sedanjih pametnih kartic in bralnikov kartic je francosko podjetje Gemplus. Zapis podatkov na kartice in distribucijo kartic zagotavlja podjetje Cetis d.d. Trenutno je v uporabi 2.017.435 kartic zdravstvenega zavarovanja in 19.916 profesionalnih kartic, ki služijo kot ključ za dostop do podatkov na KZZ.

Vse od uvedbe sistema KZZ Gemplus ni spreminjal obstoječe strukture datotek na KZZ in pravic dostopa do posameznih datotek na KZZ. Z razvojem lastnih informacijskih rešitev dodajamo nove datoteke na KZZ preko samopostrežnih terminalov ob potrjevanju kartic. Za vse podatke v datotekah lahko z lastnimi rešitvami spreminjamo pravice dostopa in uporabe podatkov na KZZ (branje, pisanje, brisanje, spreminjanje). Vzrok za razvoj lastnih rešitev je v mnogo cenejših lastnih rešitvah kot na strani Gemplusa.

Francosko podjetje je prenehalo z izdelavo sedanjega čipa, ki ga uporabljamo v karticah zdravstvenega zavarovanja in v profesionalnih karticah. Trenutno zalogo KZZ in PK bo Zavod porabil do sredine leta 2008.

Poleg prenehanja izdelave čipa ima sedanja mikroprocesorska (čipna) kartica KZZ 16 kB spominskega prostora, na katero ni mogoče zapisati vseh podatkov, ki jih Zavod hrani v centralnem računalniku in bi bili v pomoč zavarovanim osebam in izvajalcem zdravstvenih storitev (npr. elektronski recept, razširjen nabor sedanjih podatkov o IOZ, izdanih zdravilih, itd).

Priporočena življenjska doba mikroprocesorskih kartic je od pet do sedem let, kar pomeni, da bo večji del KZZ in PK potrebno zamenjati. Število KZZ, ki jim mora Zavod zamenjati zaradi okvare čipa ali druge poškodbe kartice iz leta v leto narašča, kar je razvidno tudi iz tabele 2.1. Pričakovati pa je, da se bo število novo naročenih kartic zaradi okvare čipa ali drugih poškodb na kartici še povečevalo.

Personalizacijo kartic izvaja Cetis d.d. Za zapis podatkov na kartice uporablja zaprto programsko rešitev t.i. črno škatlo, ki jo je razvil proizvajalec kartic Gemplus in so zato dopolnitve programskih rešitev onemogočene.

Ob stalnem dopolnjevanju in razvijanju sistema KZZ je postalo vzdrževanje sistema vsakdanje delo večjega števila zaposlenih na Zavodu in izven njega.

Branje in zapis podatkov na kartice poteka preko samopostrežnih terminalov, preko bralnikov kartic ob sočasni uporabi ene od aplikacij na Zavodu, ki omogoča osveževanje podatkov na KZZ ali preko bralnikov kartic, ki so nameščeni pri izvajalcih zdravstvenih storitev.

Omrežje samopostrežnih terminalov predstavlja bistveni element v kartičnem sistemu. Zavarovanim osebam omogoča potrjevanje zdravstvenega zavarovanja na enostaven in hiter način ter na mestih, kjer se kartica zdravstvenega zavarovanja največkrat uporablja, torej predvsem pri izvajalcih zdravstvenih storitev. V uporabi je 297 samopostrežnih terminalov po celi Sloveniji.

Postavitev omrežja SST in njegovo vzdrževanje je Zavod prepustil zunanjemu izvajalcu. Ker gre za dokaj specifične rešitve, je vzdrževanje omrežja SST zelo drago. Za lažjo predstavo naj tu omenim le, da samopostrežni terminal stane okoli 3.5 milijona tolarjev.

Zavod za zdravstveno zavarovanje Slovenije se je že v letu 2004 odločil, da je potrebno raziskati možnosti, kako zmanjšati rizik neupravičenega koriščenja zdravstvenih storitev na račun Zavoda, če zavarovana oseba nima urejenega obveznega zdravstvenega zavarovanja.

V sedanjem sistemu namreč velja 3-mesečna veljavnost obveznega zdravstvenega zavarovanja na KZZ za aktivno prebivalstvo in 1-letna veljavnost za otroke, šolajočo se mladino in upokojence.

Ker v tem času lahko pride do prekinitve zavarovanja in zavarovanec ne osveži podatkov na KZZ, lahko do konca veljavnosti zavarovanja na kartici še vedno koristi zdravstvene storitve v breme obveznega zdravstvenega zavarovanja.
Za zmanjšanje teh rizikov so zainteresirane tudi zavarovalnice, ki nudijo prostovoljna zdravstvena zavarovanja, saj tudi te zavarovalnice zagotavljajo kritja v določenem obdobju za podatke na KZZ.

Uporaba informacijske tehnologije v našem zdravstvu ni na visokem nivoju z izjemo nekaterih zdravstvenih izvajalcev. Vsak zdravnik se je že vsaj enkrat počutil

nemočnega pred goro podatkov. Brez uporabe najnovejše informacijske tehnologije in izobraževanja zdravstvenih delavcev bo uvedba elektronske kartoteke praktično nemogoča.

Evropska direktiva in slovenski Zakon o elektronskem poslovanju in elektronskem podpisu zahtevata uvedbo elektronskega podpisa pri elektronskem poslovanju, ki ga je mogoče zagotoviti z uporabo PKI infrastrukture.

Če povzamem zgoraj navedene probleme, se je Zavod odločil za prenovo IS KZZ zaradi naslednjih razlogov:

- prenova personalizacije ter odprava odvisnosti od proizvajalcev in lažji vnos sprememb,
- potreba po zamenjavi KZZ, zaradi prenehanja izdelave sedanjega čipa,
- preverjanje veljavnosti obveznega zdravstvenega zavarovanja neposredno z dostopom do centralne zbirke podatkov na Zavodu in drugih PZZ,
- hitrejši in neposreden dostop do ostalih podatkov in razširjen nabor podatkov,
- zagotavljanje bolj kakovostnih zdravstvenih storitev,
- racionalizacija stroškov IS KZZ,
- boljšega obvladovanja stroškov povezanih z zdravstvenem zavarovanjem,
- zagotovitev IJK infrastrukture,
- uvedba elektronskega podpisa – evropska direktiva in slovenski zakon ZEPEP,
- razvoj tehnologij pametnih kartic,
- zagotavljanja boljše varnosti in kakovosti podatkov,
- hiter razvoj informacijskih in komunikacijskih tehnologij,
- zagotovitev možnosti za uvedbo elektronskega recepta in ostalih elektronskih dokumentov.

2 Analiza obstoječega stanja

Zavod za zdravstveno zavarovanje Slovenije (ZZZS) je že leta 1994 začel s projektom kartice zdravstvenega zavarovanja (KZZ). V letu 1998 je sledila pilotna uvedba sistema KZZ v Posavju, v letu 1999 in 2000 pa je sledila nacionalna uvedba sistema KZZ.

Glede na to, da je pričakovana življenjska doba pametnih kartic od pet do sedem let, se število kartic, ki jih Zavod zamenja zaradi okvare čipa na kartici ali zaradi drugih poškodb na kartici, vsako leto povečuje, kar je razvidno tudi iz tabele 2.1.

Tabela 2.1: Število uničenih KZZ po letih

Leto uničenja KZZ	Vzrok uničenja KZZ	Število uničenih KZZ
2000	Poškodba na čipu kartice	5038
2001	Poškodba na čipu kartice	10793
2002	Poškodba na čipu kartice	12961
2003	Poškodba na čipu kartice	14203
2004	Poškodba na čipu kartice	15617
2005	Poškodba na čipu kartice	16209
2006	Poškodba na čipu kartice	8705
2004	Druge poškodbe na kartici	1950
2005	Druge poškodbe na kartici	11883
2006	Druge poškodbe na kartici	6959

Vir: Lasten

Vzrok uničenja KZZ zaradi poškodbe na čipu kartice vodimo na Zavodu že od nacionalne uvedbe KZZ, medtem ko spremljamo druge poškodbe na kartici od leta 2004 od meseca novembra dalje, zato iz tabele ni jasno razvidno naraščajoče število teh poškodb na karticah.

Sistem KZZ sestavljajo kartice zdravstvenega zavarovanja, profesionalne kartice, omrežje samopostrežnih terminalov (SST), transakcijsko komunikacijska strežnika skupaj s petimi varnostnimi strežniki (TKS), centralni računalnik IBM in podatkovne zbirke obveznega zdravstvenega zavarovanja ter strežniki in podatkovne zbirke prostovoljnih zdravstvenih zavarovalnic. Partnerji v sistemu so, poleg Zavoda in zavarovalnic za prostovoljna zdravstvena zavarovanja, še izvajalci zdravstvenih storitev, njihove programske hiše in zavarovane osebe kot imetniki kartice.

Izvajalci zdravstvenih storitev v sedanjem sistemu berejo iz KZZ naslednje podatke: EF.IIP (osebni podatki), EF.OD (podatki zavezancev), EF.CI (podatki o veljavnosti obveznega zavarovanja), EF.DDT (podatki o izdanih medicinsko tehničnih pripomočkih, EF.DDD (podatki o izdanih zdravilih na zeleni recept) ter podatke o veljavnosti prostovoljnega zavarovanja v datotekah VI1, VI2 in VI3.

Pri načrtovanju sedanjega nabora podatkov za zapis na KZZ je bilo eno od vodil tudi varčevanje s pomnilnikom na kartici. Nabor podatkov je bil zaradi tega skrčen na minimalni potrebni obseg.

Na kartici zdravstvenega zavarovanja vodimo podatke o prostovoljnem zdravstvenem zavarovanju vseh treh zavarovalnic, ki taka zavarovanja nudijo na slovenskem tržišču:

- Vzajemna,

- Adriatic-Slovenica,
- Triglav.

Vsaka zavarovalnica ima na kartici svoj nabor podatkov, ki opisuje veljavna zavarovanja (kritja), ki pa so zaradi pomanjkanja prostora na KZZ prav tako skrčeni na minimalni obseg.

Podatki o izbranih osebnih zdravnikih nastajajo pri izvajalcih zdravstvenih storitev, ko se zavarovana oseba skladno z 80. členom Zakona o zdravstvenem varstvu in zdravstvenem zavarovanju in s členi 161-171 Pravil obveznega zdravstvenega zavarovanja opredeli za osebnega splošnega zdravnika, pediatra, zobozdravnika ali ginekologa.

Izvajalci podatke o novih izbirah mesečno posredujejo na Zavod. Rok za posredovanje podatkov o novih izbirah opravljenih v preteklem mesecu je do 10. dne v novem mesecu.

Računalniško izmenjevanje podatkov poteka s polovico vseh izvajalcev. Ostala polovica podatke na Zavod pošilja v pisni obliki (drugi izvod obrazca o izbiri).

Zavod prejete podatke podrobno kontrolira, v primerih napak usklajuje z izvajalci. Petindvajsetega dne v mesecu Zavod v elektronski ali pisni obliki (odvisno od tega ali je izvajalec vključen v RIP IOZ ali ne) izvajalcu pošlje seznam zavarovanih oseb, ki so izbrale drugega zdravnika pri drugem izvajalcu. Na podlagi tega obvestila izvajalec avtomatično prekinja izbiro in zdravniku, ki ga je oseba izbrala kot novega zdravnika, pošlje medicinsko dokumentacijo.

Občasno potekajo akcije usklajevanja podatkov med Zavodom in izvajalci. Nekateri izvajalci in enote Zavoda to počnejo pogosteje, nekateri redkeje. Usklajevanje podatkov se izvaja pogosteje pri večjih izvajalcih (zdravstveni domovi). Obstajajo redki primeri, ko izvajalci s precejšnjo zamudo pošljejo podatke o posamezni izbiri (založen obrazec, težave z informacijskim sistemom pri izvajalcu, itd.). Podatke o izbranih osebnih zdravnikih na KZZ zapisujejo le v ambulantah teh zdravnikov in se pri potrjevanju KZZ na samopostrežnem terminalu podatki o izbranih zdravnikih ne osvežijo.

Podatki o izdanih in izposojenih medicinsko tehničnih pripomočkih (MTP) se oblikujejo pri dobaviteljih in v izposojevalnicah teh pripomočkov, ko le ti izdajo pripomoček zavarovani osebi. Zavod ima trenutno okrog 380 pogodbenih dobaviteljev in izposojevalnic MTP, ki zagotavljajo pripomočke, ki so pravica iz obveznega zdravstvenega zavarovanja. Dobavitelji in izposojevalnice ob izdaji

pripomočka podatke zapisujejo tudi na KZZ. Na kartici je prostora za 16 zapisov o izdanih MTP. Podatki o izdanih in izposojenih MTP se osvežujejo tudi pri potrjevanju KZZ na samopostrežnih terminalih in referentih Zavoda.

Dobavitelji in izposojevalnice do trikrat mesečno posredujejo podatke o izdajah Zavodu (odvisno od določil pogodbe z dobaviteljem). 337 dobaviteljev in izposojevalnic podatke posreduje v elektronski obliki.

Prejete podatke Zavod podrobno kontrolira s pomočjo avtomatskih kontrol (računalniške obdelave) in s pomočjo ročnih kontrol (pripravljeni izpisi in usklajevanje podatkov v oddelkih obveznega zdravstvenega zavarovanja). Isti delavci tudi vnašajo podatke v podatkovno bazo, ki jih Zavod pridobi v pisni obliki. Tudi pri ročnem vnosu so zagotovljene enake avtomatske kontrole podatkov. Kontrole so osredotočene predvsem na podatke, ki se zapisujejo na KZZ. Kakovost teh podatkov je zato zelo dobra. Kakovost ostalih podatkov je slabša.

Zavod podatke hrani v podatkovni bazi na centralnem računalniku. Podatke na KZZ uporabljajo osebni zdravniki in specialisti. Podatki so namenjeni kontroli pri predpisovanju medicinsko tehničnih pripomočkov (upoštevanje omejitev, kot jih določajo Pravila OZZ) in kot pomoč pri zdravljenju.

Zavod je v obdobju med junijem in oktobrom 2005 v novogoriški regiji izpeljal pilotno uvedbo zapisa izdanih zdravil na KZZ. V prvi polovici leta 2006 se je izvedla nacionalna uvedba zapisa zdravil.

Na KZZ se zapisujejo le podatki o zdravilih, ki so bili izdani na zeleni recept oziroma v breme OZZ. Na KZZ se lahko zapiše do 46 izdanih zdravil. Zdravila, ki so jih lekarne izdale v breme zavarovane osebe ali posebnih paketov prostovoljnega zdravstvenega zavarovanja, se na KZZ ne beležijo. Poleg zapisa podatkov na KZZ lekarne podatke dekadno posredujejo tudi na Zavod. V mesecu aprilu 2006 je bila vzpostavljena računalniška izmenjava podatkov z vsemi lekarnami, ki so zamenjale posredovanje podatkov po disketah.

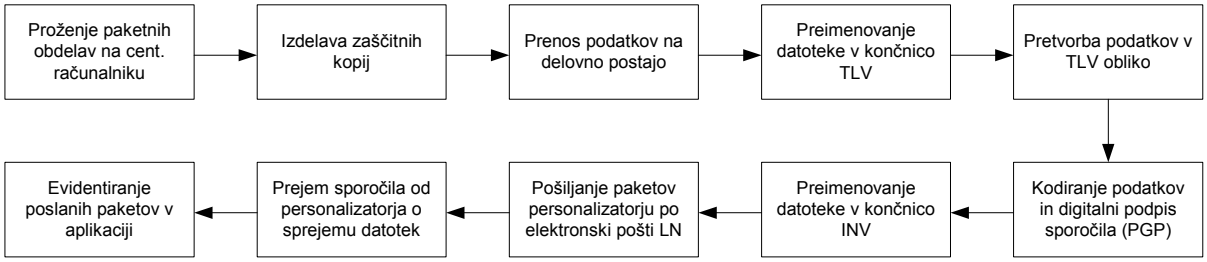
Kakovost podatkov je dobra, saj Zavod izvaja redno kontrolo podatkov. Obseg kontrol in s tem kakovost podatkov se je povečala v zadnjih dveh letih, ko se je izvajal projekt STIRA. Kakovost podatkov se je močno izboljšala z dodatnimi kontrolami ob uvedbi računalniškega izmenjevanja podatkov in dokončno vzpostavitvijo uporabe Centralne baze zdravil v lekarnah.

2.1 Posnetek obstoječega stanja personalizacije kartic

Podatki za personalizacijo kartic se pripravljajo iz centralnih baz podatkov Zavoda za zdravstveno zavarovanje Slovenije. Podatki za personalizacijo se pripravljajo v obliki paketov. Vsak paket vsebuje podatke za personalizacijo do 2.500 kartic. Paketi se pripravljajo ločeno, glede na tip kartic (kartice zdravstvenega zavarovanja, profesionalne kartice) in glede na tip izdaje kartic (uvodne izdaje kartic, ponovne izdaje kartic). Podatki za personalizacijo KZZ in PK se pripravljajo in pošiljajo personalizatorju kartic enkrat tedensko po elektronski pošti. Postopek priprave podatkov in pošiljanje datotek za personalizacijo prikazuje slika 2.1.

Priprava podatkov vsebuje korake proženja paketnih obdelav na centralnem računalniku, izdelava zaščitne kopije na kaseto, prenosa podatkov na osebni računalnik odgovorne osebe Službe za poslovanje s karticami, pretvorbe podatkov v TLV obliko in kodiranja podatkov.

Slika 2.1: Postopki priprave podatkov in pošiljanje datotek za personalizacijo



Vir: Lasten

Prvi korak priprave podatkov je proženje paketnih obdelav na centralnem računalniku. Rezultat paketnih obdelav so sekvenčne datoteke.

Po izvedbi paketnih obdelav na centralnem računalniku, se vsi podatki za personalizacijo kartic kopirajo na kasete, zaradi izdelave zaščitnih kopij.

Zadolženi delavec v Službi za poslovanje s karticami pripravljene datoteke na centralnem računalniku prenese na svojo delovno postajo, kjer datoteke preimenuje v pcbnnnnn.TLV, kjer je

p … oznaka personalizatorja (C=Cetis)
c … tip kartic (H=kartice zdravstvenega zavarovanja, P=profesionalne kartice)
b … tip izdaje kartic (N=nove kartice, R=nadomestne kartice)
nnnnn … številka paketa v okviru personalizatorja ne glede na tip kartic

TLV … konstanta TLV

Datoteke s podatki za personalizacijo kartic se v naslednjem koraku pretvorijo v TLV obliko. Ta pretvorba podatkov se izvaja zaradi omejitev orodij centralnega računalnika in zahtev izvajalca personalizacije.

Pred posredovanjem datotek personalizatorju se podatki v datotekah še kodirajo. Kodiranje se izvaja z uporabo postopka PGP. Postopek PGP izvaja asimetričen kriptografski algoritem in elektronsko podpisovanje podatkov. Slednje zagotavlja ustrezno varnost pred dostopom do osebnih podatkov v teh datotekah s strani nepooblaščenih oseb (omogočen je dostop samo pooblaščeni osebi personalizatorja) in avtentičnost (istovetnost) pošiljatelja podatkov. Uporablja se PGP nekomercialne verzije 2.6.3i.

Za kodiranje in elektronsko podpisovanje datotek se uporablja privatni kodirni ključ Zavoda za zdravstveno zavarovanje Slovenije in javni ključ personalizatorja. Ključi so bili ustvarjeni in vnešeni v operativni sistem s strani odgovornega skrbnika orodja PGP. Uporaba ključev je mogoča le z vnosom ustreznega gesla.

Rezultat postopka PGP so datoteke z istim imenom, a končnico PGP.

Pred nadaljevanjem postopkov pošiljanja podatkov personalizatorju se zaradi določil spremljanja prometa z datotekami izhodna datoteka preimenuje v datoteko z istim imenom, a končnico INP.

Elektronsko posredovanje podatkov v Cetis d.d. se izvaja preko elektronske pošte Lotus Notes.

Skupaj z oddajo podatkov se personalizatorja v istem sporočilu dodatno obvešča o posredovanih paketih. Za pošiljanje obvestil se uporablja elektronska pošta. Za te namene je bila s personalizatorjem dogovorjena standardna vsebina elektronske pošte. Za pripravo takšnega obvestila so v orodju Lotus Notes pripravljeni ustrezni vzorci, ki se jih vzame kot osnova za tvorbo obvestila.

Personalizator je dolžan za vsako prejeto obvestilo o posredovanju podatkov s strani Zavoda preveriti in potrditi prejem vseh navedenih datotek. Potrditev izvede s pošiljanjem povratnega elektronskega sporočila.

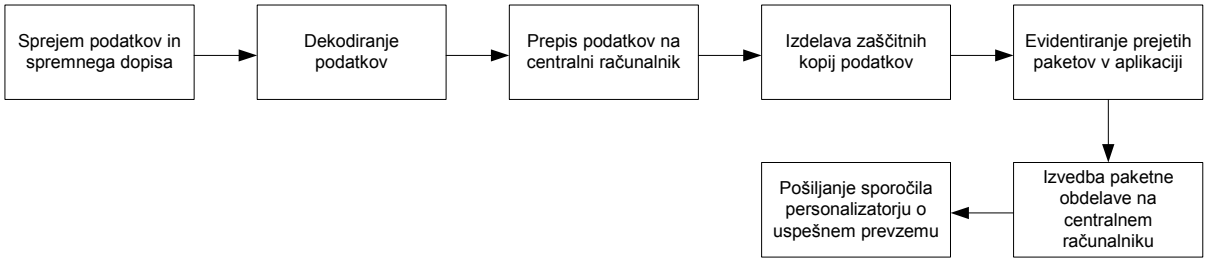
Kot zadnji korak posredovanja podatkov personalizatorju, mora odgovorna oseba Službe za poslovanje s kartico oddajo vsake datoteke (personalizacijskega paketa)

evidentirati v aplikaciji Administracija KZZ in Administracija PK. Evidentiranje se izvede v skladu z uporabniškimi navodili za ti dve aplikaciji.

Pogodbeni personalizator kartic je dolžan po opravljenem postopku personalizacije posredovati izhodne datoteke, ki vsebujejo vse podatke iz vhodnih datotek s pripisanimi podatki, ki nastanejo v času personalizacije. Za Zavod je med izhodnimi podatki najpomembnejši podatek serijska številka posamezne personalizirane kartice, ki se določi za vsako kartico ob personalizaciji. Na osnovi te številke se ugotavlja verodostojnost kartic zdravstvenega zavarovanja ob uporabi na samopostrežnih terminalih in pri referentih na Zavodu.

Po izvedeni personalizaciji vseh kartic v paketu, personalizator pošlje povratno sporočilo, v katerem so pripete datoteke, v katerih so zapisane dodatne informacije o personaliziranih karticah in sami personalizaciji. Postopke prejema podatkov od personalizatorja prikazuje slika 2.2.

Slika 2.2: Postopki prejema podatkov od personalizatorja



Vir: Lasten

Po izvedbi personalizacije kartic, personalizator kartice pošlje njegovemu imetniku po pošti.

3 Pametne kartice in pregled uvedenih rešitev IJK v Sloveniji in izven naših meja

Manj kot trideset let po prvem patentu za pametne kartice, se je uporaba pametnih kartic bliskovito razširila na mnoga področja. Največ pametnih kartic se še vedno uporablja v telekomunikacijah, zadnja leta je opazna porast v zdravstvu in financah. Prednosti uporabe pametnih kartic so velikost, prenosljivost, večkratna uporabljivost, funkcionalnost in varnost. Ravno varnost predstavlja najpomembnejšo lastnost pametne kartice.

3.1 Kratek pregled razvoja kartic

Diners Club je že leta 1950 izdal prve plastične kartice, ki so bile predhodnica pametnih kartic. Za začetnika pametnih kartic se smatra francoski novinar Roland Moreno, ki je leta 1974 prijavil prve idejne patente pametne kartice.

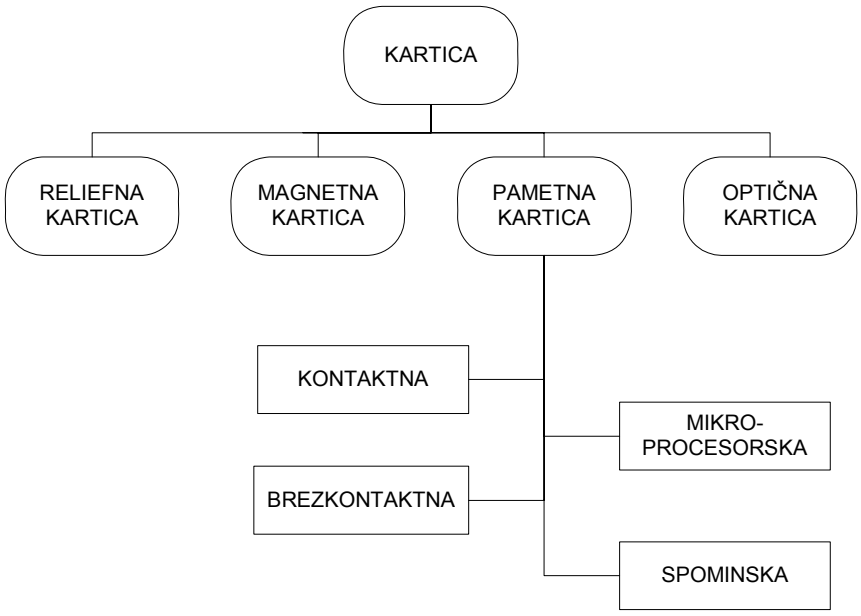
Reliefni zapis je najstarejša tehnika, ki se uporablja za berljive oznake na identifikacijski kartici. Reliefne oznake na kartici se lahko prenesejo na papir s pomočjo cenene in enostavne naprave. Standard ISO 7811 specificira postopke zapisovanja in lokacijo reliefnega zapisa. Kljub primitivnemu prenosu podatkov iz reliefne kartice na papir, se je zaradi enostavnosti te tehnologije uporaba reliefnih kartic razširila po celem svetu.

Glavna pomanjkljivost reliefnih kartic je veliko papirja, ki ga je potrebno ročno obdelati. Ena rešitev tega problema je digitaliziranje in shranjevanje podatkov na magnetni trak na zadnji strani kartice. Podatki se elektronsko preberejo z vlečenjem kartice skozi bralnik. Spominska kapaciteta magnetnega traku je 1288 bitov, kar je dovolj, da se nanj shranijo vse informacije, ki jih ima reliefna kartica. Glavna pomanjkljivost magnetnih kartic je, da lahko shranjene podatke enostavno spreminjamo, zato so proizvajalci magnetnih kartic razvili različne varovalne tehnike. Magnetni trak je občutljiv tudi na razmagnetenje, vlago, temperaturo in umazanijo, omogoča pa večkraten zapis podatkov. Splošno razdelitev kartic prikazuje slika 3.1.

Razlog za razvoj in uporabo pametne kartice je varnost shranjenih podatkov na njej in zaščita podatkov na drugih računalniških sistemih.

Prve pametne kartice so imele omejene spominske kapacitete (sedanje kartice KZZ imajo 16 KB), zadnje čase pa so na trgu dostopne tudi pametne kartice z večjo kapaciteto (64 KB in več). Te omogočajo, da poleg enostavnih podatkov, ki so namenjeni za overjanje uporabnikov (zasebni ključi, gesla), na njih varno hranimo tudi druge koristne dokumente.

Slika 3.1: Vrste kartic



Vir: Šilc, 2005, str. 20

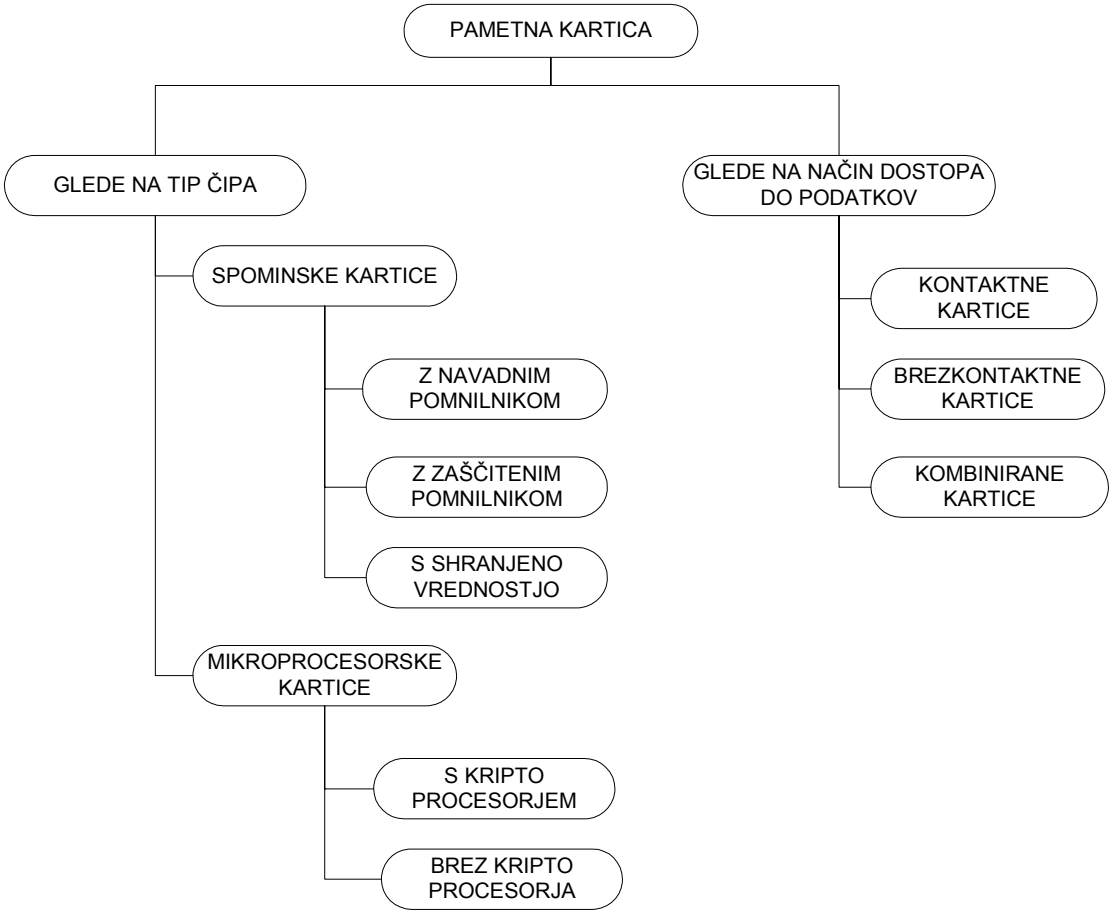
3.2 Pametne kartice

Varno shranjevanje informacij in zaščita pretoka informacij je nujna v okolju v katerem živimo. Kot idealna rešitev se ponuja pametna kartica, katere glavna prednost pred drugimi je ta, da lahko shranjene podatke učinkovito zaščiti pred nepooblaščenim dostopom. Ker je dostop do podatkov na kartici možen le preko serijskega vmesnika, ki ga nadzoruje operacijski sistem, je možno zapisati podatke na kartico na tak način, da jih ni možno prebrati od zunaj.

