UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Magistrski študij matematike - izobraževalna smer

Irena Bržan

Kartica zdravstvenega zavarovanja

Projektna naloga

Kriptografija 99/00

Lucija, maj 2000, januar 2002

Kazalo

Uvod

Zavod za zdravstveno zavarovanje Slovenije (ZZZS) je posodobilo listino za izkazovanje zdravstvenega zavarovanja. Zdravstvena izkaznica je bila v Sloveniji v veljavi in uporabi 45 let. Vsebinsko in tehnološko je bila zastarela in funkcionalno neuporabna. ZZZS se je odločila za uvedbo kartice zdravstvenega zavarovanja (v nadaljevanju KZZ) namesto dosedanje zdravstvene izkaznice.

V septembru 1995 je pričel teči projekt o uvedbi KZZ. Od oktobra 1995 do februarja 1998 so potekale analize, oblikovanje kartičnega sistema in priprava na pilotski projekt. Od marca do junija 1998 je potekal pilotni projekt kartičnega sistema v Posavju, nato pa je od junija 1998 do septembra 1999 potekala evalvacija pilotskega projekta in priprava na nacionalno uvedbo kartičnega sistema. Nacionalna uvedba kartičnega sistema je potekala postopno po slovenskih regijah od oktobra 1999 do junija 2000. Oktobra 2000 je kartica zdravstvenega zavarovanja postala edini veljavni dokument za uveljavljanje pravic iz zdravstvenega zavarovanja.

Prednosti uvedenega kartičnega sistema so:

- Boljša kakovost storitev za zavarovane osebe, neodvisnost in samostojnost pri potrjevanju administrativnih podatkov.
- Manj administrativnega in papirnatega dela za zdravstvene delavce, elektronski prenos podatkov na obstoječe obrazce.
- Delodajalcem ni potrebno izdajati in potrjevati zdravstvenih kartic.
- Zdravstvene zavarovalnice imajo večjo kakovost in natančnost podatkov ter s tem omogočene analize.

V prvi fazi je uporaba kartice namenjena predvsem za administrativne naloge:

- identifikacijski dokument,
- potrdilo veljavnosti obveznega in prostovoljnega zdravstvenega zavarovanja oziroma upravičenost imetnika kartice do uveljavljanja pravic iz zavarovanja,
- podatki o izbranih osebnih zdravnikih.

Na KZZ se nahajajo osebni podatki, ki jih je potrebno po Zakonu o varstvu osebnih podatkov ustrezno varovati. Tu najde svoje mesto kriptografija. Pri varovanju dostopa do podatkov na KZZ so uporabljeni kriptografski načini, to je 3DES in PIN.

Kartica zdravstvenega zavarovanja je pametna kartica, zato so v prvem poglavju projektne naloge najprej na kratko predstavljene vrste kartic, pametne kartice in njihov operacijski sistem ter delovanje.

V drugem poglavju je podrobneje predstavljen projekt ZZZS in njegove tehnološke komponente. Glavne tehnološke komponente sistema so:

- kartica zdravstvenega zavarovanja KZZ,
- profesionalna kartica (v nadaljevanju PK),

- čitalniki kartic, povezani z lokalnimi informacijskimi sistemi zdravstvenih delavcev,
- mreža samopostrežnih terminalov za ažuriranje KZZ in
- centralni transakcijsko-komunikacijski strežnik, ki upravlja mrežo samopostrežnih terminalov in jo povezuje z matičnimi podatkovnimi bazami ZZZS.

V tretjem delu projektne naloge je natančneje predstavljena zaščita kartic KZZ in PK. Zaščita sistema KZZ temelji na simetričnem algoritmu 3DES, ki se izvaja v CBC načinu. Podrobneje sta predstavljena simetrična algoritma DES in 3DES ter delovanje CBC načina. Predstavljena je tudi časovna zahtevnost napadov na te algoritme. Ogledali so bomo tudi protokol izmenjave podatkov med KZZ in PK ter možne napade na KZZ in PK.

Na koncu pa je s strani ZZZS ocenjen projekt uvedbe KZZ. Ogledali si bomo oceno pilotske uvedbe v Posavju, ovrednotenje uvedbe KZZ v Sloveniji in ideje o nadaljnjem razvoju KZZ ter povezavo projekta KZZ z drugimi državami ter uporaba zdravstvenih kartic v tujini.