Pametne kartice pogosto združujejo značilnosti magnetnih in reliefnih kartic. Njena najpomembnejša značilnost je ta, da vsebuje čip. Pametne kartice imajo tudi daljšo življenjsko dobo in večjo stopnjo zanesljivosti.

Pametne kartice so najmlajši in najpametnejši član iz družine identifikacijskih kartic. Spominska kapaciteta pametnih kartic je nekajkrat večja kot pri magnetnih karticah. Le optične spominske kartice imajo večjo, nekaj megabitov, spominsko kapaciteto.

Slika 3.2: Vrste pametnih kartic



Vir: Šilc, 2005, str. 22

Pametne kartice lahko razdelimo v več skupin. Glede na čip, ki je vgrajen v kartico, razlikujemo spominske in mikroprocesorske kartice, z vidika dostopa do podatkov, pa jih razdelimo na kontaktne, brezkontaktne in kombinirane. Slika 3.2 prikazuje razvrstitev pametnih kartic.

Današnje pametne kartice - najbolj znani proizvajalci so Giesecke & Devrient, Gemplus, Schlumberger in Solaic - stanejo od manj kot dolar do približno 20 dolarjev. Spominske kartice nimajo lastnega procesorja, zato ne morejo dinamično obdelovati podatkov. Glede na vrsto pomnilnika ločimo:

- kartice s shranjeno vrednostjo, ki so namenjene shranjevanju vrednosti ali žetonov in so lahko za enkratno ali večkratno uporabo
- kartice z navadnim pomnilnikom, ki so namenjene zgolj shranjevanju podatkov in
- kartice z zaščitenim ali deljenim pomnilnikom imajo vgrajena preprosta logična vezja, s katerim nadzorujemo dostop do podatkov. Določene dele pomnilnika lahko zaščitimo pred pisanjem ali branjem z gesli ali sistemskimi ključi.

Mikroprocesorske kartice omogočajo večjo stopnjo zaščite, vgradnjo kriptografskih algoritmov in zaščitnih mehanizmov. Njena funkcionalnost je omejena z velikostjo njenega pomnilnika in močjo procesiranja. Uporablja se v aplikacijah, kjer je zahtevana varnost in zasebnost podatkov. Zaradi inteligence, ki jo daje mikroprocesor, se ime pametna kartica pogosto uporablja samo za mikroprocesorske kartice.

Sestavni deli mikroprocesorske kartice (glej sliko 3.3) so centralno procesna enota CPU, vhodno-izhodna enota, numerična procesna enota NPU (opcijsko) ter več vrst pomnilnikov (RAM, ROM, EEPROM). Trenutno se uporabljajo 8, 16 in 32-bitni procesorji, ki imajo v povprečju 64 Kb ROM-a, 16 do 32 Kb EEPROM-a ter 3 Kb RAM-a, vhodno izhodna enota pa dosega prenose od 9,6 do 115 Kb/s (pri čemer je možen samo polovični dupleksni način).

Aplikacije, ki uporabljajo pametne kartice, pogosto zahtevajo uporabo kriptografskih algoritmov, zato ima mnogo današnjih pametnih kartic numerično procesno enoto NPU. Omejena procesna moč CPU-ja predstavlja ozko grlo zahtevanih kriptografskih operacij, zato mikrokontroler vsebuje numerično procesno enoto. Zmožne so generiranja in preverjanja digitalnih podpisov ter šifriranja podatkov s simetričnimi ključi. S tem je omogočena uporaba 1024-bitnih RSA ključev. Negativna stran uporabe NPU-ja je višja cena čipa.

Pomnilnik je poleg procesorja najpomembnejši sestavni del mikrokontrolerja. Pametna kartica običajno vsebuje tri vrste pomnilnikov. Samo bralnega (ROM), neizbrisljivega bralno/pisalnega (EEPROM) in delovnega bralno/pisalnega (RAM).

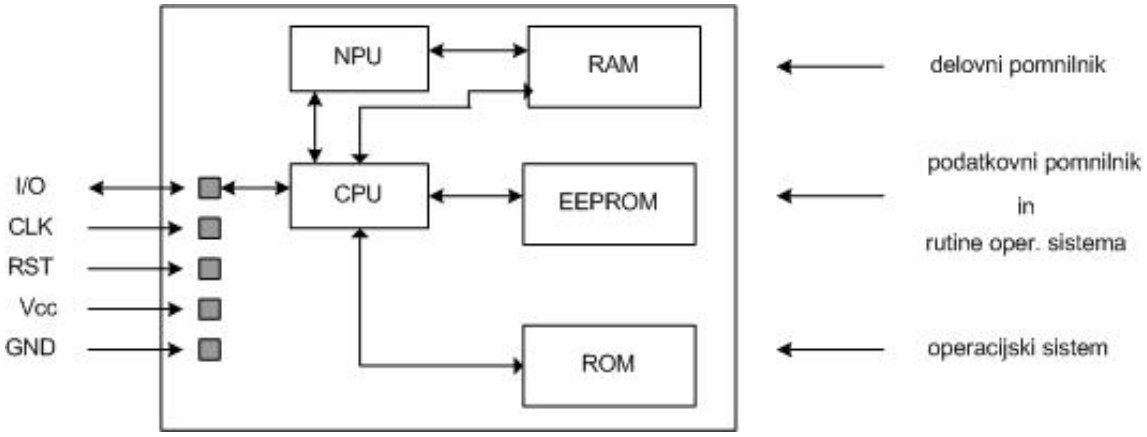
ROM vsebuje operacijski sistem, ki se zapiše ob izdelavi kartice in kasneje vsebine ni mogoče več spreminjati.

EEPROM je spremenljiv pomnilnik čipa. Zapis programske kode in podatkov se v ta pomnilnik zapišejo pod nadzorom operacijskega sistema, ki lahko te podatke kasneje tudi prebere. Tudi po prekinitvi električne energije se podatki ohranijo.

RAM je procesorjev delovni spomin. Za razliko od EEPROM-a se podatki v tem pomnilniku po prekinitvi električne energije izgubijo.

Velikost pametne kartice ustreza standardu ISO 7810 ali ID-000 (npr. SIM). Oznake na priključkih: Vcc – napajanje, GND – ozemljitev, RST – ponastavljanje (reset), CLK – urni signal.

Slika 3.3: Sestavni deli pametne kartice



Vir: Aksentič, 2004

Brez kontaktne kartice ustrezajo standardu ISO 7816. Brezkontaktne kartice so zelo podobne kontaktnim karticam, bistvena razlika je le v načinu prenosa podatkov s kartice na bralnik. Z zunanjim svetom komunicirajo preko antene, ki je vgrajena v ohišje kartice. Za komunikacijo se uporablja RFID tehnologija. Od bralnika je odvisen domet branja podatkov iz kartice in znaša od osem do sedemdeset centimetrov.

Optične kartice se uporabljajo tam, kjer je kapaciteta spominskih pametnih kartic nezadostna. S kombinacijo velike pomnilniške kapacitete optičnih in inteligence pametnih kartic, se odpirajo nova področja uporabe teh kartic. Npr. podatke zapišemo v šifrirani obliki v optični pomnilnik, medtem ko je ključ varno shranjen v trajnem spominu mikroprocesorja. Oprema za branje in pisanje na optične spominske kartice je še precej draga, kar resno omejuje množično uporabo teh kartic. Zaradi velike kapacitete je možna uporaba teh kartic v zdravstvu za zapisovanje bolnikovih podatkov in shranjevanje rentgenskih slik.

Moderni operacijski sistemi pametnih kartic omogočajo več aplikacij na eni sami kartici. Najbolj znane več aplikacijske kartice so tiste, ki temeljijo na specifikaciji JavaCard in tiste, na katerih teče operacijski sistem MULTOS.

Specifikacija JavaCard omogoča poganjanje javanskih aplikacij na pametnih in drugih napravah z omejenim pomnilnikom. Na karticah teče različica Java navideznega stroja, ki omogoča izvajanje okrnjenega izbora javanskih ukazov. Navidezni stroj zagotavlja prenosljivost aplikacij iz ene kartice na drugo in s tem neodvisnost od proizvajalca kartic.

Java kartice so več aplikacijske, omogočajo pa tudi kasnejše (ang. post-issue) dodajanje novih aplikacij na kartico.

Ena ključnih lastnosti jave je varnost na vseh nivojih. Poleg že pripravljenih razredov za kriptografijo, PIN identifikacijo, tudi zaščiteno izvajanje več aplikacij na kartici (ena aplikacija ne more posegati v pomnilniški prostor druge). Prav tako je izvajanje več aplikacij, ki se med seboj ne motijo, omogočeno na karticah z operacijskim sistemom MULTOS.

Tako platforma MULTOS kot Java sta neodvisni od operacijskega sistema. To pomeni, da aplikacijo napišemo enkrat in se izvaja kjerkoli.

Jezik Java je odprt in standardiziran, kartice ki ustrezajo specifikaciji JavaCard pa ustrezajo standardom ISO 7816 in drugim (EMV). Java kartice danes predstavljajo 90% vseh proizvedenih pametnih kartic na svetu.

Večina Java pametnih kartic, ki so na trgu, ustreza tudi specifikacijam GlobalPlatform, ki standardizirajo način nameščanja aplikacij na kartico, poizvedovanje katere aplikacije so na kartici in upravljanje z aplikacijami na kartici.

OpenCard je v Javi razvito ogrodje, ki omogoča uporabo komunikacije s pametnimi karticami, v višjenivojskih aplikacijah (Ciglarič, 2003).

Osebni računalnik in kartica oz. kartični program komunicirata s pomočjo ukazov APDU. Osebni računalnik pošlje ukaz APDU kartici, ta pa nanj odgovori bodisi z nizom podatkov ali pa z napako.

3.3 Pomembni standardi na področju uporabe pametnih kartic

Pametna kartica predstavlja le eno komponento kompleksnega sistema, kar pomeni, da mora biti vmesnik med pametno kartico in ostalim sistemom točno določen. Zaradi tega so uvedli standarde in specifikacije za pametne kartice, ki opisujejo njihove lastnosti in poenotijo uporabo.

Institucije, ki izdajajo standarde za pametne kartice so:

- ISO (mednarodna organizacija za standardizacijo)
- IEC (mednarodna elektrotehniška komisija)
- CEN (evropska organizacija za standardizacijo) in
- ETSI (evropski telekomunikacijski inštitut za standardizacijo)

Poleg institucij pa standarde izdajajo tudi velike organizacije in se imenujejo industrijski standardi (npr. Europay, MasterCard in Visa so se sporazumeli o skupni

specifikaciji EMV, ki določa osnovne protokole za komunikacijo med karticami in terminali).

Mednarodna institucija, ki izdaja standarde za pametne kartice, se imenuje ISO, ki združuje približno sto nacionalnih uradov za standardizacijo, po enega izmed vsake države. Z namenom, da se prepreči podvajanje dela, ISO tesno sodeluje z IEC, ki pokriva področje elektrotehnike in elektronike, medtem ko je ISO zadolžen za ostala področja. Obe skupini oblikujeta in izdajata ISO/IEC standarde. Večina standardov za pametne kartice je te vrste. Slika 3.4 prikazuje organizacijo delovnih skupin, ki so vključene pri razvoju mednarodnih standardov za pametne kartice.

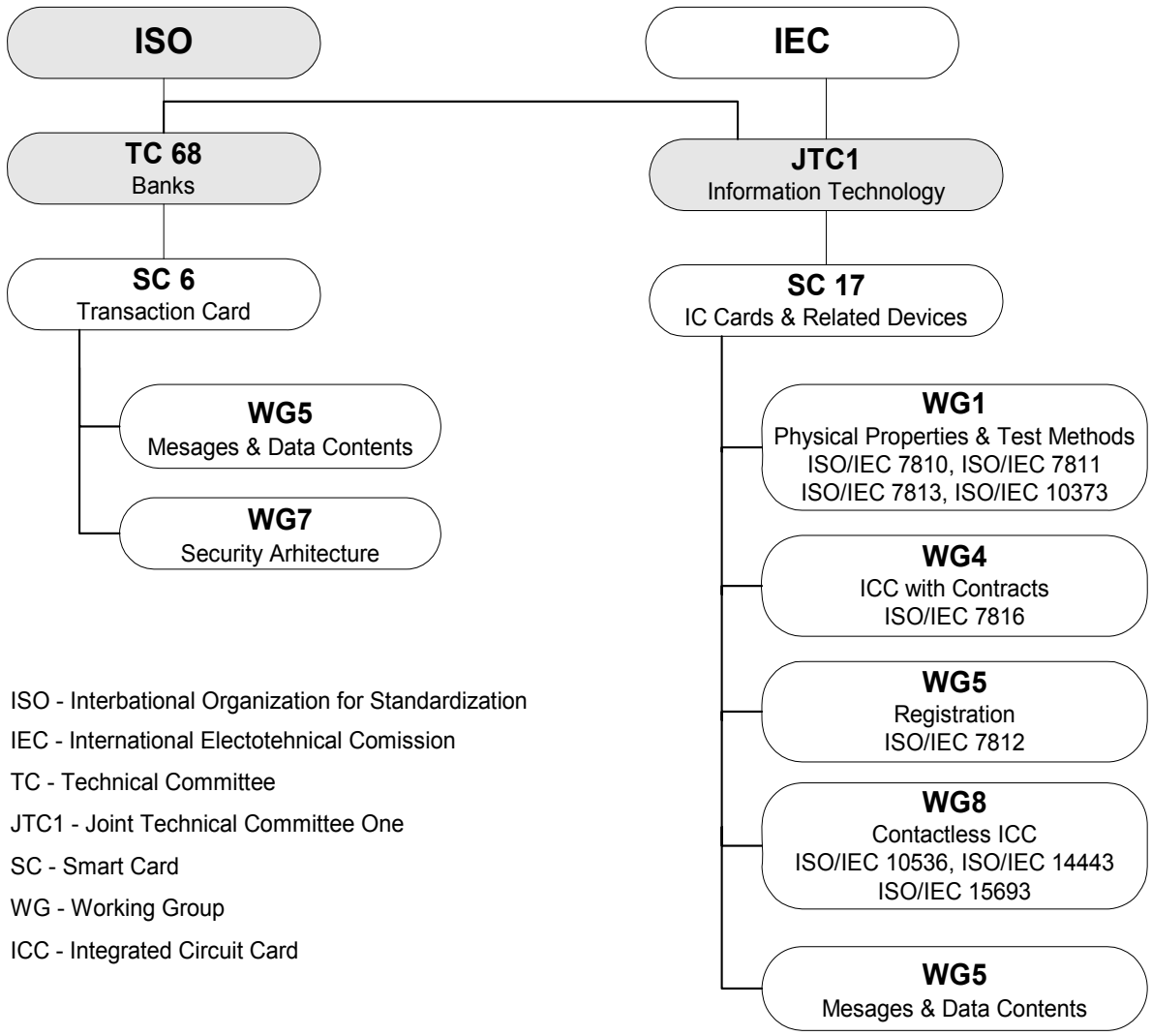
Pri standardizaciji pametnih kartic sodelujeta dva tehnična komiteja. ISO TC68/SC6 je odgovoren za standardizacijo kartic, ki se uporabljajo za finančne transakcije, ISO/IEC JTC1/SC17 pa pokriva področje za splošne aplikacije. Vsak izmed tehničnih komitejev je sestavljen iz več skupin.

Institucija, ki izdaja evropske standarde (na območju Evrope), se imenuje CEN. Njihove standarde priznava tudi ISO. Tehnični komite TC sestavlja dvanajst delovnih skupin, izmed katerih vsaka delovna skupina pripravlja standarde za določeno področje.

ETSI izdaja standarde, ki pokrivajo uporabo pametnih kartic v javnem mobilnem telekomunikacijskem omrežju.

Nacionalnemu uradu za standardizacijo običajno industrijski sektor posreduje potrebo po standardu. Na podlagi tega nastane nova tema, ki jo nacionalni urad predlaga mednarodni organizaciji za standardizacijo. Delovna skupina mora predlog sprejeti in tako je standard definiran. Nato sledi konsenz vseh udeleženih držav, kar predstavlja osnutek mednarodnega standarda. V zadnji fazi pa glasujejo o predlaganem standardu. Dve tretjini glasov članov ISO, ki so sodelovali pri nastanku standarda zadošča, da je standard mednarodno sprejet (Šilc, 2005, str. 14-17).

Slika 3.4: Hierarhija in pregled delovnih skupin, ki so vključene pri razvoju mednarodnih standardov za pametne kartice



Vir: Šilc, 2005

Najpomembnejši standardi, ki so povezani s pametnimi karticami so:

ISO 7810 Identifikacijske kartice – fizične lastnosti: Opisuje najpomembnejše fizične lastnosti identifikacijskih kartic brez čipa, med drugimi tudi velikost kartice (dolžino, širino, debelino).

ISO 7816 – 1 Identifikacijske kartice – Kartice z integriranim vezjem in kontakti. Prvi del – Fizične lastnosti: Pokriva vse kontaktne kartice s čipom, ki ustrezajo velikosti predpisani s standardom ISO 7810. Sem spadajo tudi vse pomnilniške in mikroprocesorske kartice. V standardu je določena odpornost na zunanje vplive okolja.

ISO 7816 – 2 Identifikacijske kartice – Kartice z integriranim vezjem in kontakti. Drugi del – Dimenzije in položaj kontaktov: Določa velikost in položaj kontaktnih elementov pametne kartice, kakor tudi

razporeditev čipa, magnetne steze in reliefa. Standard definira osem kontaktov, čeprav večina današnjih proizvajalcev uporablja le šest in večina aplikacij le štiri ali pet kontaktov.

ISO 7816 – 3 Identifikacijske kartice – Kartice z integriranim vezjem in kontakti. Tretji del – Električni signali in protokoli: Ključni standard, v katerem je definiran način komunikacije med pametno kartico in zunanjim svetom. Vključuje asinhrone protokole, ki se večinoma uporabljajo v mikroprocesorskih karticah. Ta standard definira strukturo ATR-ja, s katerim pametna kartica vzpostavi komunikacijo s terminalom. Določa tudi, kako naj kartica reagira ob previsoki ali prenizki napetosti.

ISO 7816 – 4 Identifikacijske kartice – Kartice z integriranim vezjem in kontakti. Četrti del – Ukazi za izmenjavo: Določa zgradbo nekaterih tipov sporočil. Definira datotečno strukturo za uporabo v pametnih karticah, ki je sestavljena iz glavne, namenske in elementarne datoteke. Naslavljanje datotek in podatkovnih objektov vsebuje varnostno arhitekturo, ki je podrobno opisana.. Vključuje možnosti, da aplikacije omejijo dostop do elementarnih datotek ali podatkovnih objektov glede na overitev in šifriranje.

ISO 7816 – 5 Identifikacijske kartice – Kartice z integriranim vezjem in kontakti. Peti del – Številčni sistemi in procedure za registracijo aplikacijskih identifikatorjev: Določa številčne sheme za enolične identifikacije državnih in mednarodnih kartičnih aplikacij. Določa tudi strukturo aplikacijskega identifikatorja in proceduro za registracijo aplikacije.

ISO 9564 Opisuje principe upravljanja in varovanja PIN kode.

ISO 9798 Opisuje kriptografske postopke za overjanje.

ISO 10373 Opisuje metode za preizkušanje magnetnih, optičnih, kontaktnih in brez kontaktnih kartic.

ISO 11770 Opisuje tehnike varovanja in upravljanje s ključi. Mehanizmi za uporabo asimetričnih tehnik.

ISO 3166 Kode za predstavljanje imen držav.

EMV Skupina standardov, ki so jih razvili Europay, MasterCard in Visa, opisuje pametne kartice za uporabo v plačniških sistemih. Napisani so tako, da omogočajo uporabo kartic različnih bank na istem bankomatu, ne da bi pri tem banka morala razkriti interni sistem plačevanja.

ANSI X9 Skupina standardov, ki opisuje kriptografijo z javnimi ključi v finančni industriji. Vključuje standarde za opis zgoščevalne funkcije SHA-1, algoritem za digitalni podpis z uporabo eliptičnih

	krivulj, itd.
IEEE P1363	Najpomembnejši standard za javno kriptografijo.
ITU X.509	Določa strukturo in zapis certifikatov, mednarodno najpogosteje uporabljena osnova za strukture certifikatov.
PKCS	PKCS #7 – Cryptographic Message Syntax (kako podpisati in kriptirati) PKCS #8 – Format shranjevanja ključa PKCS #10 – Format zahteve za certifikat PKCS #11 – Dostop do kripto naprave. Mednarodni standard za API, ki uporablja kriptografske funkcije. API si imenuje Cryptoki, vsebuje funkcije kot so RC2, RC4, RC5, MD5, SHA-1, DES, trojni DES, IDEA, RSA, DSA PKCS #12 – Zasebni ključi, certifikati, CRL.
Javacard	Industrijski standard, ki je osnova za javo v pametnih karticah. Objavil ga je Sun.
ISO 17799	Standard za upravljanje z varnostjo v zdravstvenih organizacijah.

3.4 Pametne kartice in varnost

Moderne kriptografske sisteme kontroliramo s ključi, ki določijo preoblikovanje podatkov. Lastnik ključa mora varno shraniti svoj ključ ter si prizadevati za varnost ključev in odgovornost zanje. Kriptografske ključe je zato smiselno shranjevati na ločenih napravah, kot so pametne kartice z vgrajenim sistemom, ki preprečuje njegovo odpiranje. Če se to vseeno zgodi, se samouniči celoten pomnilnik. Prava razlaga za uporabo pametnih kartic sta vsekakor varnost shranjenih podatkov na kartici in zaščita podatkov drugih računalniških sistemov. Pametna kartica omogoča svojemu lastniku ne le shranjevanje podatkov, temveč tudi varno obdelavo le teh.

Ker je naloga osredotočena na uvedbo pametnih kartic v zdravstvu, se bom osredotočil na varnost pametnih kartic uporabljenih v zdravstvu.

Glavni motiv za uvajanje pametnih kartic v zdravstvu je nadzor stroškov. Uporabljajo se za dokazovanje zdravstvenega zavarovanja pacienta, ki zahteva zdravstvene storitve.

Nove kartice zdravstvenega zavarovanja ne bodo služile več kot nosilec zdravstvenih podatkov ter podatkov o dokazovanju zdravstvenega zavarovanja, saj bo

zdravstveno osebje do podatkov prihajalo neposredno preko zdravstvenega portala sočasno z uporabo profesionalne kartice in kartice zdravstvenega zavarovanja.

Za dostop do podatkov na strežnikih bosta morali biti v bralniku kartic hkrati uporabljeni profesionalna kartica zdravstvenega delavca in kartica zdravstvenega zavarovanja pacienta. Zdravstveni delavec bo moral za uporabo svoje profesionalne kartice vnesti geslo (PIN) in tako dokazal, da je lastnik kartice.

V kolikor želimo pametno kartico uporabljati tudi za druge namene, moramo na KZZ namestiti tudi druga kvalificirana digitalna potrdila. V primeru, da v bralniku nista hkrati uporabljeni PK in KZZ, je potrebno zagotoviti overjanje pametne kartice z vnosom gesla. Na podlagi pravilno vnesenega gesla ima lastnik pametne kartice dostop do drugih podatkov in shranjenih digitalnih potrdil na kartici.

Uporaba pametnih kartic za hranjenje zasebnih ključev in profila zagotavlja, da se zasebni ključi nikoli ne prenesejo v spomin računalnika ali na disk, kjer bi bili lahko dostopni drugim. Na pametni kartici se ključi ustvarijo in se tam tudi shranijo. Tudi pri podaljšanju digitalnega potrdila se ključi na pametni kartici avtomatsko osvežijo. Nezaželena oseba lahko uporablja vaše digitalno potrdilo in zasebne ključe, če ima dostop do vaše pametne kartice in če pozna vaše geslo oziroma kodo PIN. Pametna kartica s profilom se mora hraniti tako, da ni dostopna nezaželenim osebam.

3.5 Uvedba digitalnih potrdil v drugih organizacijah v Sloveniji

Uporaba digitalnih potrdil za strežnike za to, da se omogoči šifrirana povezava z brskalnikom po protokolu SSL, je uveljavljena pri praktično vseh, ki se ukvarjajo s prodajo po internetu. S tem dosežemo to, da podatkov, ki jih je vtipkal uporabnik, ne more kdo prestreči, ker je povezava šifrirana, poleg tega pa uporabnik lahko preveri digitalno potrdilo strežnika in iz tega sklepa, ali se je priključil na pravi strežnik.

Uporabo potrdil v brskalnikih za overjanje svojih komitentov sta prvi začeli uporabljati NLB (1999) v aplikaciji Klik in SKB v aplikaciji SKBNet. Vsaka banka ima svojo službo za izdajanje digitalnih potrdil in tako potrdilo je uporabno samo za dostop do bančnih aplikacij ustrezne banke. Je pa možno nekatera potrdila, ki so jih izdale banke, uporabljati za dostop do aplikacij državne uprave.

Za elektronski način opravljanja storitev je ključnega pomena zagotavljanje ustrezne varnosti pri dostopu do posameznih aplikacij in podatkov, oziroma uvedbi takšne infrastrukture (infrastrukture javnih ključev IJK), ki bo zagotavljala zaupnost e-storitev in s tem varno elektronsko poslovanje. Omogočiti je potrebno mehanizme za nedvoumno ugotavljanje identitete, zaupnosti pri izmenjavi občutljivih podatkov,

dostop do podatkovnih baz in elektronski podpis. Najvišji nivo varnosti lahko zagotovimo z uporabo kvalificiranih digitalnih potrdil. Varnost pa še dodatno povečamo, če digitalna potrdila shranimo na pametno kartico.

Banka Koper je bila v Sloveniji med vodilnimi organizacijami, ki se je lotila projekta uporabe pametnih kartic s kvalificiranimi digitalnimi potrdili.

3.5.1 Banka Koper

V Banki Koper in v sistemu Activa uvajajo na področju elektronskega poslovanja vrsto novosti, ki bodo v naslednjih letih korenito posegle v naše vsakdanje plačilno okolje ter spremenile bančno poslovanje. Celoten sistem je že presegel število enega milijona bančnih in kreditnih kartic. Banka Koper za celoten sistem kartičnega poslovanja izvaja celovito informacijsko podporo in razvija ter uvaja nove tehnološke rešitve.

Na področju uvajanja tehnologije več aplikativnih pametnih kartic so pionirji v slovenskem prostoru (in tudi v svetovnem merilu), saj EMV več aplikativne kartice izdajajo že od avgusta 2003.

Uvajanje pametnih kartic je povezano s štirimi glavnimi značilnostmi, ki imajo za posledico finančne učinke:

- zmanjšanje stroškov zaradi povečane varnosti (zmanjšanje obstoječih oblik zlorab in preprečevanje novih)
- izboljšan nadzor nad porabo razpoložljivih sredstev in upravljanje s tveganji
- zmanjšanje operativnih stroškov
- novi poslovni izzivi in priložnosti

Kartica omogoča prvenstveno varen dostop do internetne banke po najstrožjih varnostnih merilih, del spomina na kartici v bankah sistema Activa je namenjen osebni uporabi imetnikov za elektronsko (digitalno) poslovanje, kar je popolna novost v bančništvu. To področje pokrivata dve programski rešitvi. Prvo tržijo preko paketa Burka – gre za IJK aplikacijo, ki pokriva področje uporabe javnih in zasebnih ključev in s katero je moč na kartici varno shraniti 4 različna digitalna potrdila in se nato z njimi predstavljati v elektronskem poslovanju preko njihovega CSP programa in upravitelja digitalnih potrdil.

Druga pa je namenjena internetno aktivnim uporabnikom, ki lahko v spomin pametne kartice shranijo različne osebne podatke (ime, domači naslov, službeni naslov, podatke o kreditnih karticah, priljubljenih spletnih povezavah, gesla za dostop do

zaščitenih spletnih strani, seznam naslovov, dodajajo beležke in samodejno izpolnjujejo obrazce na spletnih straneh).

Dopolnilno overjanje omogoča paket Maestral – gre za overjanje imetnika z dinamičnim geslom in je svetovna novost.

Na ta način so klasičnemu kartičnemu poslovanju dodali še funkcijo overjanje, s katero imetnik potrjuje svojo pristnost v različnih bančnih kanalih, med drugim tudi v telefonskem bančništvu in elektronski trgovini, z uporabo naprave za tvorjenje enkratnih gesel. Pri tem so uporabili tehhnologijo OTP (ang. One Time Password).

Hranjenje digitalnega potrdila na kartici bo vzpodbudilo njihove komitente k uporabi digitalnega poslovanja na vseh ravneh, uporaba osebnih podatkov iz kartice pa bo še bolj približala internetno poslovanje.

3.6 Pametne kartice namenjene uporabi v zdravstvu po svetu

Leto 2000 je mejnik, kar se tiče uvedbe zdravstvene kartice ne le v Sloveniji, ampak tudi v drugih državah: Nemčije, Belgije, Francije. Slovenski sistem je bil med tehnološko najsodobnejšimi z vidika varovanja podatkov in med najbolj izkoriščenimi, saj so bile uvedene številne aplikacije in rešitev celovito uvedena v celotnem zdravstvenem in zdravstveno-zavarovalniškem sistemu.