Pametne kartice

Vrste kartic

Kartice so hitro razvijajoča se veja informacijske tehnologije. Konec osemdesetih let so svoj pohod začele magnetne in optične kartice, v devetdesetih pa so jim sledile pomnilniške in mikroprocesorske kartice. Vsaka kartica je sestavljena iz nosilca standardnih dimenzij, na katerega je pritrjen pomnilniški medij. Našteti tipi kartic se razlikujejo glede na medij, ki služi za shranjevanje podatkov. Pri magnetnih karticah je to magnetni trak, pri optičnih se informacije shranjujejo na plasti, ki je občutljiva za laserske žarke. Pri pomnilniških karticah je to čip, pri mikroprocesnih pa mikroprocesor.

Glavna razlika med pomnilniškimi in mikroprocesorskimi karticami je v tem, da ima pomnilniška kartica v osnovi le preprosto varnostno logiko s kontrolo dostopa do pomnilnika pri branju in pisanju (telefonska kartica). Pomnilniške kartice s čipom imajo običajno manj pomnilnika kot mikroprocesorske kartice in izvajajo manjše logične operacije s pomočjo integriranih vezij. Vendar pa te kartice nimajo logike v smislu procesorja in jih zato ne moremo ponovno programirati.

Mikroprocesorska kartica ima vgrajen mikroračunalnik, ki ga je mogoče programirati (primer KZZ). Mikroprocesorska kartica ima visoke zmogljivosti pomnilnika, podatki so varno in dolgotrajno shranjeni, možno je izvajati razne kriptografske funkcije in druge algoritme. Zato mikroprocesorske kartice večkrat imenujemo pametne kartice.

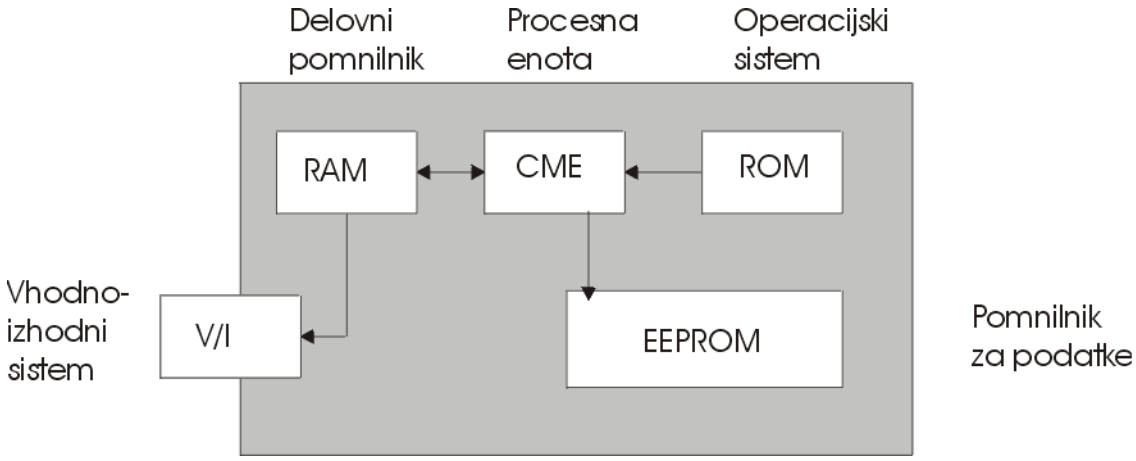
Pametna kartica ima dve značilnosti, ki onemogočata zlorabe in ponarejanje. Ena je obstojen pomnilnik, ki se ga ne da spreminjati in se ohrani tudi po prekinitvi napajanja. Ta pomnilnik lahko vsebuje podatke, ki so bili zapisani po tem, ko je bila kartica izdana, in tako zabeleži vsako spremembo. Druga značilnost pa je procesor kartice, ki nadzira vse interakcije med raznimi zunanjimi napravami, ki berejo kartico in pišejo nanjo, in pomnilnikom pametne kartice. Pomnilnik kartice je oblikovan tako, da je fizično in logično dostopen le izdajatelju kartice.

Raba imena pametne kartice ni dosledna, včasih se uporablja le za mikroprocesorske kartice, včasih pa za mikroprocesorske in pomnilniške kartice skupaj. V tem projektu bomo naziv pametne kartice uporabljali le v ožjem smislu smo za mikroprocesorske kartice.

Sestava pametnih kartic

Čip, ki je vgrajen v mikroprocesorsko kartico, je kot majhen računalnik. Vsebuje naslednje komponente:

- centralna mikroprocesorska enota (procesor),
- pomnilniki,
- vhodno-izhodni sistem.



Centralna mikroprocesorska enota ali procesor ima dve osnovni funkciji. Procesor obdeluje in prikazuje podatke. Operacijski sistem odloča, kje bodo shranjeni podatki in v kakšnih okoliščinah se bo izvedel prenos podatkov prek vhodno-izhodne enote. Procesor lahko vsebuje tudi kripro-koprocesorje za hitro kodiranje ali dekodiranje. V uporabi so 8, 16 in 32 bitni procesorji. Procesorji temeljijo na Motoroli 6805 in Intelu 8051, hitrosti do 5 MHz.

Pametna kartica mora imeti obstojen pomnilnik, ki hrani podatke (podatki se ne izgubijo po prekinitvi napajanja). Imeti mora tudi pomnilnik, kamor se vpisujejo sprotne informacije. Na splošno ima pametna kartica tri vrste pomnilnikov:

- ROM - trajni pomnilnik (Read Only Memory). Vanj je tovarniško trajno naložen kartični operacijski sistem. Ni ga možno naknadno spreminjati.
- RAM - delovni pomnilnik (Random Access Memory). Shranjuje začasne informacije med delovanjem procesorja. Za svoje delovanje potrebuje zunanji vir napetosti. Običajne velikosti so med 128 in 512 bitov.
- PROM- programabilni bralni pomnilnik. PROM se deli na EPROM - izbrisljivi programabilni bralni pomnilnik in EEPROM - bralno-pisalni pomnilnik (Electronically Erasable Programmable Read Only Memory). EPROM se uporablja za trajno shranjevanje uporabnikovih podatkov na pametni kartici. Podatke je mogoče le pisati in ne brisati. EEPROM pa se uporablja za shranjevanje programov in podatkov, ki se periodično spreminjajo. Opravlja podobno funkcijo, kot jo ima trdi disk na PC-ju. Navadno zavzema največ prostora na čipu, je največji porabnik energije ter je tudi najdražji od vseh pomnilnikov. Prenese med 10.000 do 500.000 ciklov pisanja. EEPROM se

lahko uporabi tudi za shranitev dopolnilnega kartičnega operacijskega sistema.

Nobeden od naštetih pomnilnikov ni dostopen neposredno. Vsak zunanji dostop gre preko procesne enote ter varnostne logike.

PROM je razdeljen na tri področja. V tajnem področju so shranjeni podatki, ki jih uporablja samo procesor, recimo lastnikovo geslo. V odprtem področju so shranjeni podatki, ki jih lahko preberemo s čitalniki, a jih ne moremo spreminjati, recimo priimek in ime lastnika. V delovnem področju pa je zapis podatkov, ki jih je potrebno spreminjati, recimo izdani recepti.

Čip mikroprocesorske kartice lahko vsebuje dodatne elemente (kontrolne enote za nadzor napetosti, ure ...) in varnostno logiko (dostop do pomnilnikov, generator naključnih števil, matematični koprocesor za izvajanje raznih kriptografskih algoritmov).

Vmesnike pametne kartice delimo na kontaktne in brezkontaktne. Pri kontaktnih karticah je vmesnik med čipom in zunanjim svetom kontaktna plošča s šest ali osem kontakti, ki prekriva čip. Brezkontaktna kartica nima neposrednega kontakta. Podatke in energijo prenaša na več načinov, na primer z induktivnim sklopom, z mikrovalovnim sklopom.

Kartični operacijski sistem in njegova varnost

Operacijski sistem je nekak posrednik med strojno opremo in aplikacijskim programiranjem. Gre za skupino sistemskih programov in nanje navezanih ukazov. Kartični operacijski sistem se ne more primerjati z obširnimi večopravilnimi sistemi na večjih računalnikih. Nima dela za komunikacijo z uporabnikom, vedno komunicira le z računalnikom. Glavni nalogi kartičnega operacijskega sistema sta varno izvajanje programov ter nadzor dostopa do podatkov.

Količina programske kode je zelo majhna (približno 10 kB). Praviloma je koda spravljena v ROM-u. Tja se trajno shrani že med proizvodnjo čipa, kasnejše spremembe niso možne. Zato mora biti kartični operacijski sistem celovit in praktično brez napak. Mnogo časa se posveča testiranju in odpravi napak. Zaradi majhne procesorske moči in omejenih pomnilniških kapacitet pa mora ustrezati še naslednjim zahtevam: mora biti hiter pri izračunih, optimiziran glede porabe pomnilnika.

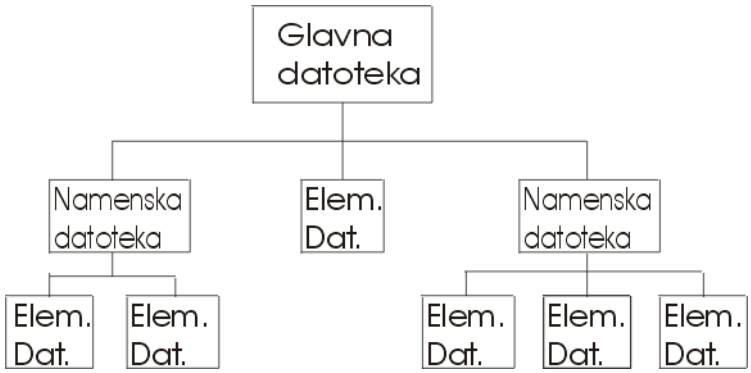
Vsi operacijski sistemi dopuščajo, da se posamezne njegove funkcije naložijo v EEPROM, ki sicer služi za shranjevanje podatkov.