V zadnjih dveh letih pa nekatere evropske države pripravljajo in uvajajo še sodobnejše rešitve, ki temeljijo na karticah, ki se uporabljajo predvsem za namen identifikacije zavarovane osebe oziroma pacienta in zdravstvenega delavca v sistemu. Podatki pa se namesto na karticah vodijo na strežnikih, do katerih uporabniki v sistemu na varen način dostopijo skozi računalniška omrežja. Avstrija, kot ena izmed držav, ki je pri vzpostavitvi takšne rešitve prišla najdlje, je v novembru 2005 vzpostavila celovit nacionalni sistem.

3.6.1 Elektronska kartica zdravstvenega zavarovanja v Avstriji

Ob začetku projekta vzpostavitve več aplikativne pametne kartice v Avstriji je bila vizija uporabe pametne kartice naslednja:

- socialna varnost; zamenjava za vse papirne dokumente za zdravstveno zavarovanje
- e-zdravstvo; ključ za dostop do zdravstvenih podatkov
- e-uprava; elektronsko poslovanje z upravo

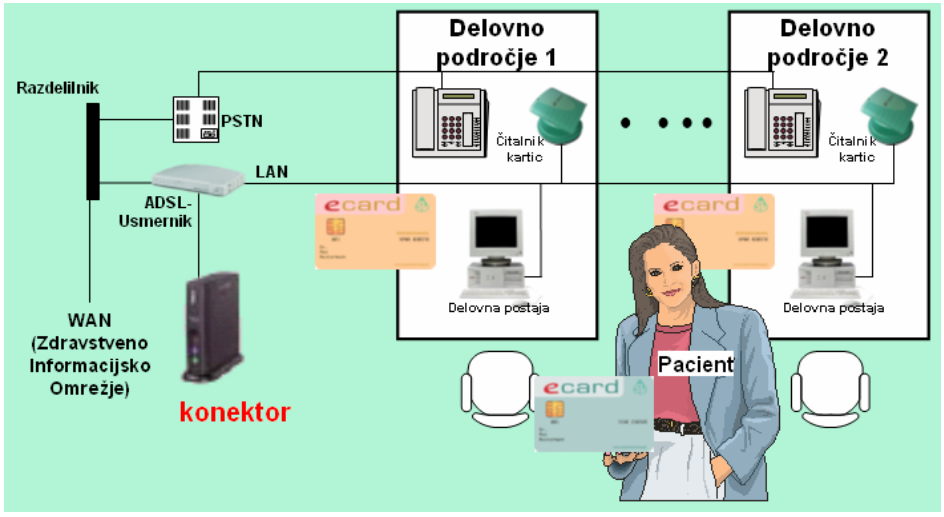
- e-aplikacije za tretje strani; uporaba osebnih podatkov shranjenih v javnem delu pametne kartice za identifikacijo
- e-poslovanje; elektronsko poslovanje s partnerji

Zahteve za mešan sistem so bile naslednje:

- dostop do osebnih podatkov po potrditvi lastnika kartice
- možnost zapisa zdravstvenih podatkov na pametni kartici
- kartični sistem mora zagotavljati transparentnost zdravstvenega dela in stroškov
- sprejem funkcionalnosti ostalih kartic, ki jih uporabljajo prebivalci (pripravljenost za e-upravo)
- standardiziran vmesnik do lokalne IT infrastrukture in omrežja
- sistem naj temelji na skupnih tehnoloških in industrijskih standardih
- zgledovanje na projekte v drugih evropskih državah
- elektronski podpis glede na SigG/SigV & VW-SigV
- dostopnost do podatkov v omrežju
- evropska kartica zdravstvenega zavarovanja na zadnji strani kartice zdravstvenega zavarovanja
- podpora evropski kartici in projektu Netc@rds

Delovno področje prenovljenega informacijskega sistema za uporaba pametne kartice v Avstriji prikazuje slika 3.5.

Slika 3.5: Delovno področje za uporabo pametne kartice



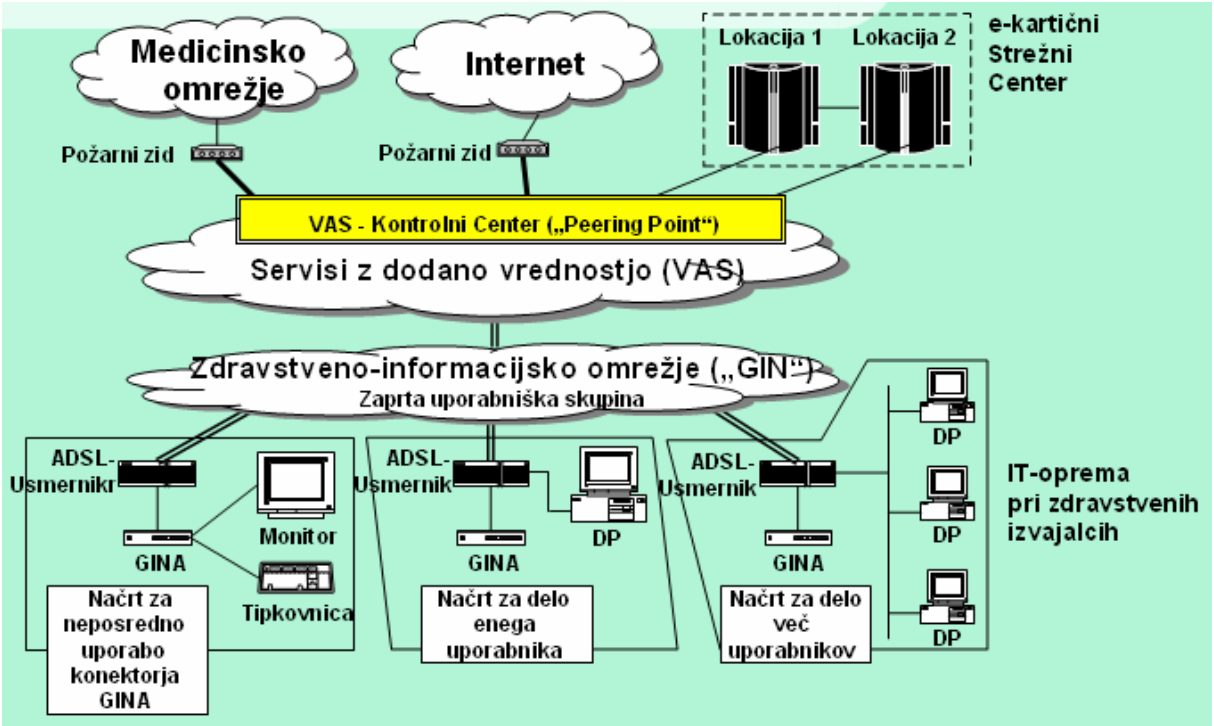
Vir: Otter, 2005

Prvi cilj uvedbe pametne kartice v Avstriji je bil nadomestiti uporabo vavčerjev zdravstvenega zavarovanja, ki so jih izdali 42 milijonov na leto. Z uvedbo pametne kartice so poleg ukinitve vavčerjev dosegli tudi naslednje prednosti:

- osem milijonov izdanih kartic je nadomestilo 42 milijonov letno izdanih vavčerjev,
- zaščita zasebnosti,
- lažji dostop do zdravniške pomoči,
- manjši administrativni stroški zdravniškega osebja,
- učinkovitost zdravstvenega osebja
- varen dostop do podatkov in s tem zmanjšanje administrativnih stroškov za socialno varnost

Dodatna varnost je zagotovljena z uporabo zaprtega zdravstveno informacijskega omrežja, do katerega ima dostop omejena skupina uporabnikov (zdravstveno osebje). Dostop do omenjenega omrežja je mogoča le preko vmesnika GINA, kar prikazuje slika 3.6

Slika 3.6: Za dostop do zdravstvenih podatkov se uporablja zaprto zdravstveno informacijsko omrežje



Vir: Otter, 2005

3.6.2 SNUH kartica zdravstvenega zavarovanja in MULTOS

Tajvanska nacionalna zdravstvena kartica je identična slovenski, saj nosi osebne zdravstvene podatke, pa tudi druge podatke, pomembne za zdravstveno zavarovanje, npr. zapise o bolnišničnem zdravljenju in podatke o medicinskih posegih in storitvah za zadnjih 6 let (proizvajalec Giesecke & Devrient, 32 KB).

Najdlje pa so na tem področju, po mojem prepričanju dospeli na področju ID kartic v HongKongu (najboljši svetovni projekt osebne izkaznice, MULTOS), na področju zdravstva pa v Južni Koreji. Njihova kartica SNUH (Seul National University Hospital) HealthOne card temelji na operacijskem sistemu MULTOS in omogoča poleg zdravstvenih aplikacij še naslednje:

- plačilne aplikacije: e-cash in /ali debetna/kreditna kartica,
- aplikacijo za spletno overjanje,
- aplikacijo za pripravo receptov preko spleta,
- življenjsko pomembne podatke za uporabo v nujnih primerih,
- brez kontaktni čip za uporabo v javnem transportu v Seulu.

Namen projekta pametne kartice v Južni Koreji je izboljšati zdravstvene storitve, kot tudi povečati skrb na področju zdravstva na nacionalnem nivoju. Pametna kartica HealthOne card shranjuje personalizirane zdravstvene informacije v varnem okolju in omogoča uporabnikom kartice elektronsko plačevanje receptov in ostalih storitev. Njihov cilj je, da bi podatkovna oblika zdravstvenega elektronskega recepta na pametni kartici HealthOne card postal standardna oblika v Koreji. Na sliki 3.7 je prikazana več aplikativna pametna kartica HealthOne card.

Slika 3.7: Pametna kartica HealthOne card

Vir: MULTOS, 2006

4 Infrastruktura javnih ključev (IJK)

IJK so si izmislili več kot dvajset let nazaj, vendar kljub temu še ni dosegla vseh svojih zmožnosti. IJK se uporablja za overjanje ljudi, za izogibanje pomnjenja večjega števila gesel (npr. PIN). Lahko se uporablja za varovanje komercialnih transakcij in zaščito elektronskih sporočil in telefonskih pogovorov. Toda število ovir, ki vključujejo pomanjkanje aplikacij, visokih stroškov, slabega razumevanja IJK, prispeva k omejeni uporabi IJK.

OASIS IJK tehnični komite (PKI TC) je definiral pet glavnih ovir, ki se pojavijo pri razvoju IJK:

- programske aplikacije ne podpirajo IJK,

- previsoki stroški,
- slabo razumevanje IJK,
- preveliko osredotočenje na tehnologijo, premalo na potrebe,
- slaba izvedba.

IJK vključuje mnogo strani od prodajalcev in uporabnikov, CA operaterjev, programerjev (za aplikacije, IJK komponente, platforme, knjižnice).

Uporaba infrastrukture javnih ključev omogoča najvišjo stopnjo varnosti pri elektronskem poslovanju. To je množica vseh komponent, ki upravljajo z digitalnimi potrdili in ključi za potrebe šifriranja in digitalnih podpisov. Varnostna aplikacija mora zagotoviti:

- zaupnost
- celovitost
- overjanje
- preprečavanje tajenja
- kontrolo dostopa

Zaupnost (ang. confidentiality)
Vsaka zaupna informacija, ki se prenaša po internetu, bi morala biti šifrirana. Šifriranje zaščiti občutljive informacije, vsebovane v elektronski pošti ali elektronskem trgovanju preko interneta. Skoraj vse rešitve pri zaupnosti podatkov uporabljajo metode šifriranja, ki je ena na najpomembnejših tehnoloških rešitev v elektronskem poslovanju.

Celovitost (ang. integrity)
Za določen tip podatkov so uporabniki interneta potrebovali zagotovilo, da se podatki niso spremenili med prenosom. Celovitost je lahko potrebna pri prenosu datotek preko elektronske pošte. Pri tem je potrebno odvreči dvom, da je bilo sporočilo med prenosom oziroma shranjevanjem spremenjeno, skrajšano ali mu je bilo kaj dodano.

Overjanje (ang. authentication)
Overjanje ali pristnost oziroma avtentikacija sporočila zagotavlja prejemniku, da je sporočilo res poslal navedeni pošiljatelj in je pristno. Pri uporabnikih interneta največkrat srečamo dve vrsti pristnosti:

- dokazana pristnost za dostopanje do nekega sistema oziroma strežnika,
- storitev mora zagotavljati, da povezava ni prestrežena ali motena na tak način, da bi neka tretja oseba prišla do možnosti neavtoriziranega oddajanja in sprejemanja podatkov. Iz tega sledi, da veliko sporočil, transakcij in

elektronske pošte preko interneta, zahteva dokazovanje pristnosti vira. To lahko naredimo z uporabo digitalnega podpisovanja, digitalnih potrdil, itd.

Preprečavanje tajenja (ang. non repudiation)
Preprečevanje tajenja ali nezavrnitev pomeni ustvarjanje dokaza o izvoru podatkov oziroma posredovanju podatkov. Pomeni zaščito pred tem, da bi pošiljatelj lažno zanikal, da je podatke poslal, ali da bi prejemnik lažno zanikal, da je podatke prejel. Pošiljatelj sporočila lahko dokaže, da je prejemnik sporočilo res prejel. Najpogosteje gre v tem primeru za različne pravne spore med dvema poslovnima strankama. Na nezmožnost zavrnitve sporočila uporabnika veže njegov digitalni podpis.

Kontrola dostopa oziroma avtorizacija (ang. access control)
Uporabnikom je potrebno zagotoviti avtoriziran dostop do podatkov ali storitev pod določenimi pogoji. Omogoča, da berejo vsebino samo tisti, ki jim je namenjena.

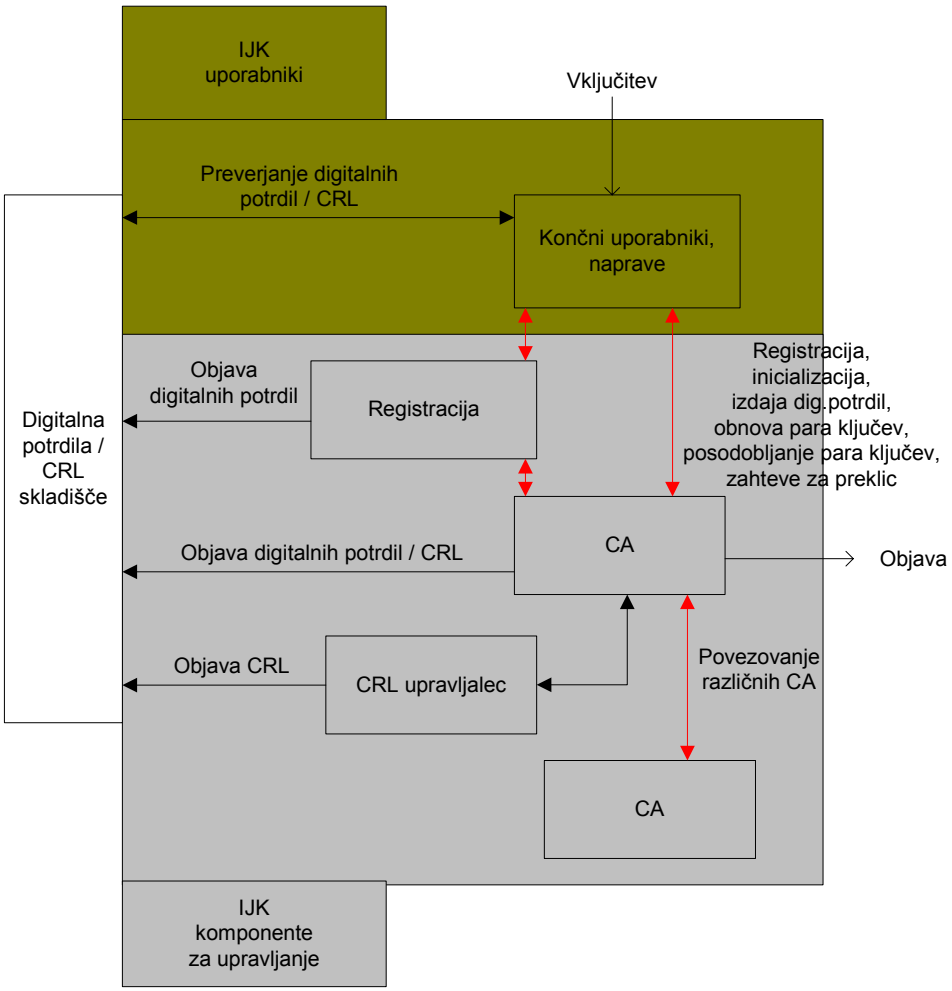
Infrastrukturo javnih ključev določajo postopki in oprema za:

- ustvarjanje in hranjenje ključev,
- overjanje imetnikov ključev in izdajanje digitalnih potrdil javnih ključev,
- objavljanje digitalnih potrdil (imeniki),
- preklicevanje digitalnih potrdil,
- časovno označitev postopkov.

Središčni del predstavlja overitelj javnih ključev (ang. Certification Authority -CA). Vsak overitelj objavi svoj javni ključ in dokument (ang. Certification Policy), ki opisuje postopek, kako in komu podeljuje potrdila ter na kakšen način varuje svoj zasebni ključ.

S komponento Končni uporabniki, (ang. End Entity) smatramo vse končne uporabnike in naprave (strežniki, usmerjevalniki, itd.). Komponenta Registracija (ang. Registration Authority RA) je namenjena za izvajanje vrste administrativnih funkcij, za katere jo pooblasti agencija za izdajo digitalnih potrdil. Agencija, ki izdaja digitalna potrdila (ang. Certification Authority CA), običajno skrbi tudi za objavo črne liste (CRL) ter izvaja še mnogo drugih funkcij, pogosto pa izvajanje funkcij preda tudi drugi komponenti (Registracija). CRL upravljalec (ang. CRL Issuer) je opcijska komponenta, ki jo lahko CA pooblasti za objavo črne liste.

Slika 4.1 Prikazuje arhitekturni model IJK



Vir: www.pkiforum.org, 2002

4.1 Uporaba tajnopisja v internetu

Tajnopisje oziroma kriptografija je znanost o prevajanju nezaščitenih podatkov v zaščitene in obratno.

Metode šifriranja in zagotavljanja varnosti so:

- simetrično,
- asimetrično,
- hibridno.

Simetrično šifriranje je enostavno šifriranje, kjer se pošiljatelj in prejemnik sporočila dogovorita o metodi šifriranja oziroma ključu, ki bo sporočilo zašifriral in dešifriral. Pošiljatelj z algoritmom za šifriranje zaščiti sporočilo in ga pošlje prejemniku.

Prejemnik sporočilo dešifrira z enakim ključem. Prednost simetričnega šifriranja je enostavnost in hitrost. Glavni problem simetričnega šifriranja pa je slaba varnost in kopičenje ključev z vsakim novim udeležencem posla.

Asimetrično šifriranje je izpopolnjeno simetrično šifriranje. Temelji na dveh ključih; zasebnem in javnem. Javni ključ se uporablja za šifriranje, zasebni pa za dešifriranje. Takšen način šifriranja zagotavlja zaupnost in nadzor nad dostopom do sporočila. Zaradi zapletenih algoritmov šifriranja je mnogo počasnejše od simetričnega šifriranja. Konkretna uporaba asimetričnega šifriranja je elektronski podpis, kjer se s posebnim postopkom zgosti vsebina sporočila, (rezultat zgoščevanja je število) in to število/vsebina se podpiše z zasebnim ključem.

Hibridno šifriranje je sestavljeno iz obeh zgoraj opisanih algoritmov. Za šifriranje se uporabi simetrični način (zasebni ključ), za prenos simetričnega ključa pa se uporabi asimetrični način. Simetrični način zagotavlja hitrost, asimetrični pa varnost prenosa šifriranega sporočila.

Danes so varnejši znani, javni in preizkušeni algoritmi, pri katerih je vsa tajnost zagotovljena s ključem. Pri varovanju podatkov uporabljamo simetrične, asimetriče ter zgoščevalne algoritme. Šifriranje podatkov je lahko vključeno v katerikoli komunikacijski sloj.

Podatki na internetu se šifrirajo z uporabo protokola IPSec (ang. Internet Protocol Security). Uvaja celovit pristop k zaščiti prenosa podatkov v omrežjih IP. Gre za skupino protokolov, ki določajo šifriranje na nivoju IP (omrežni komunikacijski sloj). Omogoča tudi gradnjo navideznih zasebnih omrežij (v praksi se uporablja kratica VPN). IPSec je vgrajen v različne produkte, ki podpirajo današnjo verzijo IPv4 in je del protokola IPv4, kar pomeni, da je pričakovati njegovo splošno uporabo. Zašifrirano je vse od glave omrežnega sloja naprej, torej vsi podatki, ki niso potrebni za usmerjanje paketov. IPSec je odprt standard. Sestavljajo ga:

- dogovor o načinu šifriranja in izmenjava ključev (Key Management),
- preverjanje nespremenjenosti podatkov in overjanje brez šifriranja (ang. Authentication Header - AH)
- šifriranje podatkov (ang. Encapsulating Security Payload - ESP).

V tunelskem načinu delovanja je omogočena tudi gradnja navideznih zasebnih omrežij. Obstaja tunelski in transportni način pošiljanja podatkov. Transportni način uporabe AH ali ESP se uporabi, kadar med sabo neposredno komunicirata dve delovni postavi preko interneta. V kolikor pa med seboj komunicirata dve delovni postaji preko posrednika (iz notranjega omrežja), se uporabi tunelski način. Če

potrebujemo samo overjanje, je uporaba protokola AH veliko bolj racionalna kot uporaba ESP.

Za elektronsko pošto se najbolj pogosto uporablja šifriranje sporočil z aplikacijo PGP (Pretty Good Privacy). Od verzije 5 naprej pa je možno izbirati med algoritmi RSA, Diffie-Hellman ter DSA, med simetričnimi pa med IDEA, CAST, trojni DES, Twofish in AES. Ključ za asimetrični algoritem Diffie-Hellman je lahko dolg do 4096 bitov, za RSA do 2048 bitov. Potrdila niso v skladu s standardom X.509v3. V plačljivi verziji pa je na voljo tudi možnost, da imamo potrdilo v tem formatu in ga pridobimo od overitelja javnih ključev. Ko imamo dopisnikov javni ključ, mu pošljemo podpisano šifrirano sporočilo. PGP iz datoteke najprej izračuna povzetek z zgoščevalno funkcijo in ga zašifrira s privatnim ključem pošiljatelja z algoritmom RSA, oziroma drugim izbranim asimetričnim algoritmom. Ta podpis doda datoteki in vse skupaj zgosti s postopkom ZIP. Izračuna enkratni ključ (ang. session key) in z njim zašifrira zgoščeno datoteko z uporabo izbranega simetričnega algoritma. Zdaj z naslovnikovim javnim ključem zašifrira enkratni ključ po asimetričnem algoritmu in vse skupaj doda prejšnji datoteki. Rezultat je šifrirano sporočilo (8-bitni znaki). To običajno pretvori v berljive znake s programom radix64 (iz treh 8-bitnih znakov naredi štiri 6-bitne). Tako prirejeno sporočilo potuje do naslovnika. Tu se vsi postopki odvijejo v obratnem vrstnem redu. Priporočljivo je, da pošiljatelj in prejemnik uporabljata isto verzijo PGP. Pri kreiranju ključa izberemo, da se bodo vsa sporočila, zašifrirana s tem ključem, zašifrirala tudi s ključem organizacije (ang. Additional Decription Key ADK), za katero delamo in s tem omogočimo, da lahko dešifriramo datoteke, ki so jih zašifrirali bivši zaposleni. V plačljivih verzijah je na voljo PGPnet, ki omogoča vzpostavljanje navideznih zasebnih povezav (VPN) na nivoju IP po protokolu IPsec.

Za povezovanje osebnih računalnikov s strežniki se uporablja protokol SSL (Secure Socket Layer). Naslednik SSL protokola je TLS (Transport Layer Security) protokol. Gre za šifrirano povezavo med strežnikom in odjemalcem. Pri Netscape-u so si pri razvoju SSL zastavili še naslednje naloge:

- odprtost - lahko ga implemetirajo drugi proizvajalci,
- možnost dograjevanja z novimi kriptografskimi algoritmi,
- učinkovitost; parametri, izmenjani s pomočjo asimetričnih algoritmov, ki so dosti počasnejši od simetričnih, se nekaj časa hranijo zato, da se asimetrični algoritmi izvajajo manjkrat.

SSL je postal 'de facto' standard. Omogoča zaščito za vse aplikacijske protokole nad TCP (http, smtp, news, pop3, ldap, itd.). SSL zaščiti zgolj povezavo med dvema postajama, medtem ko ostanejo podatki na delovnih postajah nezaščiteni.

Za varno povezovanje mobilnih aparatov s strežniki se najpogosteje uporablja WTLS (Wireless TLS) protokol. WTLS je tako prirejen TLS, da podpira izmenjavo paketov na nezanesljivih in počasnih povezavah. Element, ki služi za overitev mobilnega aparata, imenujejo Wireless Identity Module - WIM. Njegova naloga je, da izvaja kriptografske operacije, kadar se to od klienta zahteva. Zagotoviti je potrebno tudi digitalno podpisovanje ter zaščito podatkov od mobilnega aparata do strežnika z uporabo kriptografske funkcije.

Za oddaljen dostop do strežnikov in nalaganje datoteke je najbolj razširjen protokol SSH (Secure Shell). SSH je do danes skoraj v celoti izpodrinil telnet, rlogin, rsh in ftp, kjer je promet potekal nezašifrirano. Glede na to, da je OpenSSH zastonj, danes njegova uporaba prevladuje. Obstajata dve verziji protokola, ki med seboj nista kompatibilni; SSH1 in SSH2. SSH2 popravlja napake SSH1 in je zato varnejši, OpenSSH pa podpira obe verziji protokola. V kolikor overjanje strežnika in odjemalca poteka s ključi RSA, ne potrebujemo digitalnih potrdil kot pri SSL. Po namestitvi OpenSSH najprej ustvarimo pare ključev za strežnik in odjemalce.

Najbolj uporabljen asimetrični algoritem je RSA (v Ameriki DSA), ki je ime dobil po njegovih avtorjih. V prihodnosti pa bodo prevladovali asimetrični algoritmi, ki bodo temeljili na eliptičnih krivuljah (ECC), vsaj pri manj zmogljivih napravah, saj so dolžine ključev občutno krajše kot pri sistemu RSA.

Pri kriptografiji upoštevamo Kerckhoffov princip, poimenovan po Augustu Kerckhoffu, ki pravi, da nasprotnik pozna kriptosistem in algoritme, ne pa tudi ključev, ki nam zagotavljajo varnost.

Za razumevanje komunikacije aplikacij na različnih računalnikih je potrebno tudi poznavanje OSI referenčnega modela.

4.2 Strežnik ključev

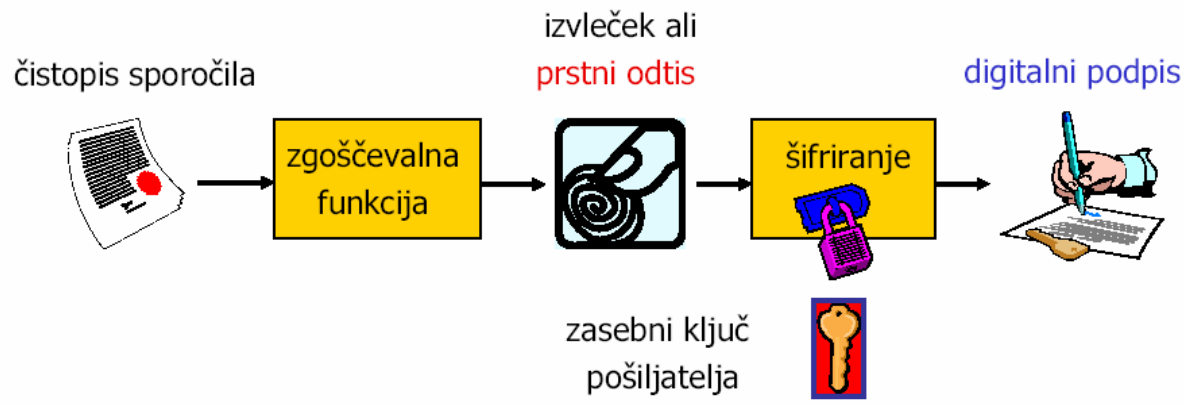
Za šifriranje podatkov vedno uporabljamo simetrične algoritme, ki so hitrejši od asimetričnih, težko pa je varno izmenjati ključ. Problem predstavlja tudi veliko število ključev, saj moramo imeti za vsakega dopisovalca svoj ključ. Ena od rešitev je centralni strežnik ključev (npr. Kerberos), s katerim se povežemo, pri tem pa dobimo začasni ključ, ki ga lahko uporabita le pošiljatelj in prejemnik, ali pa uporabimo asimetrični algoritem. Strežnik ključev ima bazo s podatki o uporabnikih, njihovih skritih ključih in njihovih dovoljenjih. Ob zahtevi za priključitev na nek strežnik preveri, ali ima uporabnik pravico dostopiti do njega.

V protokolih SSL in IPSec vedno uporabimo asimetrični algoritem za izmenjavo skupnega skritega ključa (npr. protokol Diffi Helman, digitalno potrdilo, PGP).

4.3 Zgoščevalne funkcije

V aplikacijah, ki omogočajo zaupnost pošiljanja sporočil, se uporabljata obe vrsti algoritmov. Obenem vključujejo zgoščevalne funkcije (ang. hash function), ki poljubno dolg tekst preslikajo v število fiksne dolžine (npr. 128 bitov). Izvleček (ang. Digest) imenujemo tudi prstni odtis (ang. Digital Fingerprint) sporočila. Zgoščevalna funkcija je enosmerna funkcija. Slika 4.2 prikazuje postopek zgoščevalne funkcije.

Slika 4.2: Postopek zgoščevanja sporočila



Vir: www.lkn.fe.uni-lj.si/, 2005

Danes so poznane zgoščevalne funkcije z uporabo ključa (ang. Keyed hash function), ki jih pogosto označujemo s terminom MAC (ang. Message Authentication Code) in zgoščevalne funkcije brez uporabe ključa (ang. Unkeyed hash function), ki jih označujemo s terminom MDC (ang. Modification Detection Code).