Proizvajalci procesorjev opremijo čip z okleščenim operacijskim sistemom z minimalnim naborom ukazov in funkcij, potrebnih za upravljanje z mikroračunalnikom. Ta nabor ukazov proizvajalci kartic razširijo z lastnimi ukazi. Iz enega čipa tako lahko nastane več različnih kartic, vsaka opremljena z drugačnim operacijskim sistemom.

Proizvajalčevim specifičnim ukazom so dodatni ukazi za zagotavljanje varnosti (preverjanje obojestranske identitete), ukazi za ravnanje z datotekami. Podrobnosti operacijskih sistemov so skrbno varovane skrivnosti. Uveljavljeni kartični operacijski sistemi se naslanjajo na standard ISO 7816-4, ki temelji na datotečni organizaciji podatkov v EEPROM-u.

Strukturo datotek v EEPROM-u določa standard ISO 7816-4. Struktura je hierarhična, drevesna, povsem podobna DOS-ovi strukturi. Sestavljajo jo naslednji tipi datotek:

- Glavna datoteka (Master file): vsebuje vse druge datoteke in imenika. Obsega ves razpoložljivi prostor za datoteke.
- Namenska datoteka (Dedicated file) je datoteka v vlogi imenika, je nekakšna višja organizacijska enota, vanjo so naložene sorodne elementarne datoteke ali imeniki.
- Elementarna datoteka (Elementary file) je datoteka s podatki.



Število nivojev v datotečnem drevesu je poljubno, omejuje ga razpoložljiva velikost EEPROM-a.

Varnostna shema, ki jo podpira kartični operacijski sistem, vsebuje pristopne mehanizme, pristopne pogoje in varnostni status.

Pristopni mehanizmi so ukazi, ki spreminjajo varnostni status in s tem omogočajo delo z datotekami. To so naslednji mehanizmi:

- identifikacija lastnika: preverjanje, ali je kartica v rokah lastnika, prek poznavanja osebne kode PIN (personal identification number),
- overjanje zunanjega okolja: preverjanje, ali kartico bere pravo okolje, okolje dokaže poznavanje šifrirnega ključa,
- overjanje kartice: okolje preveri, ali kartica pozna šifrirni ključ.

Pristopni pogoji do posamezne datoteke določajo predpogoje, ki morajo biti izpolnjeni, preden se lahko nad datoteko izvedejo ukazi. Pristopni pogoji so zapisani v glavi datoteke in so trajni. Odvisni so od tipa datoteke ter zaupnosti podatkov v datoteki. Do datotek dostopamo z različnimi zunanjimi ukazi (npr. branje, pisanje, iskanje, brisanje, dodajanje ...). Pristopni pogoji so zapisani za vsak ukaz posebej. Dostop do posamezne datoteke s posameznim ukazom je lahko prost, omejen s pristopnim mehanizmom (geslom ali ključem), ali pa prepovedan.

Varnostni status predstavlja stanje po izvedenem pristopnem mehanizmu. Status je vezan na glavno datoteko in namensko datoteko. Dostop do podatkov v elementarni datoteki je omejen s pristopnimi pogoji na enak način kot pri glavni in namenski datoteki.

Varnostna shema temelji na preprosti logiki: če trenutni varnostni status ustreza zahtevanim pristopnim pogojem, je omogočen dostop do datotek in izvedba nadaljnjih ukazov, kot so branje, pisanje, prehod v nižji hierarhični nivo po datotečnem drevesu. Niže lahko gremo le, ko zadovoljimo pogoje na višjem nivoju. V varnostno shemo sodita še dva varnostna mehanizma, ki služita za varen prenos podatkov. To je zagotavljanje celovitosti podatkov (preverjanje, ali se je kak del pri prenosu izgubil) in zagotavljanje zaupnosti podatkov (preprečevanje branja podatkov tretji osebi se zagotovi s šifriranjem s simetričnim ali asimetričnim algoritmom).

Primer:
Pametna kartica vsebuje elementarno datoteko, v kateri so navedeni ključi za identifikacijo in prepoznavanje okolja. Kartica omogoča dostop do te datoteke le pri identifikaciji in pri preverjanju okolja (protokol za izmenjavo podatkov). Branje take datoteke pa nikoli ni mogoče. Če bi napadalec rad prišel do podatkov, ki so zapisani v datoteki s ključi, lahko to stori posredno, to je z napadi na šifrirni sistem, pri katerem se uporabljajo ti ključi. Obstajajo tudi mehanski napadi na kartico (finamehanika…). Nekatere pametne kartice imajo vgrajene obrambne mehanizme, ki pri mehanskih napadih uničijo podatke, ki so shranjeni na kartici (samouničenje kartice).

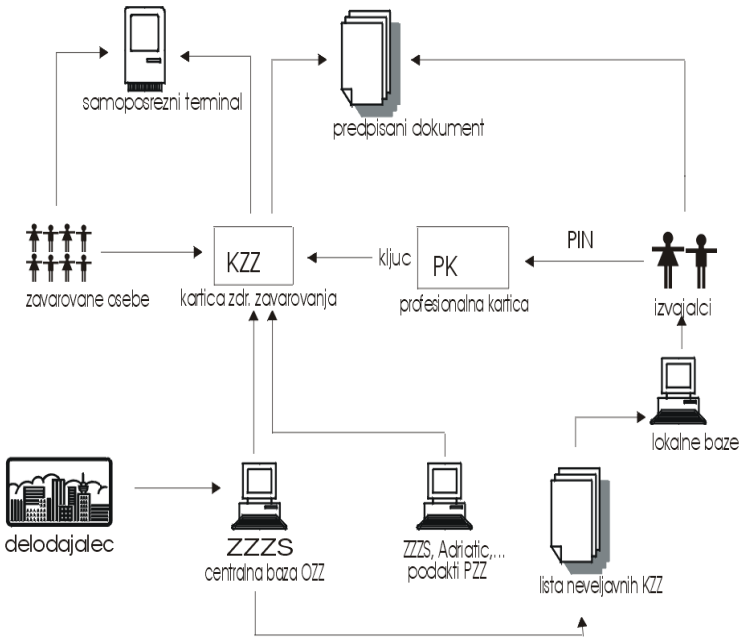
Sistem KZZ

Struktura sistema KZZ

Glavne tehnološke komponente sistema so:

- kartica zdravstvenega zavarovanja (KZZ),
- profesionalna kartica (PK),
- čitalniki kartic, povezani z lokalnimi informacijskimi sistemi zdravstvenih delavcev,
- mreža samopostrežnih terminalov za ažuriranje KZZ,
- centralni transakcijsko-komunikacijski strežnik, ki upravlja mrežo samopostrežnih terminalov in jo povezuje z matičnimi podatkovnimi bazami ZZZS.

Struktura sistema KZZ je prikazana na spodnji sliki.



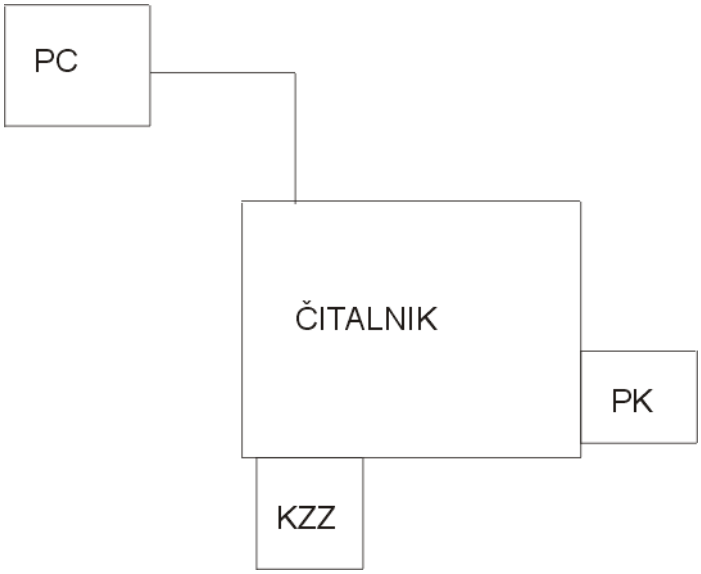
Zavarovanci ažurirajo KZZ v samopostrežnih terminalih, ki so na voljo v vseh zdravstvenih ustanovah in izpostavah ZZZS. Mreža samopostrežnih terminalov je povezana s centralno bazo ZZZS, v kateri se podatki sproti ažurirajo. Zavarovanci KZZ v bolnišnici, pri zdravniku ali v lekarni predložijo svojo kartico. Iz nje pooblaščena oseba s pomočjo svoje profesionalne kartice (PK) preko čitalnika prebere podatke. Čitalnik je povezan z lokalnim informacijskim sistemom zdravstvenih delavcev, na katerem je lista neveljavnih KZZ.