Danes najbolj znani in uporabni zgoščevalni funkciji brez uporabe ključa sta MD5 in SHA-1:

- dolžina sporočil je omejena na 2^{64} bitov,
- MD5 je računsko manj zahteven od SHA-1 (razmerje hitrosti je 7 proti 3),
- algoritem SHA-1 ima daljši izvleček (160 bitov proti 128 bitov),
- algoritem SHA-1 je del standarda (DSS).

Poleg teh dveh zgoščevalnih algoritmov se uporabljajo tudi SHA-256, SHA-384, SHA-521, RIPEMD-128, RIPEMD-160 in Haval / 128 / 160 / 192 / 224 / 256. Številke poleg imen predstavljajo dolžino izhoda v bitih.

Glavni namen zgoščevalne funkcije s ključem MAC je overjanje sporočila, ki nam zagotavlja integriteto sporočila in overjanje izvora za datoteke, poslane med dvema uporabnikoma (primer uporabe je SSL).

Od zgoščevalne funkcije pričakujemo, da:

- je nemogoče najti dve različni sporočili, ki bi ju preslikala v isti blok,
- isto sporočilo vedno preslika v enak blok,
- iz zgoščevalnega bloka ni mogoče restavrirati sporočila (od tu ime enosmerna zgoščevalna funkcija),
- vsaka sprememba v sporočilu povzroči spremembo zgoščevalnega bloka.

4.4 Digitalni podpis

K sreči vse več podjetij razume, da elektronsko poslovanje ni samo sebi namen ali nujno zlo, ampak je njegovo bistvo v izjemnih prihrankih in optimizaciji poslovnih procesov. V središču elektronskega poslovanja, kot ga definirata evropska in slovenska zakonodaja, je digitalni podpis in sredstva ter mehanizmi za vzdrževanje njegove veljavnosti.

Praviloma se za dostop do aplikacije izvaja overjanje uporabnikov na podlagi njihovega uporabniškega imena in gesla, redkeje tudi s pomočjo digitalnega potrdila.

Če želimo rezultat elektronsko podprtih procesov (dokumenti, revizijske sledi in dnevniške datoteke) obdržati izključno v elektronski obliki, ki naj ima tudi trdno dokazano vrednost, je treba uporabiti digitalni podpis.

Digitalni podpis je elektronski podpis, narejen z uporabo kriptografije in je šifrirani izvleček sporočila. Omogoča overjanje, celovitost in nezatajljivost, ne zagotavlja pa zasebnosti podatkov. Digitalni podpisi temeljijo na asimetrični kriptografiji, zato potrebujemo par ključev. Zasebni ključ uporabljamo za podpisovanje, javni ključ pa za preverjanje veljavnosti podpisov.

Javni ključ mora nositi garancijo, da res pripada navedenemu uporabniku. Urad za overjanje potrjuje verodostojnost javnih ključev z digitalnim podpisom odgovorne osebe. Uporabnik javnega ključa se mora ob registraciji identificirati in s tem prevzame odgovornost za uporabo zasebnega ključa. Registracijo izvrši uradna oseba (ang. Registration Authority RA).

Danes se običajno uporablja asimetrične algoritme. Namesto da z zasebnim ključem šifriramo celotno sporočilo, iz njega najprej naredimo prstni odtis dokumenta z ustreznim matematičnim algoritmom, ki enolično predstavlja dokument. Tako

šifriramo z zasebnim ključem le prstni odtis, dokument pa ostane nespremenjen. Rezultat, ki ga dobimo, je v resnici digitalni podpis dokumenta (slika 4.3).

Za digitalni podpis se ponavadi uporablja kombinacija:

- zgoščevalna funkcija SHA-1,
- asimetrični šifrirni algoritem RSA,
- v standardnem formatu digitalnega potrdila X-509 je v enem polju zapisan tudi tip zgoščevalne funkcije in šifrirni postopek (v spletnem potrdilu SIGEN-CA je algoritem podpisa sha1RSA).

NIST je leta 1991 postavil standard za digitalni podpis DSS. DSS podpisuje zgoščevalno funkcijo SHA-1 in šifrirni algoritem DSA.

Slika 4.3: Postopek digitalnega podpisovanja dokumenta

Vir: SETCCE, 2005

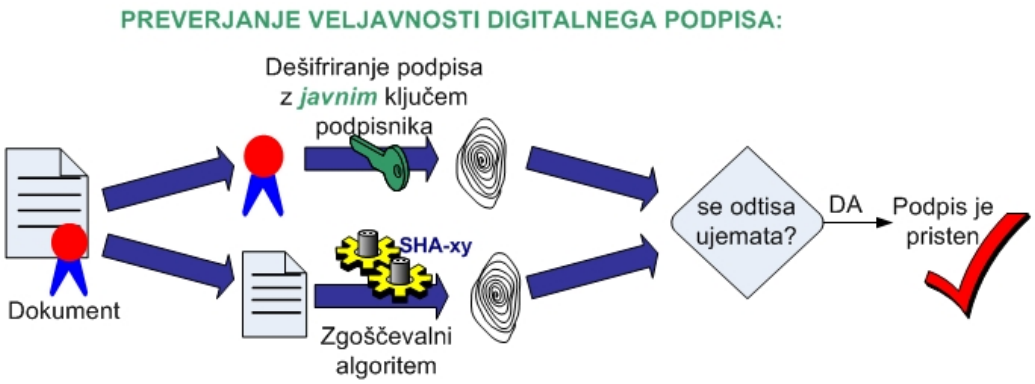
Ko prejemnik prejme dokument s priloženim digitalnim podpisom, najprej odšifrira digitalni podpis z javnim ključem podpisnika (javni ključ izlušči iz digitalnega potrdila, ki je praviloma pripeto digitalnemu podpisu). Rezultat je prstni odtis, ki ga je ustvaril že podpisnik dokumenta. Nato prejemnik iz izvirnega dokumenta tudi sam ustvari njegov prstni odtis. Sledi primerjava novo ustvarjenega (tega, ki ga je izračunal prejemnik) in izvornega (tistega, ki ga je ustvaril podpisnik) prstnega odtisa dokumenta. Če se odtisa ujemata, je prejemnik lahko prepričan, da je podpis veljaven. Postopek preverjanja digitalnega podpisa je prikazan na sliki 4.4.
Pošiljatelj z digitalnim podpisom zagotovi:

- verodostojnost sporočila,
- potrjuje svojo identiteto in s tem
- sprejme tudi odgovornost za sporočilo.

Prejemnik lahko hkrati preveri verodostojnost in avtentičnost, ali je sprejeto sporočilo res enako oddanemu sporočilu in ali nam sporočilo res pošilja predstavljeni pošiljatelj.

Elektronski podpis mora biti izveden v skladu z načelom WIPIWIS (ang. What Is Presented Is What Is Signed) in zavestno s strani podpisnika. Podpisnik mora biti vnaprej obveščen o postopku podpisa. Nezavestna izvedba e-podpisa mora biti onemogočena, razen v primerih avtomatskega podpisa strežnika oz. aplikacije (CVI, 2003).

Slika 4.4: Postopek preverjanja digitalnega podpisa



Vir: SETCCE, 2005

4.4.1 Digitalna potrdila in overitelji

Digitalno potrdilo je javni ključ in informacija o njegovem lastniku, ki jo digitalno podpiše oseba ali organizacija, ki ji zaupamo. Drugo rešitev predstavljajo overitelji javnih ključev (certifikatske agencije CA). Po zakonu o elektronskem poslovanju in elektronskem podpisu je varen elektronski podpis, overjen s kvalificiranim digitalnim potrdilom, glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost.

Namen kvalificiranih digitalnih potrdil (Overitelj na MJU, str 11) je:

- upravljanje, dostop in izmenjava podatkov,
- varno elektronsko komuniciranje med imetniki potrdil in
- storitve oziroma aplikacije, za katere se predvideva uporaba potrdil.

Digitalno potrdilo predstavlja enolično povezavo med imetnikom potrdila in javnim ključem. Digitalno potrdilo se vedno izda na podlagi verodostojnega naročila, ki omogoča, da se pred izdajo digitalnega potrdila preveri ali so podatki, ki bodo

zapisani v datoteko digitalnega potrdila točni in ažurni. Potrdilo vsebuje vse osnovne podatke o imetniku in javni ključ. Vsako kvalificirano digitalno potrdilo ima par ključev, zasebnega za tvorbo digitalnega podpisa in javnega, ki je dostopen vsakomur. V kolikor ne gre za zaprt sistem uporabnikov, so digitalna potrdila javno objavljena, kar omogoča ugotovitev in preverjanje identitete podpisnika na osnovi njegovega javnega ključa.

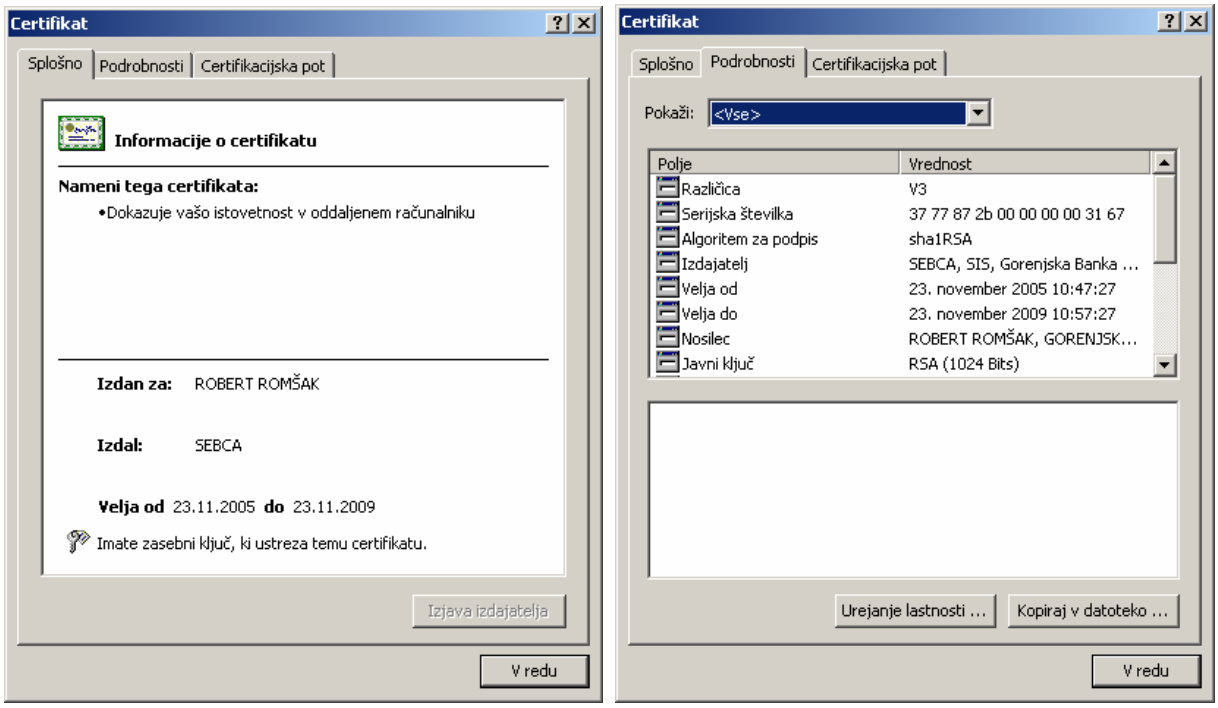
Oblika digitalnega potrdila po standardu ISO/IEC X.509V3:

- verzija (zdaj do verzije 3)
- serijska številka (enolična za potrdila posameznega overitelja)
- algoritmi in parametri (npr. SHA1 in RSA)
- izdajatelj (overitelj javnih ključev)
- datum veljavnosti od-do
- prejemnik digitalnega potrdila (njegovo ime, drugi podatki o njem)
- podatki o njegovem javnem ključu:
- algoritem
- parametri
- javni ključ
- enolična oznaka uporabnika (samo v verzijah 2 in 3)
- razširitve (verzija 3)
- digitalen podpis teh podatkov, ki je narejen z zasebnim ključem CA

Veljavnost kvalificiranih digitalnih potrdil je omejena na dobo največ petih let in jo določi izdajatelj digitalnih potrdil. Overitelj običajno določi rok veljavnosti podatkov za elektronski podpis. Z uredbo je zato predpisano, da mora kdor hrani elektronsko podpisane podatke, najkasneje en mesec pred iztekom tega roka zagotoviti ponoven podpis podatkov. Pri tem morajo sodelovati vse osebe, ki so podatke elektronsko podpisovale prvič. Pri ponovnem podpisu podatkov lahko sodeluje tudi notar, ali pa podatke podpišemo z varnim časovnim žigom overitelja (Odin, 2000, str. 9). Slika 4.5 prikazuje informacije, ki jih vsebuje digitalno potrdilo.

Z uporabo digitalnih potrdil za strežnike, kar omogoči zašifrirano povezavo z brskalnikom po protokolu SSL dosežemo to, da podatkov, ki jih je vtipkal uporabnik, ne more prestreči nepooblaščena oseba, ker je povezava zašifrirana. Poleg tega pa uporabnik lahko preveri digitalno potrdilo strežnika in iz tega sklepa, ali se je povezal na pravi strežnik.

Slika 4.5: Informacije, ki jih vsebuje digitalno potrdilo



Vir: Lasten

4.4.1.1 Časovno žigosanje

Eden od korakov k povečanju verodostojnosti elektronsko podpisanih dokumentov pomeni časovno žigosanje. Pri tem postopku dokumentu dodamo digitalni podpis, ki povezuje čas podpisa s podatki v dokumentu. Digitalni podpis, ki ga opravimo sami, ne nosi verodostojnega podatka o času, kdaj je bil opravljen! Dokument namreč podpisujemo na svojem računalniku in vključevanje sistemskega časa bi bilo nesmiselno, saj ni mogoče dokazati, da je bil le-ta v času podpisa točen.

Namen varnih časovnih žigov (Overitelj na MJU, str 11) je:

- zagotavljanje obstoja dokumenta v določenem časovnem trenutku tako, da se poveže datum in čas žigosanja z vsebino dokumenta na kriptografsko varen način,
- povsod, kjer je potrebno na varen način dokazati časovne lastnosti transakcij in drugih storitev,
- za druge potrebe, kjer se potrebuje varen časovni žig.

Če želimo za neko pomembno pogodbo ali oporoko preprečiti, da bi kdo kasneje oporekal njeni veljavnosti, si zagotovimo nepristransko pričo, ki bo prav tako kot vpletene stranke, podpisala dokument. Podobno vlogo kot nepristranska priča za

običajne dokumente ima izdajatelj časovnih žigov za elektronske dokumente. V angleščini se je zanj uveljavil naziv Time Stamp Authority oziroma kratica TSA.

Gre za dobro zaščiten strežnik. Podobno kot za izdajatelja digitalnih potrdil morajo biti izpolnjeni strogi varnostni ukrepi, sicer bi lahko dvomili v njegovo verodostojnost oziroma nepristranskost. Sinhroniziran je s časovnimi strežniki in tako zagotavlja točen čas.

Če tak časovni podpis izvede nek neodvisen strežnik oziroma institucija, ki ni pod kontrolo siceršnjih podpisnikov dokumenta, ob kasnejših preverjanjih ni dvomov o tem, kdaj je bil dokument podpisan in kakšen je bil ob podpisu, če se prstni odtis dokumenta v žigu ujema s prstnim odtisom, narejenim ob času preverjanja.

Tak časovni overitelj od novembra 2003 deluje tudi na Ministrstvu za javno upravo.

4.5 Varnost e-storitev

Gledano na splošno v vsakem računalniškem sistemu varujemo v njem shranjene podatke in zaradi tega moramo vire v omrežju identificirati in zanje določiti načine varovanja. Za varovane vire moramo zagotoviti varnost dostopa, varnost uporabe in varnost transakcij.

Storitve, ki se vršijo na elektronski način, morajo zagotoviti enak ali celo višji nivo varnosti in zaupanja, kot storitve, ki se vršijo na klasičen način. Omogočiti je potrebno mehanizme za nedvoumno ugotavljanje identitete, zaupnost pri izmenjavi občutljivih podatkov, avtenticiran dostop do podatkovnih baz, obstajajo pa tudi številne aplikacije, ki so povezane z elektronskimi podpisi oziroma potrebujejo le-te za delovanje. Najvišji nivo varnosti dosežemo z uporabo digitalnih potrdil in pametnih kartic, ki so varno sredstvo za shranjevanje digitalnih potrdil.

Varnost lahko definiramo kot minimalno ranljivosti virov. Ranljivost je kakršna koli slabost sistema, ki bi bila lahko izkoriščena proti sistemu samemu ali podatkom v njem.

V varnostne rešitve elektronskih storitev morajo biti poleg osnovnih vidikov, ki jih lahko zagotovimo z uporabo kvalificiranih digitalnih potrdil, vpeti tudi ostali splošni pogoji zagotavljanja varnosti (CVI, 2003):

- zaščita sistema s požarno pregrado,
- sistem za spremljanje vdorov,
- sistem za alarmiranje,

- varnostno kopiranje dokumentov,
- protivirusna zaščita,
- zagotovitev visoke razpoložljivosti sistema,
- opozarjanje in izobraževanje uporabnikov o varnem ravnanju.

Glede na to, da je v nalogi veliko govora o tajnopisju in šifriranju, digitalnem podpisu in overjanju digitalnih potrdil, bom v tem delu namenil le nekaj besed le o požarni pregradi, v naslednjem razdelku pa tudi varnostni politiki.

Požarno pregrado sestavlja sklop opreme, ki jo tvorijo komunikacijska oprema in računalniki. Glavni namen požarne pregrade je, da nepooblaščenim osebam ali osebam in privatnega omrežja onemogoči dostop do našega omrežja. Vsa sporočila, ki gredo preko požarne pregrade, se preverijo in v primeru neizpolnjevanja varnostnih zahtev tudi izločijo. Dostop do določenega omrežja lahko požarna pregrada nadzoruje na dva načina:

- restriktiven dostop (ang. Restrictive access), ki ne dovoljuje ničesar razen strogo dovoljenega prometa in
- dopusten način (ang. Permissive access), ki dovoljuje vse razen tveganega prometa

Priporočljivo je upoštevati standarde ISO 17779: 2000 in BS 7799-2:2002.

Varnost se ne da zagotoviti le z uporabo novih tehnologij in sodobne telekomunikacijske opreme. Velja ravno obratno, saj nove tehnologije same po sebi praviloma omogočajo še učinkovitejše napade.

4.5.1 Varnostna politika

Za uspešno zaščito sistema pred različnimi napadi moramo najprej izdelati varnostno politiko. Oceniti moramo (Tomažič, 2006):

- kdo ogroža informacijski sistem in kako je ogrožen,
- koliko so vredni podatki, ki jih želimo zaščititi,
- kako trajna je vrednost zaščitenih podatkov,
- kolikšno škodo lahko povzročijo napadalci,
- kako in v kolikšni meri je za poslovanje pomembna odprtost sistema do javnega omrežja in
- kakšne stroške bi imeli z uvedbo ustreznih zaščitnih ukrepov, pri čemer moramo upoštevati tako neposredne kot tudi posredne stroške.

Na osnovi zgornje analize je mogoče izdelati varnostno politiko, ki določa:

- kateri deli informacijskega sistema so bolj vitalni in jih je potrebno bolj zaščititi,
- kateri uporabniki imajo pravico dostopa do javnega omrežja in kakšne so te pravice,
- kakšne zaščitne ukrepe bomo uvedli (požarni zid, protivirusna zaščita, ločitev delov omrežij, itd.) in
- določiti pravila obnašanja uporabnikov sistema.

Stroški vzpostavljanja varnosti ne smejo preseči potencialne škode, ki bi nastala ob vdoru v sistem.

Pravila obnašanja uporabnikov igrajo ključno vlogo pri zagotavljanju varnosti, zato je potrebno izobraževanje in obveščanje uporabnikov informacijskega sistema.

4.5.2 Zakonodaja

Slovenija je zakonodajo s področja pravne ureditve elektronskega poslovanja sprejela dokaj zgodaj, saj spada med prvih deset evropskih držav, ki so sprejele zakonodajo na področju elektronskega poslovanja in elektronskega podpisovanja (Silič, 2001, str. 6).

Država želi s tem zakonom spodbujati hiter tehnološki razvoj elektronskega poslovanja s posebnim poudarkom na izenačitvi zanesljivih elektronskih oblik s klasično papirno obliko in izenačitvi varnih in zanesljivih elektronskih podpisov z lastnoročnim podpisom.

Zakon vzpostavlja jasna in predvidljiva pravila za izmenjavo elektronskih sporočil ter pravila za uporabo elektronskega podpisa. Zakon se ujema tudi s tujo in evropsko ureditvijo ter je tako omogočil mednarodno priznavanje elektronskih podpisov.

Elektronsko poslovanje zahteva spoštovanje zakonodaje, pravilnikov, direktiv, tehničnih standardov in uredb EU in zakonskih podlag sprejetih v Sloveniji.

Poleg ZEPEP je potrebno upoštevati še ostala pravila in zakonodajo, sprejeta v Sloveniji in EU:

- Zakonodaja elektronskega poslovanja EU
  - Direktiva o skupnem ogrodju za elektronski podpis,1999/93/EC
  - Direktiva o zasebnosti in elektronskih komunikacijah, 2002/58/EC,
  - Direktiva o elektronskem poslovanju, 2003/31/EC,

- Obligacijsko pravo pri sklepanju pogodb v elektronski obliki
- Zakon o varstvu osebnih podatkov
- Zakon o zdravstvenem varstvu in zdravstvenem zavarovanju
- Pravila obveznega zdravstvenega zavarovanja
- Uredba o poslovanju organov javne uprave z dokumentarnim gradivom
- Zakon o zbirkah podatkov s področja zdravstvenega varstva
- Zakon o odvzemu in presaditvi delov človeškega telesa zaradi zdravljena
- Pravilnik o kartici zdravstvenega zavarovanja

Tehnični standardi za elektronsko poslovanje v EU so potrebni za potrjevanje tehničnih produktov ter za nadzor in potrjevanje elektronskih storitev. Evropska komisija je za poenotenje pooblastila naslednje institucije:

- CEN (EU Committee for Standardization),
- CENELEC (EU Committee for Electrotechnical Standardization),
- ETSI EU (Teleccomunication Standards Institute).

4.6 Izdajatelji oziroma overitelji digitalnih potrdil

Digitalna potrdila izdajajo različni overitelji z različno stopnjo varnosti. Overitelj igra osrednjo vlogo pri infrastrukturi javnih ključev.

Overitelji so fizične ali pravne osebe, ki izdajajo potrdila (v elektronski obliki, ki povezujejo podatke za preverjanje elektronskega podpisa z določeno osebo, imetnikom potrdila ter potrjujejo njeno identiteto) ali opravljajo druge storitve v zvezi z overjanjem ali elektronskimi podpisi.

Obstajata dve vrsti digitalnih potrdil oziroma certifikatov in sicer kvalificirana in nekvalificirana digitalna potrdila. Nekvalificirana potrdila se uporabljajo, ko se stranke med seboj tako dogovorijo in poslujejo po že utečenih poteh. Pri tej vrsti potrdil ne potrebujemo identifikacije za izdajo digitalnega potrdila. Je potrdilo v elektronski obliki, ki povezuje podatke za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto. Pri elektronskem poslovanju strank, ki še niso poslovale ena z drugo, pa je smiselno vključiti še tretjo osebo (slika 4.6), ki izdaja kvalificirana potrdila. Kvalificirana potrdila temeljijo na natančno predpisanem uradnem postopku identifikacije imetnika in izpolnjuje zahteve iz 28. člena Zakona o elektronskem poslovanju in elektronskem podpisu in ga izda overitelj, ki deluje v skladu z zahtevami iz 29. do 36. člena tega zakona. Identifikacijo izvajajo overitelji, ali v njihovem imenu pooblaščene prijavne službe.

Izdajatelj digitalnih potrdil mora najprej izdelati svoje lastno digitalno potrdilo, s katerim nato overja potrdila, ki jih izda.

Slika 4.6: Vzpostavitev zaupanja preko overitelja

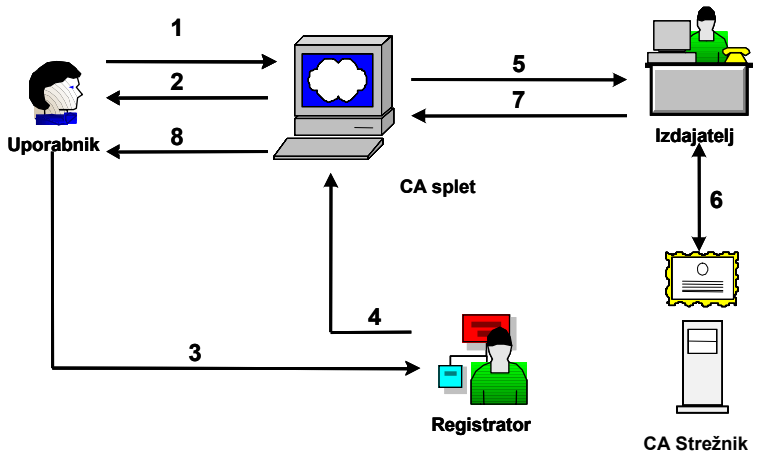
Vir: Žužek, 2000

Potrebni so naslednji koraki za pridobitev kvalificiranega digitalnega potrdila kot prikazuje slika 4.7 (Žmak, 2006):

1. Zahtevek
2. Seznam dokazil
3. Predložitev dokazil
4. Odobritev
5. Prevzem zahteve
6. Izdaja potrdila
7. Objava potrdila
8. Prevzem potrdila

Poleg izdaje potrdil mora overitelj skrbeti tudi za uničena in preklicana potrdila, zato se ob vsaki uporabi potrdila preverja, če je potrdilo še veljavno oziroma ali je na črni listi. Nekatera kvalificirana potrdila so namenjena uporabi več storitev in ne le izključno samo za eno vrsto elektronskega poslovanja (npr. digitalno potrdilo AC NLB lahko poleg elektronskega poslovanja preko Klika NLB uporabljamo tudi za elektronsko poslovanje z davčno upravo). Največja agencija v RS, ki izdaja kvalificirana digitalna potrdila, deluje v okviru Centra vlade v RS za informatiko (CVI). Izdaja tako kvalificirana digitalna potrdila za državljane in poslovne subjekte SIGEN-CA, kot tudi za upravo RS SIGOV-CA.

Slika 4.7: Pridobitev digitalnega potrdila



Vir: (Žmak, 2006)

V Sloveniji so najbolj poznani overitelji kvalificiranih digitalnih potrdil SIGEN-CA, SIGOV-CA, Halcom-CA, AC NLB, POŠTA®CA. Nekatere spletne elektronske banke omogočajo uporabo kvalificiranih digitalnih potrdil agencij SIGEN-CA in POŠTA®CA.

Overitelj mora vzdrževati tudi javni imenik, ki vsebuje naslednje informacije:

- javne informacije o imetnikih potrdil,
- veljavna potrdila, ki jih je izdal overitelj,
- veljaven register preklicanih potrdil.

5 Vzpostavitev IJK infrastrukture za varen dostop do zdravstvenih podatkov

Omrežna tehnologija ima najpomembnejšo vlogo pri dostopu in prenosu informacij za ponudnike zdravstvenih storitev. Še posebej omogoča dostop do podatkov in novih aplikacij, kot sta na primer elektronska zdravstvena kartoteka in elektronski recept, s pomočjo katerih lahko bistveno izboljšamo oskrbo bolnikov in komunikacijo z njimi. Za varno komunikacijo in izmenjavo podatkov pa je potrebno vzpostaviti IJK infrastrukturo.

Vzpostavitev infrastrukture javnih ključev je način zagotavljanja zanesljivosti glede naslednjih dejstev:

- da podpisnikov javni ključ ni bil spremenjen in dejansko ustreza podpisnikovemu zasebnemu ključu,
- da so uporabljene zanesljive, varne in ustrezne šifrirne tehnologije,
- da so različni sistemi šifriranja med seboj povezljivi ali združljivi.

V ta namen mora infrastruktura javnih ključev nuditi nabor različnih storitev, ki med drugim vključujejo:

- upravljanje s šifrirnimi ključi za digitalne podpise,
- potrjevanje, da javni ključ ustreza zasebnemu ključu,
- zagotavljanje šifrirnih ključev končnim uporabnikom,
- upravljanje s pooblastili in vlogami uporabnikov,
- objavljanje zanesljivega in varnega imenika javnih ključev ali potrdil,
- uporabo varnih medijev za shranjevanje zasebnih ključev (npr. pametnih kartic),
- preverjanje identitete končnih uporabnikov in zagotavljanje storitev tem uporabnikom,
- zagotavljanje storitev dokazovanja lastnosti sistema in veljavnosti digitalnih podpisov,
- zagotavljanje storitev časovnega žigosanja ali drugega podobnega potrjevanja podatkov v določenem trenutku,
- druge storitve, povezane s šifrirnimi ključi.

Infrastruktura javnih ključev je pogosto zasnovana na različnih hierarhičnih organizacijskih modelih. Prvi model vključuje vrhovnega overitelja, ki potrjuje tehnologijo in postopke vseh oseb, ki uporabljajo šifrirne ključe ali potrdila v povezavi s šifrirnimi ključi, in ki registrira podrejene overitelje. Drugi model pa je zasnovan kot medsebojno, vodoravno povezovanje enakopravnih overiteljev. Ti zagotovijo, da uporabniki enega od medsebojno priznanih overiteljev lahko zaupajo tudi potrdilom, ki jih je izdal drug overitelj. Oba modela imata svoje prednosti in slabosti zato pričakujemo, da se bo znotraj ene države razvilo več različnih infrastruktur javnih ključev, ki bodo zasnovane na navpičnem hierarhičnem modelu, medsebojno pa se bodo povezale v skladu z modelom vodoravnega medsebojnega povezovanja.

Kadarkoli aplikacija preverja digitalno potrdilo, mora preveriti (CVI, 2003):

- veljavnost digitalnega potrdila,
- veljavnost podpisnega zasebnega ključa (ang. PrivateKeyUsagePeriod),
- ustrezen register preklicanih potrdil (CRL),
- izdajatelja (izdajateljevo potrdilo),
- uporabo potrdila, politiko overitelja, varnostno politiko e-podpisa.

5.1 Zaprto zdravstveno omrežje ali vzpostavitev neposrednega dostopa do podatkov preko javnega internetnega omrežja

Za vzpostavitev IJK infrastrukture in s tem varnega dostopa do podatkov na Zavodu, sta možni dve rešitvi; zaprto zdravstveno omrežje ali uporaba javnega internetnega omrežja za neposredni dostop do podatkov na Zavodu.

Še nekaj let nazaj je moral Zavod drago plačevati zakupljene vode, sedaj pa je sedež Zavoda v Ljubljani povezan s svojimi območnimi enotami in izpostavami preko javnega internetnega omrežja, kjer je z uporabo navideznega zasebnega omrežja na osnovi MPLS (Multiprotocol Label Switching) tehnologije zagotovljena varna komunikacija. Ponudnik skrbi za upravljanje v tem omrežju, zato ni potrebna postavitev in upravljanje omrežja s strani Zavoda. Zaščita in šifriranje podatkov se izvede že na strani Zavoda, saj IP-MPLS VPN ne šifrira podatkov tako kot IPSec VPN.

Izvajalcem zdravstvenih storitev bo omogočen dostop do podatkov na Zavodu preko spletnega zdravstvenega portala z uporabo kvalificiranih digitalnih potrdil. Kvalificirano digitalno potrdilo mora biti shranjeno tudi na strežniku, saj s tem zagotovimo, da uporabniki lahko preverijo, če se prijavijo na pravi strežnik. Poleg tega z uporabo digitalnega potrdila šifriramo povezavo med brskalnikom in strežnikom po protokolu SSL.

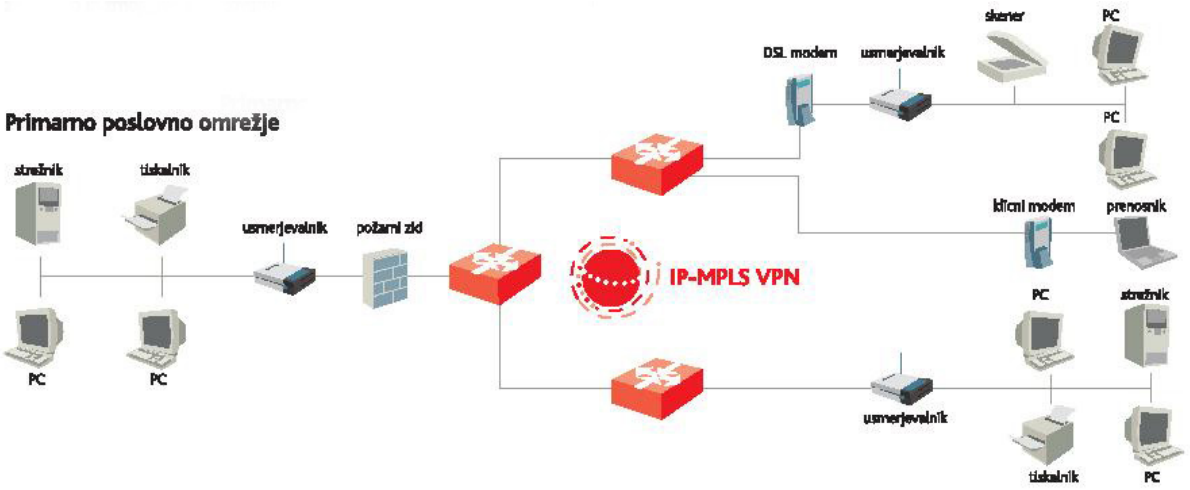
Za dostop do podatkov na Zavodu preko javnega internetnega omrežja obstaja več možnosti:

- uporaba javnega internetnega omrežja in storitve IP-MPLS VPN,
- uporaba javnega internetnega omrežja in storitve IPSec VPN
- uporaba javnega internetnega omrežja in protokola SSL.

Uporaba javnega internetnega omrežja in storitve IP-MPLS VPN

Storitev IP-MPLS omogoča zanesljivo in varno povezovanje razpršenih lokacij, kot je prikazano na sliki 5.1. Temelji na protokolu MPLS. Gre za simulacijo zasebnega širokopasovnega omrežja WAN preko javnega IP omrežja. Naročnik za izgradnjo takega omrežja ne potrebuje posebnih naprav. Za postavitev in vzdrževanje poskrbi ponudnik storitve. Vključevanje novih lokacij za naročnika predstavlja minimalen poseg.

Slika 5.1: Varen prenos podatkov preko javnega internetnega omrežja z uporabo storitve MPLS VPN



Vir: Telekom, 2006

Promet v omrežju, kjer se uporablja IP-MPLS VPN ni šifriran kar pomeni, da mora za šifriranje prometa poskrbeti naročnik sam.

Storitev je namenjena za večja podjetja, ki potrebujejo zanesljivo in zmogljivo povezovanje.

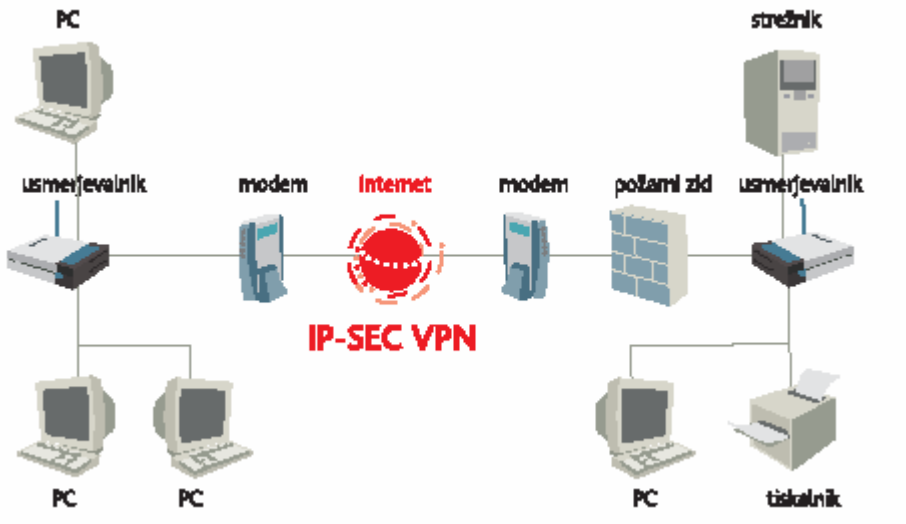
Uporaba javnega internetnega omrežja in storitve IPSec VPN

V primeru uporabe IPSec VPN tehnologije je naročnikov promet šifriran z uporabo IPSec protokola, ki zagotavlja varen prenos (glej sliko 5.2). Promet se najprej šifrira in nato uokviri ter pošlje v javno omrežje skozi vzpostavljen tunel. Šifriranje je lahko izvedeno s strojno ali programsko opremo. Na drugi strani omrežja se promet v robni napravi ponudnika razokviri in dešifrira. Slabost te tehnologije je, da ponudnik storitve ne more zagotoviti zahtevane pasovne širine, medtem ko je z uporabo MPLS tehnologije to mogoče.

Naročnikova robna naprava komunicira z robno napravo ponudnika. Naročnik mora nastaviti osnovni usmerjevalni protokol na robni napravi naročnika, ponudnik storitve pa napravi vse ostalo. Naročnik mora tako zagotoviti le pasovno širino lokacije do točke ponudnika, ne pa tudi za vsako zvezo med končnima lokacijama posebej.

Storitev je primerna za manjša podjetja z nekaj lokacijami, ko ni potrebna velika pasovna širina.

Slika 5.2: Varen prenos podatkov preko javnega internetnega omrežja z uporabo IPSec tehnologije



Vir: Telekom, 2006

Uporaba javnega internetnega omrežja in protokola SSL

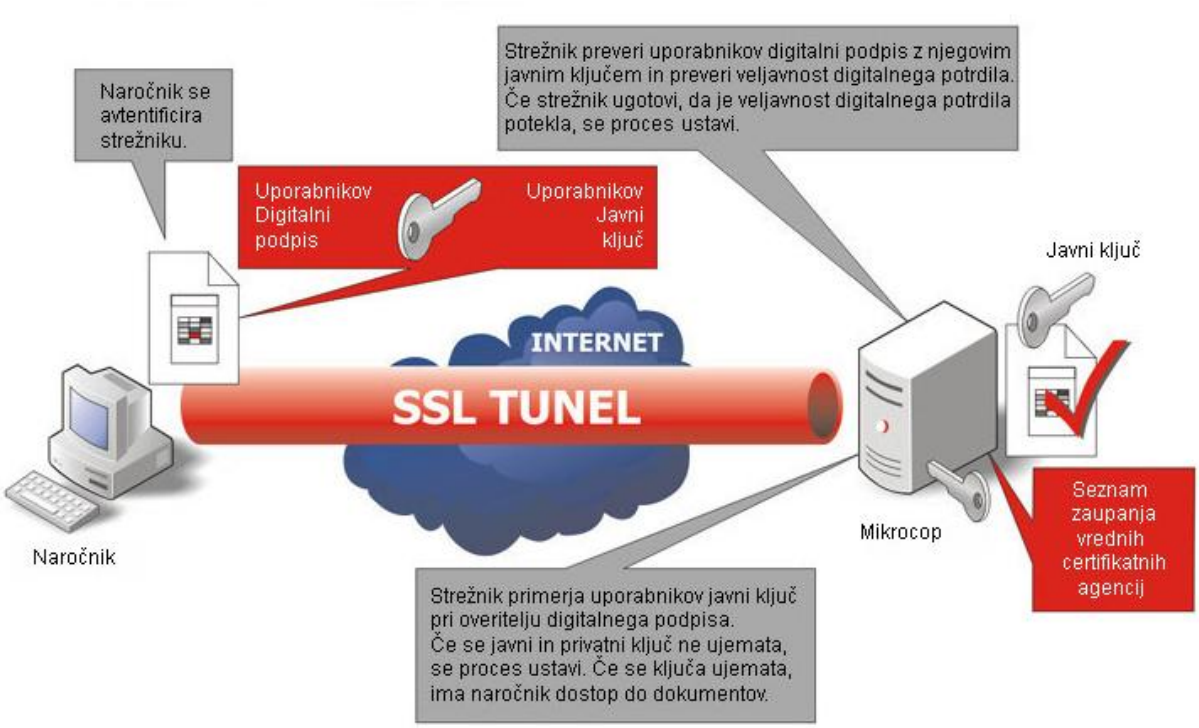
SSL je protokol, ki omogoča šifrirano povezavo med strežnikom in odjemalcem. SSL protokol pa ne omogoča le šifriranje podatkov, kar je za varno komunikacijo premalo, pač pa omogoča tudi preverjanje, da podatki niso bili spremenjeni in overjanje pošiljatelja in prejemnika sporočila. Trenutno je v uporabi SSL protokol verzije 3. Naslednik SSL protokola je protokol TLS.

SSL omogoča tudi overjanje uporabnikov preko digitalnih potrdil, ki jih hranimo na pametni kartici ali vključimo v brskalnike. Odjemalec in strežnik se morata medsebojno overiti in se dogovoriti za algoritme in ključe, s katerimi bo potekala šifrirana izmenjava podatkov med njima. Odvisno od vsebine potrdila potem strežnik dovoli priključitev ali pa prekine povezavo.

Glede na to, da za vpogled do določenih podatkov na Zavodu ne bo potrebna velika pasovna širina, je najbolj verjetna in cenovno najugodnejša rešitev vzpostavitev neposrednega dostopa do podatkov na Zavodu z uporabo kvalificiranih digitalnih potrdil in SSL/TLS protokola.

SSL/TLS protokol lahko uporabljamo v katerikoli aplikaciji, ker deluje na transportni plasti. Na sliki 5.1 je prikazana varna izmenjava podatkov po protokolu SSL/TLS.

Slika 5.3: Varna izmenjava podatkov po SSL/TLS protokolu



Vir: http://www.arhiviraj.si/varnost.php, 2006

V kasnejšem obdobju, če bo prišlo do povezovanja različnih izvajalcev (npr.bolnišnic), bo potrebno zagotoviti tudi večjo pasovno širino z uporabo IP-MPLS VPN.

Stroški, povezani z vzpostavitvijo takega načina komunikacije z izvajalci zdravstvenih storitev, bi bili v primerjavi z zasebnim zdravstvenim omrežjem bistveno nižji, saj ni potrebno plačevati najetih povezav.

V nadaljevanju naloge se bom osredotočil na vzpostavljanje povezave med Zavodom in izvajalci zdravstvenih storitev z uporabo javnega internetnega omrežja.

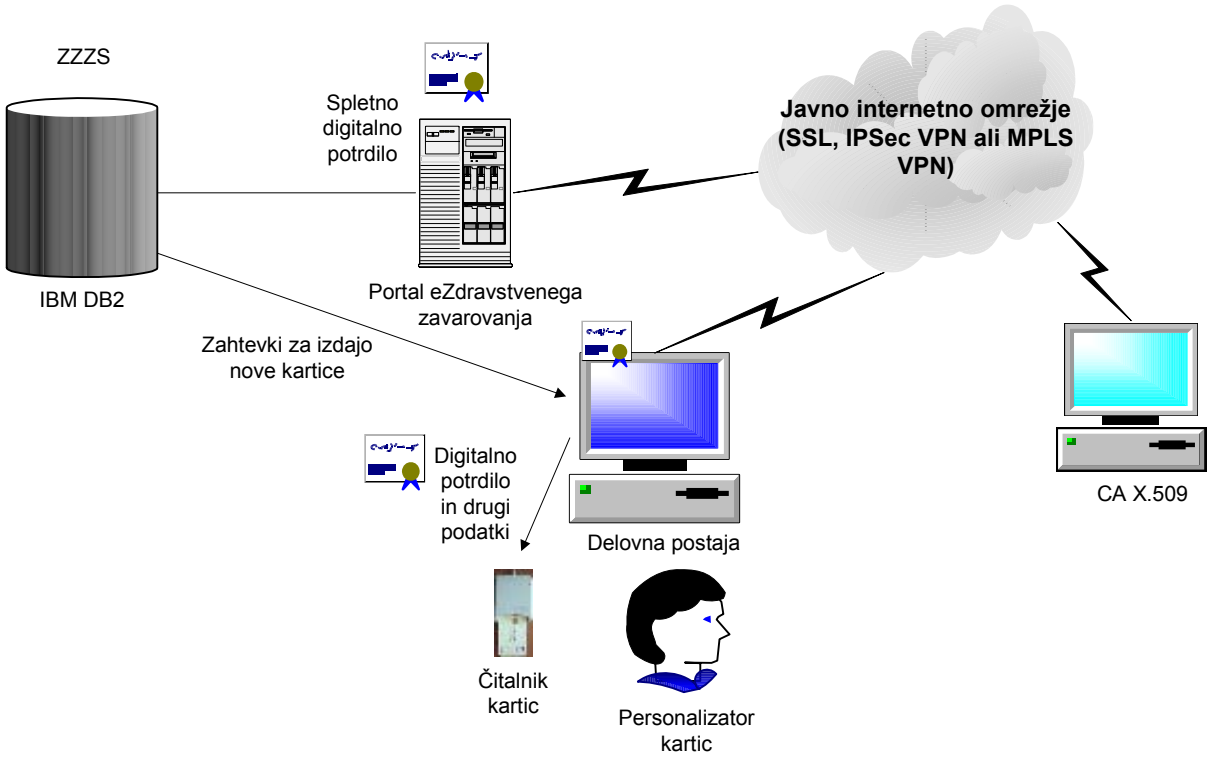
5.2 Prenova procesov (To be) v zvezi s personalizacijo kartic

Zahtevke za izdajo nove KZZ ali PK bodo referenti na Zavodu preko aplikacije vnašali v centralno bazo podatkov. Personalizator kartic bo glede na pogodbo enkrat tedensko (ali večkrat odvisno od dogovora) dostopal do baze podatkov na Zavodu in pridobil zahtevke za izdajo KZZ ali PK. Z Zavodom bo povezan preko javnega internetnega omrežja (uporaba SSL ali VPN povezave). Slika 5.1 prikazuje grafični

prikaz vzpostavitve povezave med Zavodom in personalizatorjem kartic in s tem možnost izvajanja personalizacije kartic.

Če bo Zavod k prenovi IS KZZ pristopil postopoma, kar pomeni, da bomo najprej zamenjali KZZ in PK, ki bodo nadomestile vse sedanje kartice in bodo podpirale vse funkcionalnosti sedanjih kartic, bo Zavod moral prav tako pripravljati pakete za personalizacijo z vsemi obstoječimi podatki, ki se zapišejo na KZZ in PK. Kasneje z vzpostavitvijo neposrednega dostopa do podatkov za izvajalce zdravstvenih storitev, se bo obseg podatkov za personalizacijo zmanjšal in bo na koncu potrebno prenašati le nekaj podatkov potrebnih za identifikacijo osebe, saj bodo vsi ostali podatki dostopni neposredno iz baze podatkov Zavoda in drugih prostovoljnih zavarovalnic.

Slika 5.4: Grafični prikaz personalizacije kartic KZZ in PK v prenovljenem procesu (To Be)



Vir: Lasten

5.3 Pametne kartice in digitalno potrdilo

Stopnja varnosti digitalnega podpisovanje je odvisna od nosilca, na katerem imetnik digitalnega potrdila hrani svoj zasebni ključ. Trenutno največjo varnost predstavljajo pametne kartice, katerih glavna prednost je ta, da zasebni ključ nikoli ne zapusti kartice, saj šifriranje in digitalno podpisovanje potekata na sami kartici. Na pametno kartico lahko shranimo več digitalnih potrdil za uporabo različnih storitev.

Prednost uporabe digitalnih potrdil na pametni kartici pred uporabo digitalnih potrdil na osebnem računalniku, je torej v varnosti digitalnega potrdila. Za uporabo več digitalnih potrdil na kartici, je potrebno zagotoviti takšne pametne kartice, na katere bo možno zapisati več digitalnih potrdil in več aplikacij. Poleg tega bo potrebno zagotoviti bralnike kartic, s katerimi bo mogoče namestiti digitalno potrdilo na kartici.

Aplikacije na kartici se morajo med seboj izključevati, kar pomeni, da so med seboj neodvisne.

V kolikor bo na kartico mogoče shraniti več digitalnih potrdil, bo potrebno zagotoviti bralnike pametnih kartic, ki bodo podpirali branje in zapis na pametno kartico tudi za imetnike pametnih kartic KZZ. Ob prvem shranjevanju digitalnega potrdila na pametno kartico, bo programska oprema morala omogočati tudi izdelavo varnostne kopije digitalnega potrdila, saj vsi imetniki kartice ne bodo imeli doma bralnikov kartic, ampak bodo za hranjenje digitalnega potrdila uporabljali osebni računalnik. Torej bo potrebno zagotoviti kopije digitalnih potrdil, da jih bodo uporabniki lahko namestili na osebni računalnik. Poleg tega bo kopija digitalnega potrdila potrebna, če bo imetnik kartico izgubil. V tem primeru bo na kartico potrebno shraniti varnostno kopijo digitalnega potrdila.

Menim, da je v danem trenutku najboljši izbor agencija, ki izdaja digitalna potrdila na Ministrstvu za javno upravo SIGEN-CA.

Za pridobitev kvalificiranega spletnega digitalnega potrdila je potrebno upoštevati politiko in pravila agencije, ki izdaja kvalificirana digitalna potrdila. Kvalificirana digitalna potrdila se pridobijo na podlagi zahtevka, ki ga mora podpisati bodoči imetnik (Overitelj na MJU, 2006).

Glede na izbor izdajatelja digitalnih potrdil bo potrebno namestiti tudi programsko opremo, ki uporabniku omogoča uporabo bralnikov pametnih kartic in digitalnega potrdila na pametni kartici. Prenos namestitvenega programa in namestitev programske opreme je običajno omogočena tudi preko spleta.

5.4 Izdajatelj digitalnih potrdil in personaliziranih kartic

Zelo pomembna je izbira overitelja digitalnih potrdil. To je lahko eden izmed uveljavljenih overiteljev v Sloveniji (npr. SIGEN-CA), ali pa ustanovimo novo agencijo za izdajo digitalnih potrdil za lastne potrebe. Pri tem se je potrebno vprašati, ali je smotrno ustanavljati lasten center za izdelavo in izdajo kvalificiranih digitalnih potrdil.

Za opravljanje svoje dejavnosti overitelj ne potrebuje posebnega dovoljenja. Mora pa najmanj osem dni pred pričetkom opravljanja svoje dejavnosti le-to prijaviti ministrstvu, pristojnemu za informacijsko družbo.

Predenj Agencija za telekomunikacije podeli dovoljenje za opravljanje dejavnosti akreditiranih overiteljev, je potrebno izpolnjevati naslednje zahteve glede prostora in opreme (Overitelj elektronskega podpisa, 2004):

- Overiteljevi prostori in infrastruktura morajo biti v skladu s pravili stroke, ustrezno elektronsko in fizično varovani pred nepooblaščenimi vdori.
- Zagotovljena mora biti uporaba zanesljivih sistemov in opreme, ki so zaščiteni pred spreminjanjem in zagotavljajo tehnično in kriptografsko varnost postopkov, v katerih se uporabljajo.
- Informacijsko telekomunikacijska infrastruktura, ki je povezana v drugo informacijsko telekomunikacijsko omrežje, mora biti varovana z zanesljivimi varnostnimi mehanizmi (sistem za preprečevanje in odkrivanje vdorov, požarna pregrada in podobno), ki preprečujejo nedovoljene dostope prek tega omrežja in omejujejo dostop samo po protokolih, ki so nujno potrebni za upravljanje s kvalificiranimi potrdili, vsi drugi protokoli pa morajo biti onemogočeni.
- Programska oprema mora ustrezati svetovno uveljavljenim varnostnim in tehničnim standardom (FIPS 140-1 za kriptografske module, priporočljivo EAL5 oziroma najmanj EAL3 skupnih meril - Common Criteria /ISO 15408/, priporočila izvedenske skupine Evropske iniciative za standardizacijo elektronskih podpisov - EESSI in drugo).
- Programska oprema, ki generira podatke za elektronsko podpisovanje, mora zagotavljati najmanjšo možnost poneverbe teh podatkov z uporabo trenutno razpoložljivih tehnologij.
- Šteje se, da strojna in programska oprema ter postopki izpolnjujejo predpisana merila in pogoje, če so v skladu s standardi, merili ali pogoji, ki so splošno priznani v Evropski uniji in objavljeni v Uradnem listu Evropskih skupnosti.
- Informacijski sistem overitelja za upravljanje kvalificiranih potrdil mora biti sestavljen zgolj iz strojne in programske opreme, ki je potrebna za upravljanje kvalificiranih potrdil.

Poleg tega mora imeti overitelj zaposlene osebe s primerno strokovno izobrazbo, ki morajo imeti posebna strokovna znanja glede upravljanja in poznavanja tehnologije, varnostnih postopkov in pravnih zahtev s področja elektronskega poslovanja in delovanja overiteljev, pridobljena na strokovnih usposabljanjih.

Overitelj mora spoštovati tudi ostala določila zakonodaje s tega področja (Overitelj elektronskega podpisa, 2004):

- Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 57/00, 30/01 – ZODPM-C, 25/04),
- Uredba o pogojih za elektronsko poslovanje in elektronsko podpisovanje (Uradni list RS, št. 77/00, 2/01),
- Pravilnik o prijavi overiteljev in vodenju registra overiteljev v Republiki Slovenije (Uradni list RS, št. 99/01).

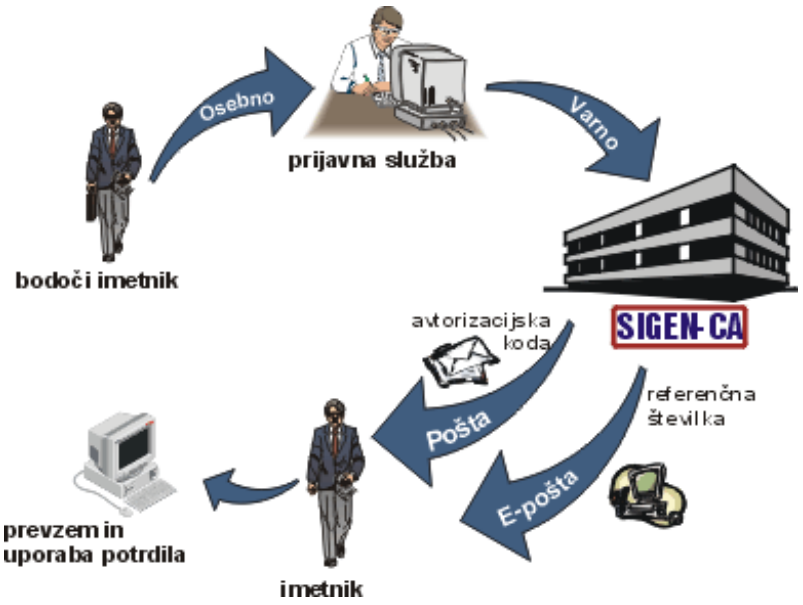
Na podlagi tega lahko sklepamo, da bi bilo ustanavljanje svoje agencije za izdajo digitalnih potrdil za potrebe zdravstvenega zavarovana dolgotrajen in drag proces, ki bi prinesel tudi veliko nepotrebnih finančnih stroškov. Poleg tega bi morali zaposliti nove sodelavce, s potrebno strokovno izobrazbo in potrebnim strokovnim znanjem iz tega področja.

Druga možnost je, da bi lahko digitalna potrdila za potrebe zapisovanje le teh na novo KZZ in PK izdajal personalizator kartic. Trenutno KZZ personalizira podjetje Cetis d.d., ki ne izdaja digitalnih potrdil, kar bi zopet pomenilo ustanavljanje nove agencije za overovljanje digitalnih potrdil v okviru personalizatorja in s tem povezanih stroškov.

Na podlagi teh dejstev se kot najbolj smiselna rešitev kaže sklenitev pogodbe z eno od agencij, ki že izdajajo kvalificirana digitalna potrdila, oziroma z overiteljem digitalnih potrdil na Ministrstvu za javno upravo, ki izdaja SIGEN-CA digitalna potrdila za fizične osebe in poslovne subjekte.

V kolikor želimo, na vse PK shraniti kvalificirano digitalno potrdilo SIGEN-CA za fizične osebe, je potrebno zagotoviti registracijo vseh zdravstvenih delavcev, ki uporabljajo in bodo tudi v prihodnje uporabljali PK. To pa pomeni, da bo moral vsak zdravstveni delavec izpolniti zahtevek za pridobitev digitalnega potrdila SIGEN-CA, ki ga bo s pomočjo aplikacije, nato pa po standardnem postopku shranil na PK (slika 5.2). Ob izdaji digitalnih potrdil SIGEN-CA, bo moral vsak posameznik poskrbeti za prevzem digitalnega potrdila in izdelavo varnostne kopije digitalnega potrdila, ki ga lahko kasneje shranimo na drugo kartico, kar pa bo predstavljalo veliko težavo, saj mnogi zdravstveni delavci niso navajeni dela z računalnikom, kaj šele sodobnih postopkov, kot je prevzem digitalnega potrdila in varno ravnanje z digitalnim potrdilom. Poleg tega se bo pojavil problem z gesli (zasebnimi ključi), ki jih bodo uporabniki pozabili.

Slika 5.5: Postopek pridobitve spletnega digitalnega potrdila pri agenciji SIGEN-CA za fizične osebe



Vir: MJU, 2006

Druga možnost je naročilo digitalnega potrdila za poslovne subjekte SIGEN-CA. V tem primeru lahko digitalna potrdila naroči pooblaščena oseba posameznega izvajalca (slika 5.3). Odgovorna oseba organizacije, kjer je bodoči imetnik potrdila zaposlen, jamči za identiteto bodočega imetnika potrdila, ki jo je preverila v skladu z 31. členom in drugimi določili ZEPEP. Pooblaščena oseba prejme tudi Pogodbo o upravljanju s kvalificiranimi potrdili SIGEN-CA za poslovne subjekte (MJU, 2006).

Prevzem in shranitev teh digitalnih potrdil bo lahko izvajala pooblaščena oseba pri izvajalcu, ali pa kakšna druga oseba v okviru personalizatorja, če bo tako dogovorjeno. Menim, da bi bilo najbolje, če bi personalizator poslal kartico njegovemu imetniku, na kateri bi bilo že shranjeno digitalno potrdilo. Pooblaščena oseba bo morala poskrbeti tudi za varno hranitev kopije digitalnih potrdil in sicer v primeru zamenjave pametne kartice ter za podaljšanje veljavnosti digitalnih potrdil. Pooblaščena oseba bo odgovorna tudi za preklic neveljavnih digitalnih potrdil.

Slika 5.6: Postopek pridobitve spletnega digitalnega potrdila pri agenciji SIGEN-CA za poslovne subjekte

Vir: MJU, 2006

5.5 Bralniki pametnih kartic, pametne kartice in digitalna potrdila

Za delo in upravljanje s pametno kartico je potrebno razviti program. Med drugim mora omogočati inicializiranje novih kartic, spreminjanje PIN-a (ob poznavanju trenutno veljavnega), registracijo digitalnega potrdila na kartici, odklepanje zaklenjenih kartic s pomočjo rešilnega niza, pregled podatkov o kartici in trenutno nameščenih komponent, pregled digitalnih potrdil na kartici, uvoz digitalnega potrdila iz datoteke na kartico, brisanje digitalnega potrdila iz kartice ipd.

Bralniki morajo ustrezati specifikaciji PC/SC. Za novejše računalnike je možno uporabiti bralnike pametnih kartic, ki imajo USB (Universal Serial Bus) priključek. Za dostop do svojih podatkov v sistemu, bodo zavarovane osebe uporabljale preproste bralnike.

Obstaja tudi možnost uporabe trenutno uporabljenih bralnikov kartic. To bi bilo aktualno predvsem, če bi nove PK in KZZ delovale kot sedanje PK in KZZ in bi hkrati simulirale tudi delovanje sedanjih PK in KZZ. Nove PK za izvajalce zdravstvenih storitev bi tako omogočale branje sedanjih in novih KZZ, vsebovale pa bi tudi kvalificirano digitalno potrdilo.

Druga možnost je, da se za uporabo novih PK in novih KZZ zagotovi uporaba novih bralnikov in da bi izvajalci zdravstvenih storitev v prehodnem obdobju uporabljali dva bralnika.