Žal pa v vsej literaturi (ki je navedena na koncu projektne naloge) o sistemu KZZ ni podatkov o povezavah, ki iz kartice PK izhajajo v centralno bazo podatkov ZZZS. Z vpeljavo elektronskega recepta, bi bilo smotrno dvojno preverjanje podatkov:
Na KZZ so zapisani podatkih o predpisanih receptih za zdravila. Ti podatki so zapisani tudi v centralni bazi ZZZS. Da bi preprečili zlorabo predpisanih receptov s strani imetnika KZZ, bi morali imeti tudi povezavo med PK in centralno bazo podatkov ZZZS. Recepte, ki jih predpiše imetnik PK, bi morali poslati v centralno bazo podatkov ZZZS. Centralna baza ZZZS bi preverjala podatke zapisane na KZZ s podatki, ki jih je poslal imetnik PK. Če bi se podatki ujemali, potem bi vedeli, da ni bilo zlorabe predpisanih receptov s strani imetnika KZZ.

Dobavitelji in proizvajalci opreme, ki sodelujejo pri tem projektu, so:

- ZZZS je nosilec projekta,
- Projektna pisarna dr. Peter DEBOLD: sodelovanje pri načrtovanju sistema kartice zdravstvenega zavarovanja,
- GMD (German National Research Center for Information Technology) za pripravo tehničnih specifikacij za kartice in čitalnike, nadzor kakovosti dobavljenega blaga
- GEMPLUS INTERNATIONAL za kartice in čitalnike kartic (Cetis d.d. - personalizacija kartic, tiskana gradiva; Plasis d.o.o. - personalizacija kartic)
- SIEMENS d.o.o. za samopostrežne terminali in centralni transakcijski strežnik (Logina d.o.o. - terminali tipa SST2 in SW za samopostrežne terminale)
- NIL d.o.o.: omrežje samopostrežnih terminalov
- TELEKOM Slovenije: telekomunikacijska infrastruktura za omrežje samopostrežnih terminalov
- METRA INŽENIRING d.o.o.: izdelava programskih vmesnikov
- INŠTITUT JOŽEF STEFAN: zasnova in nadzor varnostne sheme

Dostop do podatkov na kartici KZZ je zavarovan s sistemom varovanja, katerega temeljna komponenta je profesionalna kartica kot ključ za dostop podatkov.

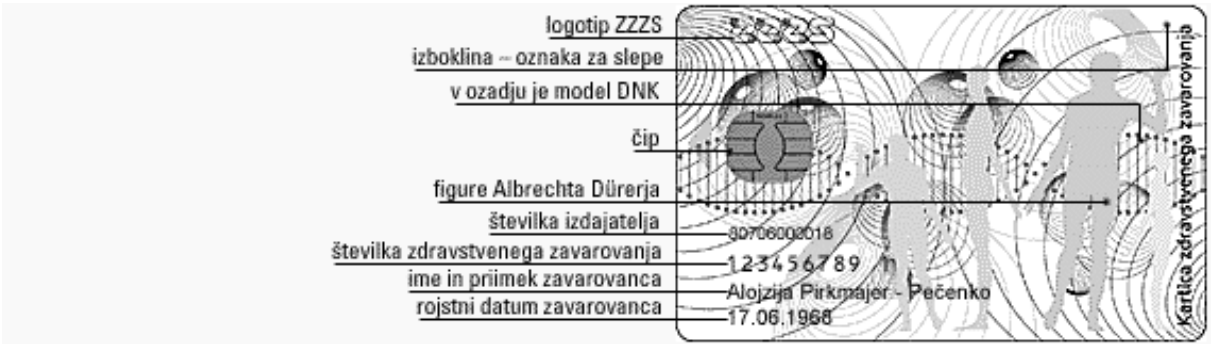


Tehnološke komponente sistema KZZ

Kartica zdravstenega zavarovanja

Kartica zdravstvenega zavarovanja je kontaktna mikroprocesorska kartica z mikroprocesorjem tipa ID-1, ki ima 16 kB pomnilnika EEPROM. Fizikalne karakteristike kartice ustrezajo standardu ISO/IEC 7816-1, dimenzije in lokacija kontakta pa standardu ISO/IEC 7816-2. Kartica je velika 85,6 x 54 mm.

Na KZZ je vidno izpisano ime in priimek zavarovanca, datum rojstva, številka zavarovanja ter ime izdajatelja. Izbočen krogec v zgornjem desnem kotu je namenjen slepim.