Za branje pametnih kartic enega proizvajalca lahko uporabljamo bralnike več proizvajalcev. Na ta način lahko izberemo najbolj primerne bralnike za določeno vrsto uporabnikov in namen uporabe. Glede na možnost izbire različnih bralnikov kartic imamo možnost, vplivati tudi na ceno bralnikov.

Kvalificirana digitalna potrdila na pametni kartici lahko uporabljajo en par ključev ali dva para ključev. Digitalna potrdila z enim parom ključev imenujemo tudi standardna potrdila in se uporablja tako za podpisovanje, kot za kriptiranje. Digitalna potrdila z dvema paroma ključev pa imenujemo tudi napredna potrdila. En par ključev je namenjen digitalnemu podpisu, drugi par ključev pa je namenjen kriptiranju. Zasebni ključ za podpisovanje je shranjen samo pri uporabniku, zasebni ključ za šifriranje pa je shranjen pri uporabniku in v bazi overitelja. Prednost tega mehanizma je predvsem v tem, da lahko uporabnik za dokumente, ki so bili zašifrirani za njega, od overitelja zahteva svoj zasebni ključ in prebere svoje dokumente, če iz kakršnega koli razloga izgubi svoj zasebni ključ.

5.6 Fizično varovanje in varovanje zasebnega ključa digitalnega potrdila

S postopki in ukrepi fizičnega varovanja se zagotavlja varovanje objektov in varnostnih območij za varovanje tajnih podatkov s ciljem, da se prepreči dostop do objekta ali varnostnega območja nepooblaščenim osebam. Ukrepi se izvajajo s posebej izdelanimi postopki, in sicer:

Ukrepi fizičnega varovanja so tisti postopki in ukrepi, kjer varnostniki na vstopih in izstopih izvajajo neposredno kontrolo oseb, vozil, itd. Naloge varnostnikov na posameznih točkah, kjer izvajajo varovanje, morajo biti natančno opredeljene. Varnostniki lahko opravljajo varovanje na sledeče načine:

- z neposrednim fizičnim varovanjem (na točki - določenem delovnem mestu),
- varovanje v kontrolni sobi (spremlja dogajanje v okolici objekta ali v objektu s pomočjo video nadzornih kamer, ki so vezane v kontrolno sobo, sprejema pozive alarmnih sistemov in alarmira pristojne),
- z načrtom obhodov objekta ali prostorov in
- z intervencijskim posredovanjem ob sprožitvi alarma ali klica na pomoč (blokadna mesta, itd.).

Varovanje zasebnega ključa digitalnega potrdila je zagotovljeno že s shranjevanjem digitalnega potrdila na pametni kartici. Razen pri naprednih digitalnih potrdilih (dva zasebna ključa) je zasebni ključ za šifriranje shranjen tudi pri overitelju. Varnost je

veliko večja, kot če imamo digitalno potrdilo shranjeno na trdem disku našega računalnika, do katerega je mnogo lažje dostopati.

Overitelj mora zagotoviti fizično varovanje strojne opreme in varovanje nepooblaščenega dostopa do podatkov.

Informacijska varnost obsega določanje in uporabo ukrepov za zaščito tajnih podatkov, ki se obdelujejo, shranjujejo in prenašajo s pomočjo komunikacijskih, informacijskih in drugih elektronskih sistemov pred naključno ali namerno izgubo tajnosti, celovitosti ali razpoložljivosti in ukrepov za preprečevanje izgube celovitosti in razpoložljivosti samih sistemov.

5.7 Zagotavljanje kakovosti podatkov in kontrola podatkov

Zagotavljati je potrebno nadzor nad kakovostjo strojne in programske opreme, ki se vključuje v takšno omrežje, da ne povzroča nezaželenega prometa v omrežju in da ne povzroča okužb z računalniškimi virusi, s čimer dosežemo tudi kakovost in kontrolo podatkov. Z vzpostavitvijo zaprtega zdravstvenega omrežja ali navideznega zasebnega omrežja bi se varnost in s tem kakovost podatkov močno povečala.

Zavod si že nekaj let prizadeva za kakovostne podatke in v zvezi s tem izvaja tudi kontrolo podatkov, ki nam jih preko RIP pošiljajo izvajalci zdravstvenih storitev. Zavod ima tudi že vzpostavljeno centralno DB2 bazo podatkov, v kateri je poskrbljeno za kakovostne in urejene podatke.

Večji problem predstavlja dodeljevanje profesionalnih kartic izvajalcem zdravstvenih storitev. V sedanjem sistemu se PK izdaja na podlagi pisnega obrazca, za katerega je odgovorno vodstvo izvajalcev zdravstvenih storitev. Veliko problemov se pojavlja tudi s preklicem, oziroma odjavo zdravstvenega delavca, v primeru zamenjave službe, upokojitve ali prenehanja delovnega razmerja zdravstvenega delavca. Izvajalci zdravstvenih storitev bi morali v teh primerih preklicati PK za zdravstvenega delavca, ker pa se to pogosto ne zgodi, zdravstveni delavec uporablja pridobljeno PK pri drugem izvajalcu, kar je v nasprotju s Pravilnikom o kartici zdravstvenega zavarovanja.

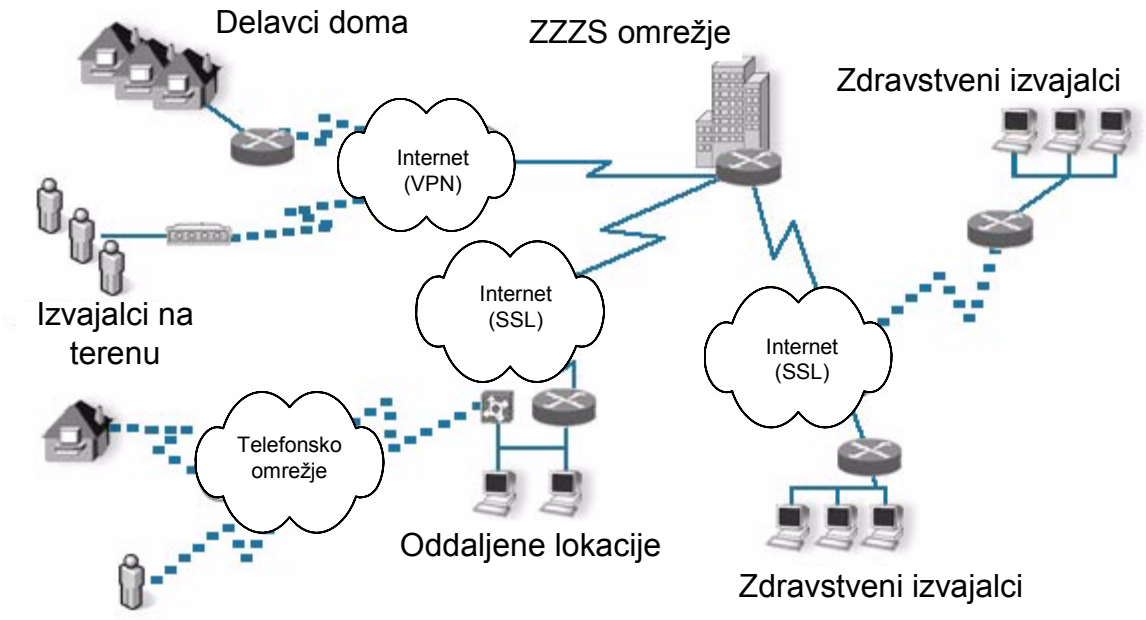
V prenovljenem sistemu KZZ bi bilo nujno vspostaviti register uporabnikov in njihovih pooblastil, kar pomeni izboljšanje sedanje Baze podatkov o izvajalcih, ki jo vodi IVZ. S pridobitvijo kvalificiranega digitalnega potrdila bomo tako pridobili točen seznam vseh uporabnikov profesionalnih kartic.

Kontrola dostopa do podatkov na centralnem računalniku Zavoda bi bila zagotovljena z dodeljevanjem pooblastil zdravstvenim delavcem, kot imamo to urejeno že sedaj s profesionalnimi karticami. Določena skupina zdravstvenih izvajalcev npr. zdravniki, lahko dostopajo samo do določenih datotek na KZZ.

6 Prednosti, ki jih dobimo s prenovo IS KZZ

Kartice zdravstvenega zavarovanja v novem sistemu ne bi bile več nosilec zdravstveno zavarovalniških in zdravstvenih podatkov, ampak bi bile namenjene le za identifikacijo in kot ključ za varen dostop do podatkov o zavarovani osebi. Nove kartice zdravstvenega zavarovanja naj bi se uporabljale za identifikacijo, preverjanje istovetnosti zavarovane osebe in za zagotavljanje varnih komunikacij v omrežju. Nove profesionalne kartice, ki v sedanjem sistemu predstavljajo ključ za dostop do podatkov na KZZ, naj bi bile v novem sistemu zelo podobne novim karticam zdravstvenega zavarovanja in naj bi se uporabljale za identifikacijo, preverjanje istovetnosti zdravstvenega delavca in zagotavljanje varnih komunikacij. Izvajalci zdravstvenih storitev bodo lahko neposredno preko javnega internetnega omrežja dostopali do baze podatkov na Zavodu in PZZ (slika 6.1).

Slika 6.1: Uporaba javnega internetnega omrežja za dostop do podatkov na Zavodu



Vir: Povzeto po Telprom (http://www.telprom.si/vpn.htm), 2006

S prenovo IS KZZ bi pridobili naslednje koristi:

- poenostavljen postopek personalizacije KZZ in PK,
- neodvisnost od proizvajalca kartic in lažji vnos sprememb,
- večja varnost podatkov,
- informatizacija celotnega zdravstva,
- izvajalci zdravstvenih storitev bi lahko neposredno preko zdravstvenega omrežja ali VPN dostopali do zdravstvenih podatkov oseb, ki se trenutno nahajajo na KZZ:
    - podatki o zdravstvenih zavarovanjih in osebni podatki,
    - podatki o izbranih osebnih zdravnikih,
    - podatki o medicinsko tehničnih pripomočkih,
    - podatki o izdanih zdravilih,
    - podatki o darovalcih,
    - podatki o alergijah in preobčutljivostih na zdravila,
- odprava rizika dolge veljavnosti zavarovanja na KZZ,
- manjši stroški povezani z IS KZZ,
- PKI infrastruktura in novejša platforma za prenosne čitalnike.

Z uporabo IJK, pametnih kartic in digitalnih potrdil omogočimo najvišjo stopnjo varnosti zdravstvenih podatkov in nedvoumno ugotavljanje istovetnosti vseh sodelujočih v storitvi, nadzor nad dostopom, zaupnost, celovitost ter podporo za nezatajljivost.

Uvajanje novega sistema zahteva spremembe v poslovnem procesu, obstoječih informacijskih rešitvah ter precejšnja vlaganja v komunikacijsko infrastrukturo in varnost podatkov, zaradi česar je, tudi zaradi visokih stroškov celovite prenove sistema KZZ smiselno razmišljati o postopni prenovi informacijskega sistema KZZ.

Z uvedbo IJK in shranjevanjem digitalnih potrdil na pametnih karticah zdravstvenih delavcev (PK) in zavarovanih oseb (KZZ), ustvarimo pogoje za varno neposredno dostopanje do podatkov.

Izvajalci zdravstvenih storitev bodo za preverjanje podatkov, ki se trenutno nahajajo na KZZ v novem sistemu, neposredno dostopali do podatkov, ki so shranjeni v centralni evidenci Zavoda. Poleg tega bodo izvajalci lahko pridobili tudi druge pomembne podatke, ki jih v sedanjem sistemu na KZZ ne moremo zapisati.

Določene podatke bo mogoče zapisati tudi na strežnike, do katerih bodo lahko dostopali le pooblaščeni izvajalci zdravstvenih storitev (npr. pri vzpostavitvi elektronskega recepta, bo zdravnik napisal elektronski recept, ki ga bo farmacevt v lekarni lahko pogledal na podlagi svoje PK in KZZ zavarovane osebe).

Lekarnam in izdajateljem medicinsko tehničnih pripomočkov ter tudi ostalim izvajalcem zdravstvenih storitev (npr. bolnišnice), bo omogočen vnos podatkov, ki jih na Zavod preko RIP-a pošiljajo že sedaj, neposredno v bazo podatkov na Zavodu. S tem bomo pridobili bolj ažurne podatke, ki bodo prispevali k večji kakovosti izvajanja zdravstvenih storitev in zmanjšanju stroškov za zdravstvo.

6.1 Koristi za izvajalce

6.1.1 Izbrani osebni zdravniki

Po prenovi celega sistema KZZ bo izvajalcem omogočeno neposredno posredovanje podatkov o izbranih osebnih zdravnikih. Obstaja možnost za razširitev nabora podatkov, ki bi bili izvajalcem na voljo, glede na sedanji nabor podatkov na KZZ.

- Pri zobozdravnikih in ginekologih bi lahko zagotovili priimek in ime zdravnika, ki ga sedaj ni na KZZ.
- Posredovali bi lahko tudi podatke o izvajalcu (naziv, naslov), pri katerem je oseba izbrala osebnega zdravnika.

Ker se izbire osebnih zdravnikov izvajajo pri izvajalcih, ki so pogodbeni partnerji Zavoda, Zavod razpolaga s podatki o nazivu in naslovu izvajalca. Za zagotovitev navedenih dodatnih podatkov zato niso potrebne dodatne pravne podlage.

Navedeni dodatni podatki bi bili pomembna pridobitev za izvajalce zdravstvenih storitev, saj bi olajšali komunikacijo med subjekti v zdravstvu (npr. pri pošiljanju odpustnega pisma iz bolnišnice, pri pošiljanju izvidov in rezultatov preiskav).

Če vzpostavimo rešitev za dostope izvajalcev do podatkov o izbranem osebnem zdravniku na centralnem računalniku Zavoda, je smiselno v okviru istega sistema izvajalcem tudi omogočiti vpis novih izbir. S tem bi odpadla potreba po računalniškem izmenjevanju teh podatkov med izvajalci in Zavodom. Izvajalci, ki do sedaj niso bili vključeni v RIP IOZ, so podatke o novih izbirah posredovali pisno. V novem sistemu takšnega pisnega posredovanja podatkov ne bi bilo več potrebno. S tem bi zagotovili tudi večjo kakovost in točnost podatkov.

6.1.2 Izdani medicinsko tehnični pripomočki

Na KZZ se lahko zapiše maksimalno 21 zapisov o izdanih MTP.

Dosedanjemu naboru podatkov o izdanih MTP na KZZ bo pri neposrednem dostopu do centrane baze podatkov Zavoda možno dodati še naziv in naslov dobavitelja medicinsko tehničnega pripomočka (podatek je v bazi podatkov Zavoda zanesljiv).

Ta podatek bi lahko koristil zdravniku za vzpostavitev komunikacije z dobaviteljem, kjer je to v postopku zdravljenja potrebno. Računalniška izmenjava podatkov ne bi bila več potrebna, zato bi dosegli večjo kakovost in točnost podatkov, ter manjše stroške.

6.1.3 Izdana zdravila

Na KZZ se zapisujejo le podatki o zdravilih, ki so bili izdani v breme OZZ. Zdravila, ki so jih lekarne izdale v breme zavarovane osebe ali posebnih paketov prostovoljnega zdravstvenega zavarovanja, se na KZZ ne beležijo.

Podatke na KZZ lahko berejo zdravniki in farmacevti. Zavarovana oseba lahko farmacevtu onemogoči branje (in posledično tudi pisanje) podatkov na kartici.

Trenutno se na KZZ lahko zapiše maksimalno 46 zapisov o izdanih zdravil. Zdravila zapisana na KZZ, ki so starejša od dveh let, se ob naslednjem potrjevanju KZZ na samopostrežnem terminalu zbrišejo iz kartice.

V prenovljenem sistemu KZZ bi lahko omogočili vpogled do širšega nabora izdanih zdravil. Lekarne bi lahko podatke o izdanih zdravilih oziroma podatke iz receptov zapisale neposredno v centrano bazo podatkov na Zavodu, s čimer računalniška izmenjava podatkov ne bi bila več potrebna, zato bi dosegli večjo kakovost in točnost podatkov. Poleg zdravil, izdanih na zeleni recept, bi imel zdravnik vpogled tudi v druga izdana zdravila v kolikor bi zavarovana oseba za prejem zdravil izdanih na beli recept, dopustila branje podatkov iz KZZ.

6.1.4 Podatki o darovalcih

Podatki o darovanju organov po smrti so izredno občutljivi osebni podatki, zato je bila pri postavitvi sistema namenjena velika pozornost zagotovitvi zanesljivega sistema varovanja podatkov pred nepooblaščenim dostopom.

Podatke o darovalcih iz KZZ lahko preberejo le posebej pooblaščene osebe v bolnišnicah, ki so usposobljene za posmrtni odvzem organov in tkiv za transplantacije.

Skladno z 20. členom Zakona o odvzemu in presaditvi delov človeškega telesa zaradi zdravljenja, (Ur. l. 12/2000), je vodenje predpisanih evidenc s tega področja ena izmed nalog organizacije Slovenija Transplant. Zdravniki, ki izvajajo transplantacijo organov, bi lahko v prenovljenem sistemu KZZ prišli do podatka

neposredno s pogledom v bazo podatkov na Zavodu. V kolikor pravnih podlag za neposreden dostop do podatkov o darovalcih ne bi spremenili, obstaja še vedno možnost zapisa podatkov na novo KZZ.

6.1.5 Podatki o prostovoljnih zdravstvenih zavarovanjih

Podatki o veljavnosti prostovoljnega zdravstvenega zavarovanja se ob potrjevanju KZZ na samopostrežnem terminalu zapiše na KZZ. Obvezno zdravstveno zavarovanje, kakor tudi prostovoljno zdravstveno zavarovanje velja tri mesece za odrasle osebe, ki imajo zavarovanje potrjeno na KZZ.

Pri neposrednem dostopu do podatkov na strežnikih prostovoljnih zdravstvenih zavarovalnic, bi lahko izvajalci dobili razširjen nabor podatkov o prostovoljnih zdravstvenih zavarovanjih osebe in bolj točne podatke o veljavnosti zavarovanja.

6.1.6 Podatki o težkih alergijskih reakcijah in preobčutljivostnih reakcijah po zdravilih

Zavod je v letih 2004 in 2005 pripravljal pilotno uvedbo zapisa podatkov o težkih alergijskih reakcijah na hrano, pike žuželk, lateks, idiopatična anafilaksija in drugo na KZZ. Pripravljal je tudi uvedbo zapisa podatkov o preobčutljivostnih reakcijah po zdravilih na KZZ.

Predvideno je bilo, da bodo podatke na KZZ zapisovali specialisti, ki ugotavljajo alergije in preobčutljivosti ter osebni zdravniki. Podatki naj bi bili dostopni zdravstvenemu osebju povsod, kjer so ti podatki koristni za zdravljenje. Zavod naj ne bi imel kopije teh podatkov v svojem informacijskem sistemu, ampak bi takšna kopija podatkov obstajala pri izbranem osebnem zdravniku.

S prenovo informacijskega sistema KZZ, bo tovrstne podatke mogoče zapisovati in shranjevati na strežniku. Dostop do podatkov bo mogoče z uporabo digitalnih potrdil omejiti le na zdravstveno osebje.

Informacijsko podporo za upravljanje s temi podatki bi bilo zato smiselno zagotoviti v okviru (vzpostavitve) elektronskega zdravstvenega kartona, kar je predvidoma naloga Ministrstva za zdravje v okviru uresničevanja strategije eZdravje.

6.1.7 Elektronski recept

Elektronski recept bo mogoče zagotoviti skupaj z evidentiranjem izdanih zdravil (v tem primeru lekarna k podatkom o predpisovanju zdravila doda le podatke o izdaji zdravila na posameznem receptu). Z oblikovanjem enotnega sistema za elektronski recept in evidentiranje izdaj in če bi bili podatki na Zavodovem centralnem računalniku, bi lahko prišlo do očitkov o koncentraciji zdravstvenih podatkov, kar prinaša možnosti zlorab, če podatki niso pravilno zaščiteni. Glede na to, da že več desetletij Zavod in IVZ zbirata podatke o izdajah zdravil (avtomatska obdelava receptov AOR), se smatra, da javnost zaupa varno vodenje teh podatkov Zavodu.

6.1.8 Elektronski zdravstveni karton

V prenovljenem informacijskem sistemu bi bili dani pogoji za vzpostavitev elektronskega zdravstvenega kartona. Podatki bi bili dostopni na internetu na posebnem strežniku-ih zdravstvenemu osebju in bi lahko bistveno prispevali k povečanju kakovosti zdravstvenih storitev in obravnavi zavarovanih oseb.

6.1.9 Elektronske listine za uveljavljanje pravic iz obveznega zdravstvenega zavarovanja

S prenovo informacijskega sistema KZZ bodo zagotovljeni pogoji za uvedbo elektronskih listin za uveljavljanje pravic iz obveznega zdravstvenega zavarovanja. Vse listine, ki jih zavarovane osebe lahko trenutno dobijo le na Zavodu, bi bile dosegljive v elektronski obliki.

6.1.9.1 Elektronska potrdila o zadržanosti z dela

V prenovljenem sistemu KZZ bo mogoče zagotoviti zapisovanje podatkov izdanih potrdilih o zadržanosti od dela v centralno bazo podatkov na Zavodu:

- zapisovanje podatkov ob izdaji potrdila pri osebnem zdravniku v centralno podatkovno bazo na Zavodu (izvorno in ažurno stanje podatkov),
- neposredni nadzor izdanih potrdil po zdravnikih pri izvajalcih in na Zavodu,
- neposredno dostopanje in preverjanje podatkov izdanih potrdil na področju izvajanja obveznega zdravstvenega zavarovanja na Zavodu:
    - v postopkih preverjanja upravičenosti do zadržanosti od dela in izplačila nadomestil v breme Zavoda pri imenovanih zdravnikih Zavoda,
    - v postopkih preverjanja zahtevkov za izplačilo in obračun nadomestil zavarovanim osebam v službah za obračun nadomestil Zavoda,

- možnost vzpostavitve neposrednega dostopanja do podatkov izdanih potrdil osebe pri zavezancu, ki ima za dostop do podatkov ustrezna pooblastila zavarovane osebe:
    - v postopkih preverjanja podatkov o upravičeni zadržanosti od dela osebe in za izračun nadomestila osebe
    - v postopkih pripravljanja zahtevka refundacije za Zavod (osnova za elektronsko posredovanje zahtevkov za refundiranje izplačanih nadomestil na Zavod brez priloženih potrdil v papirni obliki)

6.1.9.2 Druge elektronske listine

Sčasoma bi bilo mogoče vzpostaviti elektronsko obliko drugih listin, ki se uporabljajo pri uresničevanju obveznega zdravstvenega zavarovanja. Elektronske listine je mogoče vzpostaviti na način neposrednega posredovanja podatkov v centralno bazo podatkov Zavoda in potem dostopanje do teh podatkov s strani tistih uporabnikov in institucij, ki takšne dostope potrebujejo. Ker gre za uresničevanje pravic iz obveznega zdravstvenega zavarovanja je smiselno, da se podatki hranijo na centralnem računalniku Zavoda.

V takšni obliki je možno zagotoviti rešitve za naslednje listine:
- napotnica (obrazec NAP),
- naročilnica za tehnični pripomoček (obrazec NAR-1),
- naročilnica za pripomoček za vid (obrazec NAR-2),
- potrdilo o upravičenosti do potnih stroškov-spremstva (obrazec PS),
- predlog zobnoprotetične rehabilitacije (obrazec ZB),
- predlog zdravniški komisiji (obrazec ZK),
- delovni nalog (obrazec DN).

6.2 Koristi za zavarovance

Pri sedanjem sistemu lahko zavarovana oseba pridobila podatke iz KZZ le ob izdaji kartice, na enoti Zavoda ali pri svojem osebne zdravniku. Ob izdaji kartice je zavarovana oseba prejela izpis, ki je vseboval le tiste podatke, ki so bili na KZZ shranjeni ob personalizaciji kartice, ne pa ostalih podatkov, ki so se na kartico zapisali preko samopostrežnih terminalov.

Zavarovanim osebam bo na podlagi pametne kartice in uporabe digitalnega potrdila lahko omogočen vpogled do podatkov, ki jih Zavod hrani o njih. Podobne rešitve obstajajo tudi že v slovenskem prostoru (npr. vpogled v lastne osebne podatke v centralnem registru prebivalstva na naslovu http://vpogled-crp.gov.si/).

Neposreden dostop do točnih in ažurnih podatkov bo izvajalcem zdravstvenih storitev omogočilo bolj kakovostno in hitrejšo obravnavo pacienta, zaradi česar se bo povečalo zadovoljstvo zavarovanih oseb s storitvami zdravstvenih delavcev in se bo okrepil ogled zdravstva v Sloveniji.
Z ukinitvijo osveževanja podatkov o zdravstvenem zavarovanju na samopostrežnih terminalih ali okencih zavarovalnic bomo zavarovanim osebam omogočili, daj jim za ta namen ne bo več potrebno obiskovati samopostrežnih terminalov ali poslovnih enot zavarovalnic, kar je povezano s potnimi stroški in izgubljenim časom.

V vzpostavitvijo elektronskega recepta zdravnik zavarovani osebi ne bo več izročil papirnatega recepta, ampak bo napisal elektronski recept, ki se bo shranil na strežniku. Pacient bo tako lahko dobil zdravila napisana na elektronskem receptu v katerikoli lekarni na podlagi svoje kartice zdravstvenega zavarovanja. Zavarovanim osebam tako ne bo več potrebno skrbeti za papirnati recept in izgubo le tega, kar bo olajšalo postopke izdaje zdravil predpisanih na recept.

Ostale koristi so še:

- dostop do večjega števila storitev in informacij,
- večja udobnost za zavarovane osebe (dostop do storitev in informacij 24 ur na dan),
- uporabniki spletnega portala se lahko aktivno vključijo v njegovo izboljšavo in dopolnitve,
- hitrejše reševanje problemov in manj administrativnih ovir,
- nižji stroški,
- uporaba pametne kartice skupaj z digitalnimi potrdili tudi za ostale storitve (elektronsko bančništvo, edavki, itd.),
- itd.

6.3 Koristi za Zavod

Personalizacija kartic bi se lahko izvajala bolj pogosto kot enkrat tedensko. S tem bi zavarovane osebe in zdravstveni delavci naročeno kartico dobili mnogo prej kot v sedanjem sistemu. Poleg tega bi se močno skrajšal sam proces izdelave novih kartic in potrebnih korakov od naročila do izdelave kartice (npr. odgovorni osebi na Zavodu ne bilo več potrebno enkrat tedensko izvajati postopkov za kreiranje izhodnih datotek za personalizacijo in pošiljanje datotek preko elektronske pošte personalizatorju kartic). Zaradi tega se bodo zmanjšali tudi stroški povezani s personalizacijo.

Mreža samopostrežnih terminalov ne bi bila več potrebna, saj bi imeli izvajalci neposreden dostop do baze podatkov na Zavodu in tako osveževanje kartice na

samopostrežnih terminalih ne bi bila več potrebna. Strošek povezan s samopostrežnimi terminali bi tako odpadel, poleg tega bi izboljšali kakovost zdravstvenih storitev in hitrost izvajanja zdravstvenih storitev, saj zavarovanim osebam ne bi bilo potrebno pogosto ob obisku zdravnika osveževati podatkov na KZZ, kar bi dolgoročno vplivalo na boljši ugled Zavoda.

Prav tako bi poenostavili postopke, ki jih izvajajo referenti na zavarovalnicah, saj prav tako ne bilo potrebno več osveževati podatkov na KZZ.

V Službi za poslovanje s kartico na Zavodu bi ukinili nekatere postopke povezane s sedanjimi karticami (npr. osveževanje KZZ pred pošiljanjem iz depoja ne bi bilo več potrebno).

Neposredno dostopni podatki preko omrežja o izbranih osebnih zdravnikih prinašajo koristi tudi za Zavod. Zagotavljanje podatkov na tak način je nedvomno cenejše od zagotavljanja podatkov na KZZ, saj se na ta račun poceni personalizacija kartic in postopki ažuriranja podatkov kartice v Službi za poslovanje s KZZ, na območnih enotah in izpostavah. Izvajalci bi lahko sami vnašali spremembe podatkov v bazo podatkov na Zavodu.

Na takšen način bi Zavod prišel do ažurnejših podatkov o novih izbirah, ki so pomembni pri kontroli uveljavljanja pravic iz naslova OZZ (pravice, ki so vezane na pooblastila izbranega osebnega zdravnika). Osveženi podatki pa so zelo pomembni oziroma nujni tudi za zagotavljanje čim bolj točnih podatkov pri neposrednih poizvedbah (npr. zdravnika v bolnišnici, da ugotovi, kam je potrebno poslati odpustno pismo). S tem bi zagotovili, da bi bili neposredno dostopni podatki enako ažurni, kot so sedaj podatki na karticah.

Podobno kot pri zagotavljanju podatkov o izbirah osebnih zdravnikov, je tudi z zagotavljanjem podatkov o izdanih medicinsko tehničnih pripomočkih. V tem primeru bi dobavitelji in izposojevalnice MTP podatke posredovali neposredno na Zavod. Namesto zapisa podatkov na KZZ bi torej ob izdaji ali izposoji pripomočka podatke neposredno poslali na Zavod. Tako bi bili podatki v podatkovni bazi Zavoda enako ažurni in točni kot sedaj na KZZ. Prav tako bi lahko razširili tudi nabor podatkov, ki bi jih videli dobavitelji in izposojevalnice MTP.

Enak postopek bi veljal tudi za izdana zdravila. Namesto zapisa podatkov na KZZ bi ob izdaji zdravila lekarna lahko poslala podatke neposredno na Zavod. Tako bi bili podatki v podatkovni bazi Zavoda enako ažurni kot sedaj na KZZ. Zdravniki bi lahko imeli vpogled v vsa izdana zdravila ter celotno zgodovino izdanih zdravil, v kolikor bi jih to zanimalo, poleg tega bi dobili še dodatne informacije o izdanem zdravilu, kot npr. priimek in ime zdravnika, ki je zdravilo predpisal (trenutno je na KZZ samo šifra

zdravnika, pri zdravnikih pa ni nameščena podatkovna baza zdravstvenih delavcev, preko katere bi lahko povezali šifro zdravnika iz KZZ z ostalimi podatki iz podatkovne baze o zdravstvenih delavcih).