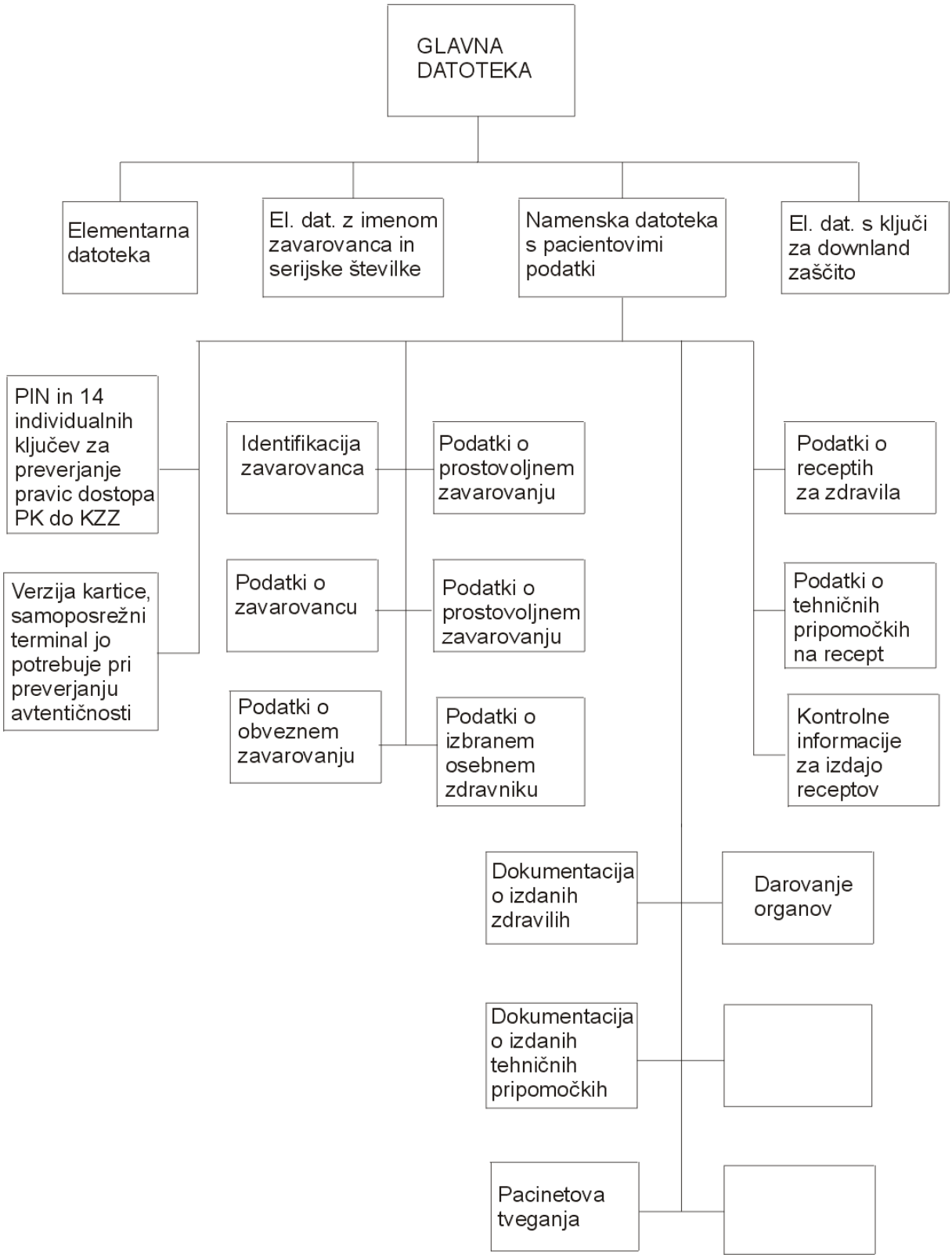


V mikroprocesorju KZZ so shranjeni podatki, ki jih je možno prebrati le s čitalnikom ob sočasni uporabi profesionalne kartice. Tako so zaščiteni pred nepooblaščenim vpogledom. To so naslednji podatki:

- o zavarovancu (ime in priimek, naslov, spol, datum rojstva...),
- o zavezancu za prispevek (registracijska številka, ime oziroma naziv, naslov...),
- o obveznem zdravstvenem zavarovanju (datum potrjevanja in veljavnost zavarovanja),
- o prostovoljnem zdravstvenem zavarovanju (vrsta police, datum potrjevanja in veljavnost zavarovanja),
- o izbranem osebnem zdravniku (splošnem zdravniku/pediatru, zobozdravniku, ginekologu).

Kartica je nosilec prepisa podatkov iz centralnih baz. Ob potrjevanju na samopostrežnih terminalih se iz centralne baze vpišejo na kartico najnovejši podatki. Na kartici ni nobenih medicinskih podatkov. Gre torej za nabor podatkov, ki jih pooblaščene osebe uporabljajo izključno v administrativne namene.