Zavod bi s tem pridobil bolj ažurne in točne podatke, kar omogoča boljše kontrole in nadzor nad uresničevanjem pravic iz obveznega zdravstvenega zavarovanja.

6.4 Kvantitativna ocena koristi in stroškov vzpostavitve neposrednega dostopa do podatkov

V tem razdelku bom prikazal kvantitavivno oceno koristi in stroškov povezanih s prenovo informacijskega sistema KZZ in predvideno dobo vračila investicije:

- Prenova personalizacije KZZ in PK,
- Vzpostavitev neposrednega dostopa do podatkov
- Vzpostavitev zdravstvenega portala

6.4.1 Prenova personalizacije KZZ in PK,

Trenutno se uporablja 2.021.921 aktivnih kartic zdravstvenega zavarovanja, ki jih uporabljamo zavarovane osebe in 10.586 profesionalnih kartic, ki jih uporabljajo izvajalci zdravstvenih storitev. Za branje podatkov na KZZ, izvajalci zdravstvenih storitev, dobavitelji MTP in referenti Zavoda ter ostalih zavarovalnic uporabljajo 5.160 namiznih, 920 prenosnih in 200 bralnikov kartic nameščenih v tipkovnici.

V tabeli 6.1 in 6.2 so prikazane približne cene kartic, personalizacije kartic ter bralnikov kartic, ki se uporabljajo v sedanjem sistemu KZZ. Dobavitelj pametnih praznih kartic in bralnikov kartic je Gemplus, personalizacijo kartic KZZ in PK izvaja Cetis d.d., izdelavo in personalizacijo plastičnih kartic EU-KZZ pa trenutno izvaja še Radeče papir d.d, vendar je že podpisana nova pogodba s Cetisom d.d.

V novem sistemu KZZ se bodo verjetno uporabljale pametne kartice z 32 Kb EEPROM, po vsej verjetnosti Java kartice, saj več kot 90% vseh izdelanih pametnih kartic podpira JavaCard specifikacijo. Poleg tega bi z uporabo Java kartic, specifikacijo GlobalPlatform in OpenCard ogrodja razvitega v Javi lahko postopoma zamenjali sedanje KZZ, saj bi imele nove kartice enako funkcionalnost kot sedanje KZZ z dodatnimi možnostmi. V tabeli 6.3 so navedene predvidene cene novih Java kartic in personalizacije. Cena shranjevanja digitalnega potrdila na kartice je povzeta po ceni priprave osebnega gesla. Glede na to, da je Evropska kartica zdravstvenega zavarovanja lahko natisnjena na zadnji strani KZZ, izdelovanje in personalizacija

plastične EU-KZZ ne bi bila več potrebna. Bralnike pametnih kartic, ki jih sedaj uporabljamo, se bodo lahko uporabljali tudi v novem sistemu KZZ. Cena sedanjih in bodočih bralnikov kartic je prikazana v tabeli 6.2.

Tabela 6.1 in 6.2: Približne cene kartic, personalizacije kartic in bralnikov kartic v sedanjem sistemu KZZ

	KZZ	PK	EU-KZZ
Prazna pametna kartica z OS	719,00 SIT	719,00 SIT	
Personalizacija kartice	335,00 SIT	335,00 SIT	
Prazna plastična kartica in personalizacija kartice			68,00 SIT
Priprava osebnega gesla (PIN)		93,00 SIT	
Shranitev digitalnega potrdila na kartico			
Pošiljanje kartic imetnikom po pošti	300,00 SIT	300,00 SIT	300,00 SIT
Pošiljanje PIN-ov imetnikom po pošti		300,00 SIT	
Skupaj:	1.354,00 SIT	1.747,00 SIT	368,00 SIT

Namizni bralniki kartic	Prenosni bralniki kartic
45.000	80.000

Vir: Povzeto po podatkih Zavoda, 2006

Tabela 6.4 prikazuje cene kvalificiranih digitalnih potrdil, ki jih izdajata slovenski agenciji za izdajo digitalnih potrdil. V tabeli sta navedeni le dve največji agenciji, ki izdajata kvalificirana digitalna potrdila za različne storitve.

Kljub temu, da so kvalificirana digitalna potrdila za fizične osebe agencije SIGEN-CA brezplačna, pa mora za potrdilo zaprositi vsak posameznik, ki želi pridobiti digitalno potrdilo.

Tabela 6.3: Predvidene cene kartic, personalizacije kartic v novem sistemu KZZ

	Nova KZZ in EU-KZZ	Nova PK
Prazna pametna kartica z OS	719,00 SIT	719,00 SIT
Personalizacija kartice	335,00 SIT	335,00 SIT
Prazna plastična kartica in personalizacija kartice		
Priprava osebnega gesla (PIN)		93,00 SIT
Shranitev digitalnega potrdila na kartico	93,00 SIT	93,00 SIT
Pošiljanje kartic imetnikom po pošti	300,00 SIT	300,00 SIT
Pošiljanje PIN-ov imetnikom po pošti		300,00 SIT
Skupaj:	1.447,00 SIT	1.840,00 SIT

Vir: Lasten

Bolj smiselna in organizacijsko lažja rešitev je odločitev za digitalna potrdila SIGEN-CA za poslovne subjekte, kjer pooblaščena oseba uredi vse potrebno za pridobitev kvalificiranih spletnih digitalnih potrdil.

Ob predpostavki, da bo Zavod lahko uporabil trenutne bralnike kartic, bi zamenjava kartic zdravstvenega zavarovanja Zavod glede na cene prikazane v tabeli 6.3 stala približno 2.017.435 KZZ * 719 SIT = 1.450.535.765 SIT, skupaj s prsonalizacijo pa

1.450.535.765 SIT + (1.477,00 SIT * 2.017.435) = 4.430.287.260 SIT. Zamenjava profesionalnih kartic za zdravstvene delavce bi znašala približno 19.916 * 719 SIT = 14.319.604 SIT, skupaj s personalizacijo pa 14.319.604 SIT + (1.840,00 SIT * 19.916) = 50.965.044 SIT. Če ob tem upoštevamo še pridobitev kvalificiranih spletnih potrdil agencije SIGEN-CA za poslovne subjekte za zdravstvene delavce moramo k vrednosti za nove profesionalne kartice prišteti še znesek letne naročnine za kvalificirano digitalno spletno digitalno potrdilo, kot je navedeno v tabeli 6.4. Vrednost novih profesionalnih kartic skupaj z letno naročnino za kvalificirano spletno digitalno potrdilo za poslovne subjekte za prvo leto uporabe bi tako znašala 50.965.044 SIT + (19.916 SIT * 2.100 SIT) = 92.788.644 SIT. Zamenjava vseh profesionalnih kartic skupaj s kvalificiranimi spletnimi digitalnimi potrdili agencije SIGEN-CA in kartic zdravstvenega zavarovanja skupaj z letno naročnino za digitalna potrdila za prvo leto bi znašala približno 4.523.075.904 SIT .

Ob tem je potrebno upoštevati, da bi Zavod za vsako naslednje leto moral plačati še naročnino za kvalificirana spletna digitalna potrdila za poslovne subjekte, ki bi znašala 19.916 * 2.100 SIT = 41.823.600 SIT na leto.

Tabela 6.4: Cene kvalificiranih digitalnih potrdil

Izdajatelj digitalnega potrdila	Vrsta digitalnega potrdila	Letna naročnina	Uporaba
SIGEN-CA			
	Spletno digitalno potrdilo za poslovne subjekte	2.100,00 SIT	
	Posebno spletno digitalno potrdilo za poslovne subjekte	7.220,00 SIT	Dva para ključev, namenjeno za pravne in fizične osebe za opravljanje dejavnosti
	Digitalno potrdilo za strežnik	15.060,00 SIT	
	Spletno kvalificirano digitalno potrdilo za fizične osebe	brezplačno	En par ključev, namenjeno fizičnim osebam
POŠTA®CA			
	Standarno kvalificirano digitalno potrdilo z obvezno uporabo pametne kartice	2.000,00 SIT	En par ključev, namenjeno končnim uporabnikom ali strežnikom
	Napredno kvalificirano digitalno potrdilo z obvezno uporabo pametne kartice	6.000,00 SIT	Dva para klučev, namenjeno končnim uporabnikom ali strežnikom

Vir: Lasten

6.4.2 Vzpostavitev neposrednega dostopa do podatkov

Najbolj verjetna in najcenejša rešitev s katero bo Zavod omogočil neposreden dostop do podatkov, je uporaba javnega internetnega omrežja z uporabo SSL oziroma TLS protokola, ki omogoča varen prenos podatkov. Za dostop do podatkov bi lahko izbrali ADSL povezavo s pasovno širino 2Mbps.

Na strežniku bo moralo biti nameščeno digitalno potrdilo, ki omogoča uporabo zaščitenega kanala (SSL) za prenos podatkov. S tem zagotovimo, da se podatki varno prenašajo med brskalnikom in spletnim strežnikom.
Ob prijavi na strežnik se morata odjemalec in strežnik medsebojno overiti. Poleg tega je pomembno, da se ob prijavi na strežnik preveri tudi veljavnost digitalnih potrdil. S tem zagotovimo, da se na strežnik lahko prijavi le uporabnik z veljavnim kvalificiranim digitalnim potrdilom, ki ga je izdala določena organizacija. Hkrati lahko tudi uporabnik preveri, če se je prijavil na pravi strežnik z veljavnim digitalnim potrdilom strežnika.

Letni najem digitalnega potrdila za spletni strežnik znaša 15.060 SIT (tabela 6.4).

Mesečna naročnina paketa Poslovni ADSL znaša 32.000 SIT. Osnovna hitrost prenosa podatkov v tem paketu je 2084/384 kbit/s, ki pa jo je možno nadgraditi tudi do 8 Mbit/s (vir: http://www.telekom.si/). Za izračun predvidenih informativnih stroškov vzpostavitve varnega neposrednega dostopa do podatkov v tabeli 6.5 sem uporabil paket Poslovni ADSL z osnovno hitrostjo.

Glede na to, da znamka Cisco na področju usmerjevalnikov obvladuje 90% trga in je med vodilnimi na področju mrežnih varnostnih naprav ter glede na to, da tudi na Zavodu uporabljamo usmerjevalnike in požarne pregrade znamke Cisco, sem izbral usmerjevalnik Cisco serije 800, katerega cena znaša približno 123.000 SIT, cena požarne pregrade PIX 501 znamke Cisco pa znaša približno 113.000 SIT (vir: www.xenya.si/sup/ceniki/ cisco/cisco.xls).

Izbira strojne opreme je odvisna od velikosti organizacije in njenih potreb, zato so lahko cene usmerjevalnikov tudi bistveno višje. Nekateri usmerjevalniki imajo tudi funkcijo požarne pregrade kot npr. Cisco 1702, s čimer se zmanjša strošek povezan z nakupom požarne pregrade. Prikazane cene izbranih naprav in izračunani stroški so zato v tabeli 6.5 zgolj informativni.

Za postavitev spletnega portala na spletnem strežniku, preko katerega bi izvajalci zdravstvenih storitev dostopali do podatkov na Zavodu, bi lahko uporabili spletni strežnik Zavoda. Izdelovalci spletnih strani oz. spletnih portalov neradi govorijo o ceni spletnega portala, če ne poznajo natančno projekta in želja naročnika. Predvidevam, da bi strošek povezan z izdelavo spletnega portala za dostop do podatkov znašal približno 3.000.000 SIT.

Zavod je v letu 2005 sklenil pogodbe z 1382 izvajalci zdravstvenih storitev:

- 70 zdravstvenimi domovi,
- 1082 zasebniki,
- 26 bolnišnicami,

- 101 lekarno,
- 16 zdravilišči in
- 92 socialnimi varstvenimi zavodi.

Poleg stroškov prikazanih v tabeli 6.5, je potrebno dodati še stroške na strani izvajalcev za vzpostavitev lokalnega omrežja (stikala, računalniki, strežniki, itd.). Nekateri izvajalci zdravstvenih storitev so že sedaj dobro opremljeni z informacijsko tehnologijo in pri vzpostavljanju neposrednega dostopa do podatkov na Zavodu ne bi bilo potrebno veliko dodatnega dela in stroškov, medtem ko bi bilo pri izvajalcih, ki so trenutno slabo podprti z informacijsko tehnologijo obratno.

Tabela 6.5: Informativni predvideni stroški potrebni za vzpostavitev varnega dostopa do podatkov na Zavodu

Izvajalci zdr.storitev	Število	Skupna cena usmerjevalnikov	Skupna cena požarne	Skupna cena
	izvajalcev	CISCO 3725	pregrade CISCO PIX 501	Poslovni ADSL/mesec
zdravstvenimi domovi	70	8.610.000,00 SIT	7.910.000,00 SIT	2.240.000,00 SIT
zasebniki	1082	133.086.000,00 SIT	122.266.000,00 SIT	34.624.000,00 SIT
bolnišnice	26	3.198.000,00 SIT	2.938.000,00 SIT	832.000,00 SIT
lekarne	101	12.423.000,00 SIT	11.413.000,00 SIT	3.232.000,00 SIT
zdravilišča	16	1.968.000,00 SIT	1.808.000,00 SIT	512.000,00 SIT
socialnimi varstvenimi zavodi	92	11.316.000,00 SIT	10.396.000,00 SIT	2.944.000,00 SIT
Skupaj:	1387	170.601.000,00 SIT	156.731.000,00 SIT	44.384.000,00 SIT

Vir: Lasten

Poleg investicije je potrebno upoštevati tudi stroške vzdrževanja prenovljenega informacijskega sistema KZZ. V naslednjih odstavkih bom navedel približne stroške vzdrževanja sedanjega in prenovljenega sistema KZZ ter dobo vračila investicije.

V sedanjem sistemu Zavod letno zamenja 16.209 KZZ zaradi okvare čipa, kar pomeni da znašajo stroški zamenjave teh kartic približno 16.209 * 719 SIT = 11.654.271 SIT na leto. Skupaj s poštnino znaša strošek 11.654.271 + (300 SIT* 16.209) = 16.516.971 SIT na leto. Predvidevam, da se bo število zamenjanih KZZ zaradi okvare čipa v prenovljenem sistemu zmanjšalo pod 5.000, kar pomeni, da se bodo stroški bistveno zmanjšali in bodo znašali približno 5.000 * 719 SIT = 3.595.000 SIT na leto. Skupaj s poštnino bo strošek znašal približno 3.595.00 SIT + (300 SIT * 5.000) = 5.095.000 SIT na leto. Število zamenjanih PK zaradi okvare čipa Zavod ne vodi posebej, vendar je to število zaradi majhnega števila izdanih PK proti število izdanih KZZ zelo nizko in ne bo bistveno vplivalo za stroške vzdrževanja in dobo vračila investicije.

Na Zavodu je organizirana služba za poslovanje s kartico, ki je zadolžena za vsa administrativna dela povezana s KZZ. Prav tako skrbi za naročanje PK in njihovo vzdrževanje. Tudi v prenovljenem sistemu KZZ se naloge službe ne bodo bistveno spremenile.

Bistveni element sedanjega sistema KZZ so tudi SST terminali. Letni strošek rednega in izrednega vzdrževanja vseh 295 SST terminalov po celi Sloveniji znaša približno 139.000.000 SIT.

Letni strošek povezan z vzdrževanjem dveh TKS strežnikov in petih varnostnih strežnikov znaša približno 11.725.505 SIT.

V kolikor bo Evropska kartica zdravstvenega zavarovanja natisnjena na zadnji strani nove KZZ, se bodo stroški povezani z Evropsko kartico zdravstvenega zavarovanja bistveno zmanjšali. Kartica skupaj s personalizacijo, stane Zavod približno 68 SIT, poštnina za EUKZZ pa znaša približno 300 SIT. Glede na to, da je bilo v letu 2005 izdanih 623.296 EUKZZ, to pomeni, da se bodo stroški povezani z izdelavo EUKZZ zmanjšali za približno (623296 * 68 SIT) + (623.296 * 300 SIT) = 229.372.928 SIT.

Na podlagi analize zlorab KZZ, ki je bila narejena v lanskem letu, približno 26000 oseb, ki so imetniki KZZ, ni imelo urejenega obveznega zdravstvenega zavarovanja (podatek se lahko dnevno spreminja). V kolikor so te osebe KZZ potrdile pred koncem veljavnosti obveznega zdravstvenega zavarovanja, to pomeni, da imajo na KZZ zapisano veljavno obvezno zdravstveno zavarovanje in lahko KZZ uporabljajo in koristijo zdravstvene storitve na račun Zavoda kljub temu, da niso več upravičeni do brezplačnih zdravstvenih storitev, oz. do storitev, ki so pokrite z veljavnim obveznim zdravstvenim zavarovanjem. Glede na to, da Zavod še ne vodi stroškov zdravstvenih storitev po osebi, podatka o višini zlorab zaradi neurejenega obveznega zdravstvenega zavarovanja ne morem navesti. Predvidevam, da lahko znesek zlorab obveznega zdravstvenega zavarovanja znaša okoli 5.000.000 SIT mesečno. V prenovljenem sistemu KZZ, osebe, ki nimajo urejenega obveznega zdravstvenega zavarovanja, na dan koriščenja zdravstvenih storitev ne bodo mogle več koristiti le teh v breme Zavoda, kar pomeni zmanjšanje stroškov za Zavod.

Na podlagi podatkov navedenih v nalogi predvidevam, da bo vrednost investicije prenove informacijskega sistema KZZ znašala okoli 4.526.075.904 SIT. Pri tem sem zajel celotne stroške zamenjave KZZ in PK ter stroške postavitve spletnega portala. Stroški sedanjega vzdrževanja sistema KZZ znašajo približno 167.242.476 SIT na leto. Pri tem sem upošteval letne stroške rednega in izrednega vzdrževanja SST terminalov, stroške povezane z vzdrževanjem TKS sistema ter stroške povezane z zamenjavo KZZ zaradi okvare čipa. Letni stroški vzdrževanja prenovljenega sistema KZZ bodo znašali okoli 60.659.165 SIT. Pri tem sem upošteval znesek letne naročnine za spletna digitalna potrdila za izvajalce zdravstvenih storitev in letni najem digitalnega potrdila za spletni strežnik, stroške povezane z vzdrževanjem TSK sistema in predvidene stroške zaradi menjave KZZ zaradi okvare čipa.

Stroške, povezane z vzpostavitvijo neposrednega dostopa do podatkov kot so zagotovitev ADSL povezave, nakup usmerjevalnikov in požarne pregrade, nisem upošteval, ker bodo ti stroški povezani s posameznimi izvajalci zdravstvenih storitev. Predvideno celotno vrednost investicije, s katero si bodo izvajalci zdravstvenih storitev zagotovili možnosti za vzpostavitev neposrednega dostopa do podatkov, se lahko izračuna iz tabele 6.5.

Predvidena razlika med letnimi stroški v sedanjem sistemu KZZ in v prenovljenem sistemu KZZ bo 396.956.239 SIT. Največji strošek v sedanjem sistemu, v primerjavi s prenovljenim sistemom je pri vzdrževanju SST terminalov, izdajanju EU-KZZ in zlorabi obveznega zdravstvenega zavarovanja.

Iz tabele 6.6 je razvidno, da je na podlagi podatkov predvidena doba vračila investicije v prenovljeni sistem KZZ 11 let.

Pri tem še enkrat poudarjam, da bo zaradi poteka življenjske dobe pametnih kartic zamenjava KZZ in PK potrebna ne glede na to, ali bi prenavljali informacijski sistem KZZ ali ne.

Tabela 6.6: Informativni predvideni stroški investicije za prenovo sistema KZZ ter prikaz približnih sedanjih in predvidenih prihodnjih stroškov v sistemu KZZ

Vložek za prenovo sistema KZZ		4.526.075.904,00 SIT
Sedanji letni stroški vzdrževanja		
	SST terminali	139.000.000,00 SIT
	TKS sistem	11.725.505,00 SIT
	Menjava KZZ zaradi okvare čipa	16.516.971,00 SIT
	Skupaj:	167.242.476,00 SIT
Naročilo EUKZZ / leto		229.372.928,00 SIT
Znesek zlorab obveznega zdravstvenega zavarovanja zaradi potrjene KZZ		60.000.000,00 SIT
	Skupaj:	456.615.404,00 SIT
Letni stroški vzdrževanja v prenovljenem sistemu		
	TKS strežnik	11.725.505,00 SIT
	Menjava KZZ zaradi okvare čipa	5.095.000,00 SIT
	Naročnine za dig.potrdila za PK	41.823.600,00 SIT
	Najem dig.potrdila za strežnik	15.060,00 SIT
	Vzdrževanje spletnega portala	1.000.000,00 SIT
	Skupaj:	59.659.165,00 SIT

Razlika med sedanjimi in novimi predvidenimi stroški vzdrževanja sistema KZZ:	396.956.239,00 SIT
Predvidena doba vračila investicije (v letih):	11,40

Vir: Lasten

Glede na to, da bodo stroški povezani s prenovo informacijskega sistema KZZ in s tem vzpostavitve neposrednega dostopa do podatkov na Zavodu za izvajalce zdravstvenih storitev zelo visoki, bo sredstva moralo zagotoviti tudi Ministrstvo za

zdravje. Potrebno je narediti vse potrebno, da Zavod del sredstev pridobi tudi iz skladov EU za strukturni razvoj.

V kolikor bi se Zavod odločil, da bo dostop do podatkov in izmenjava podatkov potekala preko MPLS VPN omrežja, je potrebno upoštevati še strošek priklopa, ki skupaj z davkom znaša 432.000 SIT ter mesečno naročnino na storitev, ki znaša 153.600 SIT z davkom (vir: http://www.telekom.si/zasebni_uporabniki/ceniki/?sid= 1891). Navedene cene veljajo le za pasovno širino 2 Mbit/s. Pri večjih pasovnih širinah je cena storitve višja.

Poleg neposrednih koristi zaradi prenove informacijskega sistema KZZ bo imel Zavod tudi posredne koristi. Glede na to, da ima Zavod zaradi sedanjega sistema KZZ ne le dober ugled v Evropski uniji pač pa tudi drugih državah, bo s prenovo sistema KZZ še bolj utrdil ugled Zavoda izven naših meja. To pa bo pomenilo tudi mednarodno udeležbo na strokovnih dogodkih in sodelovanje v delovnih skupinah EU na področju informatizacije zdravstva.

Tudi razpoznavnost Slovenije bi se s tem nekoliko povečala.

Zavod ima že sedaj zaradi svojih izkušenj veliko prednosti pri uvajanju informatike v zdravstvu pred drugimi državami EU, kar lahko izkoristi za pomoč pri uvajanju informatike v zdravstvu v bivših Jugoslovanskih republikah (Srbija, Črna gora) in tudi v državah, ki se bodo odločile za prenovo informatike v zdravstvu.

Zaradi prenove sistema KZZ, ki bo v večji meri neodvisen od proizvajalcev strojne in programske opreme, bo Zavod lažje prilagajal informatiko v zdravstvu in sistem KZZ novim standardom in tehnologijam.

Z neposrednim dostopom do podatkov zavarovane osebe, le te ne bodo mogle več izkoriščati tri mesečne veljavnosti OZZ na sedanji KZZ, v kolikor ne bodo imele urejenega OZZ. S tem se bo povečala tudi finančna disciplina zavezancev za prispevek in zavarovancev pri plačilu premij za prostovoljna zdravstvena zavarovanja.

Zavarovancem KZZ ne bo potrebno več potrjevati na SST terminalih, s čimer se bo povečala avtonomnost zavarovancev pri uporabi KZZ.

7 Možnost uporabe kartice zdravstvenega zavarovanja tudi za druge namene

Novo IJK infrastrukturo in nove kartice zdravstvenega zavarovanja bi bilo smiselno uporabiti tudi za druge namene kot npr. za elektronsko osebno izkaznico, za shranjevanje ostalih digitalnih potrdil za elektronsko poslovanje, za evropsko kartico zdravstvenega zavarovanja na zadnji strani kartice, itd.

7.1 Uporaba kartice zdravstvenega zavarovanja kot osebnega dokumenta

Glede na to, da smo v dobi plastičnih kartic in imamo zaradi tega v denarnici vedno več tovrstnih kartic, bi veljalo razmisliti, da bi novo KZZ lahko uporabili tudi kot veljaven identifikacijski dokument, oziroma kot nadomestilo osebne izkaznice.

Na prvo stran KZZ bi lahko vstavili sliko imetnika kartice, dodali določene grafične podatke, varovalne elemente in tako omogočili uporabo nove KZZ kot osebnega dokumenta. Slika 7.2 prikazuje primer zdravstvene kartice, ki bi jo lahko z nekaj dodatnimi grafičnimi podatki uporabili tudi kot identifikacijski dokument v slovenskem prostoru. Edina slabost je, da bi morala ob uvedbi tovrstne rešitve zavarovana oseba dostaviti tudi svojo sliko.

Slika 7.1: Prikaz nemške kartice zdravstvenega zavarovanja

Vir: Gieseke & Devrient, 2006

7.2 Evropska kartica zdravstvenega zavarovanja kot del kartice zdravstvenega zavarovanja

Z zamenjavo kartice zdravstvenega zavarovanja, se bo spremenila tudi grafična podoba kartice. V sedanjem sistemu KZZ, zavarovane osebe posebej naročajo evropske kartice zdravstvenega zavarovanja s katerimi uveljavljajo zdravstvene storitve v tujini. V novem sistemu KZZ bi bilo smiselno evropsko kartico zdravstvenega zavarovanja prenesti na novo KZZ. Tako rešitev so uvedli tudi v Avstriji ob uvajanju tovrstne rešitve. S tem bi se strošek za evropske kartice zdravstvenega zavarovanja močno zmanjšal oz. bi ga povsem odpravili. Ker je personalizacijo evropskih kartic zdravstvenega zavarovanja prevzel Cetis d.d., se mi zdi to idealna rešitev.

Pred nekaj meseci je bila sprožena uvedba pilotnega projekta Netc@rds. S tem se osebe, ki nimajo urejenega zavarovanja ne morejo več koristiti zdravstvenih storitev v državah EU, ki sodelujejo v projektu. Cilj tega projekta je, da bi lahko izvajalci zdravstvenih storitev v tujini iz kartice zdravstvenega zavarovanja brez uporabe profesionalne kartice zdravstvenega osebja prebrali ključne podatke o zavarovani osebi in njeni veljavnosti obveznega zavarovanja. V državah EU, kjer nimajo razvite tehnologije, s katero bi lahko izvajalci zdravstvenih storitev prebrali podatke iz KZZ, bi osebe kljub temu lahko koristile zdravstvene storitve na podlagi KZZ, vendar bi Zavod lahko od oseb zahteval povrnitev stroškov, če v času koriščenja zdravstvenih storitev v tujini niso imele veljavnega obveznega zavarovanja. Slika 7.1 prikazuje primer kartice zdravstvenega zavarovanja v Avstriji.

Slika 7.2: Avstrijska zdravstvena kartica skupaj z evropsko kartico zdravstvenega zavarovanja na zadnji strani kartice

Vir: Koch, 2005

7.3 Uporaba kartice zdravstvenega zavarovanja za druge namene

Do sedaj je bila predstavljena možnost uporabe KZZ kot evropska kartica zdravstvenega zavarovanja in kot identifikacijski dokument, ki bi nadomestil osebno izkaznico.

V slovenskem prostoru obstaja že kar nekaj rešitev elektronskega poslovanja z uporabo kvalificiranih digitalnih potrdil, tako z javno upravo (npr. e-davki), kot gospodarskimi družbami (npr. elektronsko bančništvo).

Glede na zamisli in možnost prenove informacijskega sistema KZZ obstaja možnost, da na novo KZZ dodajamo tudi kvalificirana digitalna potrdila za elektronsko poslovanje z ostalimi organizacijami in uporabo drugih aplikacij. Pri elektronskem poslovanju z banko, bi moral lastnik KZZ izbrati ustrezno digitalno potrdilo na kartici in vnesti zasebni ključ.

Shranjevanje digitalnih potrdil na pametni kartici KZZ bi pomenilo večjo varnost pri elektronskem poslovanju za državljane, poleg tega pa bi se zmanjšali stroški državljanov povezani z digitalnimi potrdili in potrebno opremo za elektronsko poslovanje.

8 Sklep

Ko se odločimo za elektronsko poslovanje, je bistvenega pomena, da skrbno izdelamo varnostno politiko, metodologijo možnih tveganj, privzeto servisno tehnično kulturo, vse standarde, sprejeta merila kakovosti računalniških rešitev, varnostnih sistemov in priporočil za varnost ter kakovost na področju elektronskega poslovanja.

Stanje slovenskega zdravstva vezano na uporabo informacijske tehnologije je trenutno na nizkem nivoju, zato bo v prihodnjih mesecih in letih potrebno vložiti največ napora za vzpostavitev prenovljenega informacijskega sistema KZZ prav na tem področju. Zdravstveno osebje bo potrebno motivirati in izobraziti za uporabo sodobne informacijske tehnologije.

Informacijska tehnologija predstavlja odlično priložnost za izboljšanje kakovosti, učinkovitosti in zmanjšanje stroškov, s pomočjo večje zanesljivosti in hitrosti komunikacij med izvajalci zdravstvenih storitev in bolniki.

Obstaja več razlogov zaradi katerih naj bi Zavod prenovil IS KZZ:

- prenova personalizacije ter odprava odvisnosti od proizvajalcev in lažji vnos sprememb,
- potrebe po zamenjavi KZZ, zaradi prenehanja izdelave sedanjega čipa,
- zagotavljanje boljše varnosti in kakovosti podatkov,
- preverjanje veljavnosti obveznega zdravstvenega zavarovanja neposredno z dostopom do centralne zbirke podatkov na Zavodu in drugih PZZ,
- hiter razvoj informacijskih in komunikacijskih tehnologij,
- zagotavljanje bolj kakovostnih in hitrejših zdravstvenih storitev,
- zmanjševanje in racionalizacija stroškov IS KZZ,
- boljše obvladovanje stroškov povezanih z zdravstvenem zavarovanjem,
- hitrejši dostop do podatkov in razširjen nabor podatkov,
- zagotovitev PKI infrastrukture,
- uvedba elektronskega podpisa – evropska direktiva in slovenski zakon ZEPEP,
- uvedba elektronskega recepta in
- razvoj tehnologij pametnih kartic.

Tako v slovenskem, kot tudi v širšem evropskem in svetovnem prostoru, so že uvedli rešitve infrastrukture javnih ključev v povezavi z uporabo pametnih kartic.

Glavi del predstavlja overitelj javnih ključev (Certification Authority -CA). Izhodišče je standard za digitalno potrdilo X.509v3, ki je splošno sprejet. Digitalna potrdila, ki so iz različnih razlogov neveljavna, se objavljajo na posebnih seznamih, za katere se je uveljavila kratica CRL.

Glede na dejstvo, da več kot 90% vseh izdelanih pametnih kartic podpira JacaCard specifikacijo menim, da je smiselno obstoječe KZZ in PK zamenjati z java pametnimi karticami. Pri tem lahko Zavod izbere postopen prehod na nov sistem KZZ, kar pomeni, da ne bi bilo potrebno zamenjati vseh KZZ naenkrat, ampak postopoma, pri tem pa je potrebno zagotoviti enako funkcionalnost sedanjih in novih KZZ.

Profesionalne kartice je potrebno zamenjati v celoti, saj bo na novih PK shranjeno kvalificirano digitalno potrdilo.

Zdravstvenemu osebju je potrebno zagotoviti čim lažjo pridobitev kvalificiranega digitalnega potrdila, zato menim, da bi najmanj težav povzročalo pridobivanje kvalificiranih digitalnih potrdil za poslovne subjekte, kjer pooblačena oseba organizacije, lahko uredi vse potrebno za izdajo in prevzem potrdila. Menim, da je trenutno najboljša izbira agencija, ki izdaja kvalificirana digitalna potrdila izbira SIGEN-CA.

Smiselno se mi zdi, da bi novo KZZ uporabili tudi za druge namene in ne le zgolj kot identifikacijsko kartico zdravstvenega zavarovanja in kot ključ za dostop do zdravstvenih podatkov. S personalizacijo le nekaj ključnih podatkov na kartici in dodajanjem slike na kartico, bi lahko novo KZZ uporabili tudi kot identifikacijski dokument.

Zadnja stran nove kartice zdravstvenega zavarovanja bi bila namenjena evropski kartici zdravstvenega zavarovanja, kap bi pomenilo manjše stroške povezane z naročili in izdelavo evropske kartice zdravstvenega zavarovanja. Za zavarovane osebe pa bi to pomenilo, da morajo KZZ pri odhodu v tujino vedno nositi s seboj. Kljub temu bi imeli samo eno plastično kartico, kot sedaj.

Možni so različni scenariji prehoda na nov sistem KZZ, med katerimi je, zaradi časovne stiske (zaloga dosedanjih KZZ bo potekla do sredine leta 2008) in visokih stroškov zamenjave IS najbolj verjetna postopna zamenjava dosedanjih KZZ z novimi, ki morajo biti povsem kompatibilne s sedanjimi KZZ. Sledi lahko uvajanje neposrednega dostopa izvajalcev zdravstvenih storitev do podatkov na Zavodu ter dodajanje digitalnih potrdil na nove KZZ. Profesionalne kartice bo potrebno zamenjati v celoti, ob tem pa bo potrebna registracija uporabnikov PK, zaradi uporabe kvalificiranih digitalnih potrdil.

Ob tem bo potrebno uporabiti specifikacijo za GlobalPlatform, ki je podprta na različnih karticah različnih proizvajalcev, saj omogoča lažjo prenosljivost aplikacij med karticami. Potrebno bo uporabiti tudi java ogrodje OpenCard.

V novem sistemu KZZ Zavod ne želi biti več odvisen od programske in strojne opreme posameznih proizvajalcev, ampak teži k uporabi odprtega okolja, kar bo pocenilo celotni sistem KZZ.

Za dostop izvajalcev zdravstvenih storitev do podatkov in povezovanje izvajalcev z Zavodom je najcenejša in dovolj varna rešitev uporaba javnega internetnega omrežja, s sočasno uporabo kvalificiranih digitalnih potrdil in vzpostavitev SSL povezav.

Za računalniško izmenjavo podatkov je potrebno uporabiti tudi nove možnosti strukturirane izmenjave podatkov, z uporabo razširljivega označevalnega jezika XML (ang. eXtensible Markup Language), ki je neodvisen od operacijskega sistema in aplikacij.

Za uspešno elektronsko poslovanje državljana z državo v prvi vrsti potrebno zagotoviti varen način dostopa državljanov do informacij in storitev javne uprave. Predpostavljam, da bodo državljani z zanimanjem sprejeli novo zdravstveno kartico

skupaj s digitalnim potrdilom, ki predstavlja sodobno alternativo klasičnim osebnim identifikatorjem (osebna izkaznica, potni list, zdravstvena izkaznica, bančna izkaznica,…) in hkrati osnovo za varen način komuniciranja z državo na elektronski način (Silič, 1998, str 127-129).

Naj odgovorim še na zastavljeno vprašanje v uvodu magistrskega dela.

V zadnjih nekaj letih je tehnologija in s tem večja uporaba pametnih kartic na katerih so shranjena digitalna potrdila zelo napredovala in omogoča najbolj varno poslovanje med poslovnimi subjekti in s tem izmenjavo podatkov. Sedanje kartice zdravstvenega zavarovanja in profesionalne kartice, bo v naslednjih letih potrebno zamenjati zaradi izteka življenjske dobe sedanjih kartic, zato je smiselno, da hkrati z zamenjavo kartic prenovimo celoten informacijski sistem KZZ in posledično zmanjšamo stroške povezane z vzdrževanjem informacijskega sistema KZZ. Glede na dejstvo, da so podobne rešitve že uvedene v slovenskem in evropskem prostoru, lahko pozitivne izkušnje uporabimo pri prenovi sedanjega sistema KZZ. Gledano s pravnega vidika je potrebno upoštevati zakonodajo in pravilnike tako v slovenskem kot v evropskem prostoru. Smiselno bi bilo dopolniti slovensko zakonodajo na področjih, ki bi prispevala k izboljšanju zdravstvenih razmer v Sloveniji.

9 Literatura in viri

1. Aksentič Željko: Napredna uporaba pametnih kartic, Fakulteta za računalništvo in informatiko, diplomska naloga, 2004

2. Avison David, Fitzgerald Guy: Information Systems Development: Methodologies, Techniques and Tools, 3rd ed. McGraw-Hill publishing company, London 2003, 592 str.

3. Avison, D.E. and Catchpole: Information system for the community health services, Medical Informatics, Vol.13, 2, 1987

4. Bentley Trevor: Information systems strategy for business. London: CIMA Publishing,1998. 162 str.

5. Boar Bernard H.: Strategic Thinking for Information Technology. New York: John Wiley & Sons, Inc., 1997, 270 str.

6. Ciglarič M., at al.: Uporaba pametnih kartic za varno hranjenje dokumentov, različica 1.0, Ljubljana, Fakulteta za računalništvo in informatiko, 2003, 15 str.

7. Clarke S.: Information systems strategic management. London: Routledge, 2001. 199 str.

8. Deitel, H.M., Deitel, P.J. in Nieto, T.R.: E-business & e-commerce : how to program. Upper Saddle River (N.J.) : Prentice Hall, cop. 2001. – XLV, 1254 str.

9. Dustin Elfriede, Rashka Jeff, at. al.: Quality web systems : performance, security, and usability, Boston: Addison Wesley, cop. 2002, XVII, 318 str.

10. Earl M.: Management Strategies for Information Technology, New York, Prentice-Hall, 1989, X, 218 str.

11. Fidler C., Rogerson S.: Strategic Managemnt Support Systems, London, Pitman, 1996, XII, 334 str.

12. Frančeškin B: Storitev navideznih zasebnih omrežij preko omrežja s preklapljanjem na osnovi labele, magistrsko delo, Ljubljana, Fakulteta za elektrotehniko, 2002

13. Garrett Jesse James: The Elements of User Experience: User-Centered Design for the Web. Pearson Education. 2002.

14. Gradišar Miro, Resinovič Gortan: Informatika v poslovnem okolju, 3. dopolnjen in razširjen ponatis, Ljubljana, Ekonomska fakulteta, 2001, XVI; 508 str.

15. Jemec Barbara: Razvoj elektronske osebne izkaznice v evropskih državah z analizo prednosti, slabosti, priložnosti in nevarnosti uvedbe in uporabe slovenske elektronske osebne izkaznice, diplomsko delo, Ljubljana, Ekonomska fakulteta, 2003

16. Kovačič A., Bosilj Vukšić V.: Management poslovnih procesov: prenova in informatizacija poslovanja s praktičnimi primeri, 1. natis, Ljubljana, GV založba, 2005, 487 str.

17. Kovačič A., Jaklič J., Indihar Štemberger M., Groznik A.: Prenova in informatizacija poslovanja, 1. natis, Ljubljana, Ekonomska fakulteta, 2004, IX, 345 str.

18. Kuniavsky Mike: Observing the User Experience: A Practitioner's Guide to User Research. Morgan Kaufmann. 2003

19. Lobe Jaka: Razvoj elektronskih plačilnih sredstev : stanje v Sloveniji, diplomsko delo, Ljubljana, Ekonomska fakulteta, 2003

20. Nielsen Jakob: Designing Web Usability: The Practice of Simplicity. New Riders Press. 1999

21. Nielsen Jakob, Tahir Marie: Homepage Usability: 50 Websites Deconstructed. Pearson Education. 2001

22. Odin: Zakon o elektronskem poslovanju in elektronskem podpisu – pravni, poslovni in tehnični vidiki. Gradivo za seminar, Portorož 17. – 18.11.2000, str. 2-10

23. Osojnik Mojca: Skrivnosti elektronskega poslovanja: priročnik za mala in srednja podjetja, 1. natis, Ljubljana, Gospodarska zbornica Slovenije, 2002, 288 str.

24. Ošlak Darinka: Varnost elektronskega poslovanja v slovenskem bančništvu, magistrsko delo, Ljubljana, Ekonomska fakulteta, 2005

25. Shelly, Gary B at al.: Systems Analysis and Design, 6th ed., Boston, Thomson Course Technology, cop., 2003, XIX, 689 str.

26. Silič M., Colnar M., etc.: E-poslovanje v javni upravi RS za obdobje od leta 2001 do 2004, Center vlade RS za informatiko, 2001

27. Šilc Milan: Pregled tehnologije pametnih kartic, Ljubljana, Fakulteta za računalništvo in informatiko, magistrsko delo, 2005

28. Vitgen Richard: Developing web information systems: from strategy to implementation, Oxford: Butterworth-Heinemann, 2002, XIII, 274 str.

29. Trnovšek Bojan: E-Centralni register prebivalstva, E-matične knjige in možnosti inkorporacije digitalnega potrdila na identifikacijski dokument. Pravnosistemski vidiki informacijske družbe 2002, str. 73-87.

30. Turban, Efraim and King David: Introduction to e-commerce. Upper Saddle River (N.J.) : Prentice Hall, cop. 2003, XXXIV, 537 str.

31. Turban, McLean, Wetherbe: Information Technology for Management: transforming organizations in the digital economy, 4rd ed. Wiley international ed , Hoboken (NJ) : J. Wiley, cop. 2004 , XIX, 731 str.

32. Timothy M. Jurgensen et. al., Smart Cards: The Developer's Toolkit, Prentice Hall PTR, 2002

33. Uwe Hansmann, Smart Card Application Development Using Java, Springer Verlag 2002

34. Vallabhaneni S. Rao: CISA Examination Textbooks, Volume 1: Theory. Second Edition.¸B.k.: SRV Professional Publications, 1996. 995 str.

35. Vidic Tomaž: Elektronsko poslovanje v državni upravi - predlog prenove poslovnih procesov vzdrževanja, magistrsko delo, Ljubljana, Ekonomska fakulteta, 2005

36. Zdravje na informacijski poti: Zbornik kongresa SDMI, Terme Zreče, april 2006

37. Wodtke Christina: Information Architecture: Blueprints for the Web. Pearson Education. 2002.

Viri

1. Akmal Bhatti: Healthcare Smart Cards – The Movement from Concept to Reality (URL: www.verisign.com.au/guide/extendpki/ExtendingManagdPKI.pdf), 07.02.2006

2. Banka Koper: Splošne informacije uporabe pametne kartice Aktiva, 17.1.2005

3. Bugnar W: The e-card expirience, 14.10.2005, SVC, Viena

4. Computer Security Resource Center: (URL: http://csrc.ncsl.nist.gov/), 31.05,2006

5. CVI – Center Vlade RS za informatiko: Zahtevana programska oprema za spletna digitalna potrdila [URL: http://www.sigen-ca.si/programska-oprema.htm], 25.02.2006

6. CVI – Center Vlade RS za informatiko: Navodila za varno ravnanje s spletnimi digitalnimi potrdili [URL: http://www.sigen-ca.si/varnoravnanje- spletna.htm], 25.02.2006

7. CVI – Center Vlade RS za informatiko: Prijavne službe SIGEN-CA za fizične osebe [URL: http://www.sigen-ca.si/prijavne-slu.htm], 26.02.2006

8. CVI – Center Vlade RS za informatiko: Predstavitev overitelja digitalnih potrdil na Centru Vlade RS za informatiko [URL: http://www.gov.si/ca/namen.htm], 26.02.2006

9. CVI – Center Vlade RS za informatiko: Namestitev čitalnika pametnih kartic [URL: http://www.sigov-ca.gov.si/spletna/pametne-kartice.htm], 26.02.2006

10. CVI – Center Vlade RS za informatiko: Varnostni vidik aplikacij z uporabo digitalnih potrdil SIGEN-CA in SIGOV-CA, verzija 1.0, 1.avgust 2003

11. Črešnar Pergar Nevenka: Državljani se vse bolj zavedajo svojih pravic. Slovenska uprava 2.2002. str. 7-9

12. Ivona Bezakova, Oleg Pashko, Dinoj Surendran: Elements of Smart Card Architecture [URL: http://people.cs.uchicago.edu/~dinoj/smartcard/], 2000

13. Gemplus: (URL: http://www.gemplus.com/smart/index.html), 10.05.2006

14. Get smarter : exploting smart card technology, London, Financial Times Business Publishing, 2002

15. Gieseke & Devrient: Smart Health Card:The key to the health care system of the future, 08.06.2006

16. Health Card Technology, inc. (URL: http://www.hct.com/frameset/noflash.htm), 07.02.2006

17. Hong Kong residents get MULTOS-based Smart ID Card (URL: www.multos.com/library/pdf/HongKong_ID.pdf), MAOSCO Ltd , 07.02.2006

18. H.Otter: An Overview of the Austrian e – card, 14.10.2005, SVC, Viena

19. Iljaž R.: Elektronski zdravstveni zapis in 'online' zdravstvene storitve v osnovnem zdravstvu, Informatica Medica Slovenica, Revija Slovenskega društva za medicinsko informatiko, letnik 10, številka 1, str. 26-34

20. JavaCard tehnologija za pametne kartice (URL: http://java. sun.com/ products/ javacard/), 10.3.2006

21. Kiran S., Lareau P., Lloyd S.: PKI Basics – A Technical Perspective, November 2002

22. Koch T: E – card and Signature Card, 14.10.2005, SVC, Viena

23. Laboratorij za komunikacijske naprave (URL: http://www.lkn.fe.uni-lj.si/), 1.6.2006

24. MAOSCO Ltd: Hong Kong residents get Multos – based Smart ID Card,

25. Ministrstvo za javno upravo: Kako pridobim spletno digitalno potrdilo SIGEN-CA, (URL: http:// www. sigen-ca.si/pridobitev_fizicni.php), 19.06.2006

26. Medical Smart Card Offers Korean Patients Improved Healthcare Services (URL:www.multos.com/library/pdf/02-10-00%20Korean%20CS.pdf), MAOSCO Ltd , 07.02.2006

27. Ministrstvo za javno upravo: Priporočila-PKI-aplikacije-v1.0.pdf (URL: http://www.si-ca.si/priporocila-PKI-aplikacije.htm). 20.02.2006

28. MULTOS operacijski sistem za pametne kartice (URL: http://www.multos.com), 10.3.2006

29. Ochsenbauer: GIN – The Austrian Health Information Network, 14.10.2005, SVC, Viena

30. Overitelj elektronskega podpisa (URL: http://www.pcmg.si/upload/files/), 12.11.2004

31. Overitelj na Ministrstvu za javno upravo: Politika SIGEN-CA (URL: http://www .sigen-ca.si/politika-sigen-ca-fizicne-osebe.php) 28.02.2006

32. Piccola: smart card management library, (URL: http://titanium.dstc.edu.au/ security/Piccola, 26.02.2006

33. Pličanič Senko: Pravno sistemski vidiki E-uprave. Javna uprava 1,2002.str. 47-62

34. Polajnar M.: SSL / TLS, maj 2004

35. Pregled pametnih kartic (URL: http://www.cardwerk.com/smartcards/), 21.4.2006

36. Public-Key Cryptography Standards (URL: http://www.rsasecurity. com/ rsalabs/pkcs/index.html#docs)

37. RSA standard (http://www.rsasecuruty.com), 21.4.2006

38. SETCCE – Security Technology Competence Center (URL: http:// www. setcce.si/slo/index2b4.php), 2005

39. Schmidradler: Rollout and training, 14.10.2005, SVC, Viena

40. Silič Marin: Vloga Centra vlade za informatiko pri uvajanju elektronskega poslovanja. Organizacija 3, 1998, str. 127-129.

41. Slovar informatike (URL: http://www.islovar.org/iskanje_enostavno.asp), 21.02.2006

42. Smart Card Alliance: The Taiwan Health Care Smart Card Project, 2005

43. Smart Card Basics (URL: http://smartcardbasic.com), 21.4.2006

44. Smart Health Cards: The key to the healthcare system of the future (URL: http://64.233.179.104/search?q=cache:2l58TXUERCAJ:www.gi-de.com/pls/ portal/maia.display_custom_items.DOWNLOAD_SEEALSO_FILE%3Fp_ID%3

D5446%26p_page_id%3D54976%26p_pg_id%3D42+Medical+Smart+Card+in+Austria&hl=sl&ct=clnk&cd=2), 07.02.2006

45. Strategija e-poslovanja v javni upravi RS za obdobje od leta 2001 do leta 2004, verzija 1.2, 2001, 156 str.

46. Strategija e-poslovanja v javni upravi RS za obdobje od leta 2005 do leta 2008, osnutek, 13.09.2004, 6 str.

47. Telekom: Storitev navideznega zasebnega omrežja (URL: http://www.telekom.si/poslovni_uporabniki/korporacijska_omrezja_vpn/), 18.07.2006

48. Tomažič S: Varnost v telekomunikacijah in kako jo zagotoviti, Univerza v Ljubljani, Fakulteta za elektrotehniko, 12.06.2006

49. Toplišek Janez: Elektronski podpis - usklajevanje tehnoloških in pravnih rešitev pri elektronskem poslovanju, Organizacija 29, št. 5, 1996, str. 291-300

50. Uporaba kriptografije v internetu; (URL: http://www.ca.gov.si/kripto/index.htm), 20.02.2006

51. Varnost v IP VPN omrežijih z tehnologijo IPsec: (URL: http://lms.uni-mb.si/vitel/14delavnica/predstavitve/ppt-robert_kolar.pdf), 31.05.2006

52. Zakon o elektronskem poslovanju in elektronskem podpisu (Uradni list RS, št. 57/2000 in 30/01 - ZODPM-C)

53. Žmak Peter: Infrastruktura javnih ključev; (URL: personal.l-sol.si/peterzmak/diploma/pki.ppt), 20.02.2006

54. Žmak P.: Infrastruktura Javnih ključev, 12.06.2006

55. W. Ibl: Workshop @ ZZZ-S; PKI based Applications for e-Health & e-Gov, 11.01.2006, PSE

10 Priloge

10.1 Pojmovnik

Certifikatska agencija (CA), ang. Certification Authority

Ustanova, ki izdaja digitalna potrdila. Ob tem jamči, da določeno digitalno potrdilo pripada osebi, kateri ga je izdala, vodi listo preklicanih digitalnih potrdil in skrbi za njeno objavo. Za preverjanje veljavnosti izdanih digitalnih potrdil objavi certifikatska agencija svoj javni ključ. V Sloveniji imamo več certifikatskih agencij, npr. SIGEN-CA, ki izdaja kvalificirana digitalna potrdila za državljane ter za pravne in fizične osebe, registrirane za opravljanje dejavnosti.

CSP (Cryptographic Service Provider)

Programska oprema na vašem operacijskem sistemu Windows, ki omogoča izvajanje splošnih kriptografskih funkcij. Zagotavlja izvajanje različnih algoritmov za kriptiranje in elektronsko podpisovanje.

Digitalni podpis, ang. digital signature

Z digitalnim podpisom dokazujete pristnost z vaše strani poslanega elektronskega sporočila, torej da ste samo vi in nihče drug določeno elektronsko sporočilo poslali izbranemu naslovniku po e-pošti. Prav tako mora digitalno podpisovanje omogočati tudi spletna stran, ki digitalni podpis zahteva (npr. e-davki, e-uprava). V ta namen se na vaš osebni računalnik namesti komponenta za digitalni podpis, ki od vašega pletnega brskalnika zahteva, da izbrani dokument digitalno podpiše.

Digitalno potrdilo, tudi digitalni certifikat, ang. Digital Certificate.

Je potrdilo v elektronski obliki, ki povezuje podatke iz potrdila z zasebnim ključem določene osebe, institucije ali strežnika ter potrjuje njeno identiteto. za preverjanje elektronskega podpisa z določeno osebo (imetnikom potrdila) ter potrjuje njeno identiteto.

Kvalificirano digitalno potrdilo

Je potrdilo, ki izpolnjuje zahteve iz 28. člena Zakona o elektronskem poslovanju in elektronskem podpisu in ga izda overitelj, ki deluje v skladu z zahtevami iz 29. do 36. člena tega zakona. Digitalno potrdilo vsebuje javni in zasebni ključ ter informacijo o

njegovem imetniku, ki ju podpiše oseba ali institucija, ki ji zaupamo. Javni ključi potrdil so objavljeni v splošno dostopnih imenikih ali na spletnih straneh.

Elektronski podpis, glej digitalni podpis

Javni ključ, ang. public key

Javni ključ digitalnega potrdila pomeni, da je le-ta javno dostopen oz. objavljen v t.i. javnem imeniku. Javni ključ nekega uporabnika uporabimo, če mu želimo poslati šifrirano sporočilo. Tako sporočilo bo lahko prebral le prejemnik tako, da ga bo odšifriral z uporabo svojega privatnega ključa.

Kriptiranje, ang. encryption

Je postopek zagotavljanja tajnosti elektronsko izmenjanih podatkov. S pomočjo kriptiranja oziroma šifriranja se podatki pred pošiljanjem pretvorijo v nerazumljivo obliko. Le prejemnik z ustreznim ključem za dekriptiranje oziroma dešifriranje jih lahko pretvori v prvotno – izvorno obliko.

Kriptiranje elektronske pošte

Pri kriptiranju elektronske pošte gre za to, da izbranemu naslovniku pošljete elektronsko sporočilo, ga zakodirate z njegovim javnim ključem, naslovnik pa ga lahko odpre s svojim privatnim ključem, ki se nahaja na njegovi pametni kartici. To pomeni, da nihče drug ne more odpreti oziroma prebrati vašega elektronskega sporočila razen naslovnika samega.

Overitelj digitalnih potrdil, glej Certifikatska agencija (CA)

Pametna kartica, ang. smart card

Pametna kartica je kartica z vgrajenim čipom, ki omogoča poleg hranjenja podatkov in potrdil (certifikatov) tudi procesiranje podatkov in izvajanje kriptografskih funkcij na sami kartici.

PIN, ang. Personal Identification Number

Osebna identifikacijska številka iz štirih numeričnih znakov, ki jo že poznamo iz poslovanja na bankomatih in POS terminalih. PIN se uporablja za dostop do privatnega ključa na pametni kartici.

PKI, Public Key Infrastructure, infrastruktura javnih ključev

PKI določa postopke in opremo za generiranje in hranjenje ključev, overjanje imetnikovih ključev in izdajanje digitalnih potrdil javnih ključev, objavljanje digitalnih potrdil (imeniki), preklicevanje digitalnih potrdil, časovno označitev postopkov itd.
Uporablja se za varnejše elektronsko poslovanje pravnih in fizičnih oseb.

POŠTA®CA

Certifikatska agencija POŠTA®CA je overitelj digitalnih potrdil, ki izdaja kvalificirana digitalna potrdila in normalizirana digitalna potrdila, namenjena končnim uporabnikom, ki so lahko fizične osebe, pravne osebe ali strežniški sistemi.

Privatni ključ, ang. private key

Dostop do privatnega oz. zasebnega ključa digitalnega potrdila ima samo imetnik digitalnega potrdila. Privatni ključ uporabljamo za digitalno podpisovanje (overjanje) ter za dešifriranje sporočil, ki so bila šifrirana z našim javnim ključem.

SIGEN-CA

Izdajatelj potrdil za pravne in fizične osebe overitelja potrdil na Centru Vlade za informatiko (CVI). (Angl.: SI, Slovenian, GEN, General, CA, Overitelj).

SIGOV-CA

Izdajatelj potrdil za institucije javne uprave overitelja potrdil na Centru Vlade za informatiko (CVI). (Angl.: SI, Slovenian, GEN, General, CA, Overitelj). Upravitelj kartičnih certifikatov (UKC) Programska oprema, ki nam omogoča rokovanje z digitalnimi potrdili (certifikati) na kartici. Upravitelj kartičnih certifikatov omogoča pregled digitalnih potrdil na kartici, nalaganje in brisanje digitalnih potrdil s kartice ter izvoz javnega ključa digitalnega potrdila.

Zasebni ključ, glej Privatni ključ

10.2 Kratice

AOR – avtomatizirana obdelava receptov
APDU – Aplication Protocol Data Units
CA – Certification Authority
CEN – Comite Europeen de Normalisation / European Committee for Standardization
CI – Compulsory Insurance Data
CRL – Certificate Revocation List
DSS – Digital Signature Standard

ECC - Elliptic Curve Cryptosystems
EF – Elementary File
EMV – Europay, MasterCard, VISA kartica
ESP – Encapsulation Security Payload
ETSI – European Telecommunications Standards Institute
IEC – International Electricity Committee
IIP – Identification of Insured Person
IJK – infrastruktura javnih ključev
IKE (Internet Key Exchange)
IOZ – izbira osebnega zdravnika
IPSec – protokol za šifriranje podatkov v internetu
IP VPN – Internet Protocol Virtual Private Network
IKE – Internet Key Exchange
ISO – International Organization for Standardization
IVZ – Inštitut za varovanje zdravja
KZZ – kartica zdravstvenega zavarovanja
Microsoft IIS – Microsoft Internet Information Server
MJU – Ministrstvo za javno upravo
MTP – medicinsko tehnični pripomoček
NIST – National Institute of Standards and Technology
OASIS – Organisation for the Advancement of Structured Information Standards
OD – Obligator Data
OCF – OpenCard Framework
OTP – One Time Password
OZZ – obvezno zdravstveno zavarovanje
PGP – Pretty Good Privacy
RIP – računalniška izmenjava podatkov
PK – profesionalna kartica
PZZ – prostovoljno zdravstveno zavarovanje
RA – Registration Authority
RSA – agoritem za asimetrično kriptografijo (R. Rivest, A. Shamir in L. Adleman)
SHA in MD5 – zgoščevalni algoritem
SIGEN-CA – kvalificirano digitalno potrdilo za fizične osebe in za poslovne subjekte na MJU
SIGOV-CA – kvalificirano digitalno potrdilo za državne organe na MJU
SI-TSA – izdajatelj varnih časovnih žigov na MJU
SOA – Service Oriented Arhitecture
SSH – Secure Shell
SSL – Secure Socket Layer
SST – Samopostrežni terminal
TC – Technical Comittee

TKS – transakcijsko komunikacijski sistem, ki ga sestavljata dva transakcijsko komunikacijska strežnika in pet varnostnih strežnikov
TLS – Transport Layer Security
TSA – Time Stamp Authority
USB – Universal Serial Bus
ZEPEP – Zakon o elektronskem poslovanju in elektronskem podpisu
ZZZS – Zavod za zdravstveno zavarovanje Slovenije
XML – EXtensible Markup Language
WTLS – Wireless Transport Layer Security

10.3 Slovar tujk

Access Control – kontrola dostopa
Authentication – overjanje
Certification Authority – agencija za izdajo digitalnih potrdil
Certification Policy – dokument v katerem overitelj objavi svoj javni ključ in opiše način varovanja zasebnega ključa
Comite Europeen de Normalisation – Evropska organizacija za standardizacijo
Common Criteria – skupna merila
Compulsory Insurance Data – podatki o obveznem zdravstvenem zavarovanju
Confidentiality – zaupnost
CRL Issuer – upravljalec črne liste digitalnih potrdil
Digest – izvleček
Digital Fingerprint – prstni odtis
End Entity – uporabniki in naprave v arhitekturnem modelu IJK
European Telecommunications Standards Institute – Evropski telekomunikacijski inštitut za standardizacijo
Hash Function – zgoščevalna funkcija
GlobalPlatform – organizacija, ki vzdržuje odprte standarde za uporabo pametnih kartic
Identification of Insured Person – identifikacijski podatki o zavarovani osebi
Integrity – celovitost
International Electricity Committee – Mednarodna elektrotehniška komisija
Link – povezava
Netc@rds – zapis osebnih podatkov zavarovanca in podatkov o veljavnosti zdravstvenega zavarovanja na KZZ za uporabo KZZ v tujini
Nonrepudiation – preprečevanje tajenja
Obligator Data – podatki o zavezancih za prispevek
One Time Password – enkratna gesla
Permissive access – dopusten dostop
Post-issue – dodajanje novih aplikacij na kartice

Registration Authority – center za registracijo ob izdaji kvalificiranih digitalnih potrdil in za izvajanje ostalih administrativnega del
Reset – ponovni zagon
Restrictive access – restiktiven dostop
Template – vzorec
Time Stamp Authority – izdajatelj časovnih žigov
Virtual Private Network – navidezno zasebno omrežje