Struktura datotek v KZZ je prikazana na spodnji sliki:



V elementarni datoteki s ključi je zapisan PIN lastnika KZZ in individualni ključi za preverjanje pravic dostopa PK do KZZ.

Lastnik kartice KZZ ima možnost, da zavaruje dostop do določenih datotek na KZZ. Zavarovanec mora vnesti svoj PIN, preden se lahko preberejo ali spreminjajo podatki v datoteki. Za enkrat je ta možnost le pri datoteki o izdanih zdravilih.

V elementarni datoteki s ključi je še 14 individualnih ključev za preverjanje pravic dostopa PK do KZZ. To so individualni ključi za preverjanje:

1. avtentičnosti KZZ,
2. pravic dostopa za uslužbence obveznega zdravstvenega zavarovanja,
3. pravic dostopa za uslužbence dodatnega zdravstvenega zavarovanja,
4. pravic dostopa za uslužbence dodatnega zdravstvenega zavarovanja družbe Adriatic,
5. pravic dostopa za zdravnike s koncesijo, ki so lahko izbrani kot osebni zdravniki in imajo svoj digitalni podpis,
6. pravic dostopa za ostale zdravnike z ali brez koncesije, ki imajo svoj digitalni podpis in ne morejo biti izbrani kot osebni zdravniki,
7. pravic dostopa za zdravniško osebje: sestre in administrativno osebje v zdravnikovi ordinaciji,
8. pravic dostopa za ostale zdravstvene delavce (fizioterapevte, logopede ipd.)
9. pravic dostopa za zdravnike na intenzivni negi,
10. pravic dostopa za farmacevte z digitalnim podpisom,
11. pravic dostopa za farmacevtsko osebje v lekarni,
12. pravic dostopa za dobavitelje tehničnih pripomočkov (privatnih podjetji pogodbeno vezanih na ZZZS),
13. pravic dostopa za osebje obveznega in prostovoljnega zavarovanja na regionalnih enotah,
14. pravic dostopa za samopostrežne terminale.

Ti kriptografski ključi so dolgi 16 bytov = 16*8 bitov = 128 bitov in se uporabljajo v 3DES enkripciji - dekripciji v CBC načinu. 3DES se izvaja po protokolu ANSI X9.17 (v zaporedju enkripcija - dekripcija - enkripcija). Ključ za preverjanje KZZ mora biti implicitno izbran, ključ za preverjanje pravic dostopa PK do KZZ pa mora biti izbran eksplicitno. Ker imamo le en kriptografski algoritem (3DES), mora biti ta algoritem implicitno izbran. Vseh 14 ključev v KZZ je specifičnih (individualnih) za KZZ. Dobimo jih s pomočjo skupinskih ključev PK, skupinskega (master) ključa za preverjanje KZZ in serijske številke KZZ.
3DES algoritem je podrobneje opisan v naslednjem poglavju Zaščita sistema KZZ.

Profesionalna kartica

Profesionalna kartica je prav tako kontaktna mikroprocesorska kartica s 8 kB pomnilnika EEPROM. Fizikalne karakteristike kartice ustrezajo standardu ISO/IEC 7816-1, dimenzije in lokacija kontakta pa standardu ISO/IEC 7816-2. Kartica je velika 85,6 x 54 mm.

Izdana je pooblaščenim osebam (zdravnikom, medicinskim sestram, administrativnim delavcem v sprejemnih pisarnah, farmacevtom, fizioterapevtom, uslužbencem zavarovalnice…) v skladu z njihovimi pooblastili in pravicami dostopa.

Profesionalna kartica ima vidno zapisane podatke, prikazane na spodnji sliki, Osnovna motiva kartice sta podoba Hipokrata in tekst iz Hipokratove prisege.

V mikroprocesorju profesionalne kartice so zapisani naslednji podatki: ZZZS številka imetnika kartice, številka izvoda kartice, ime in priimek imetnika, poklic, šifra države, IVZ številka, specializacija, tip pooblastila. Če imetnik kartice ni zdravnik, pa so na kartici še naslednji podatki: šifra države pooblaščene pravne osebe, IVZ številka pooblaščene pravne osebe, naziv pooblaščene pravne osebe.

V datoteki s ključi so zapisani:

a) skupinski (master) ključ za preverjanje KZZ,

b) skupinski ključ, ki pripada imetniku PK glede na njegovo profesionalno delo. Glede na status imetnikov PK so profesionalne kartice razdeljene na več tipov, ki se med seboj razlikujejo po ključih dostopa. Svoj skupinski ključ imajo

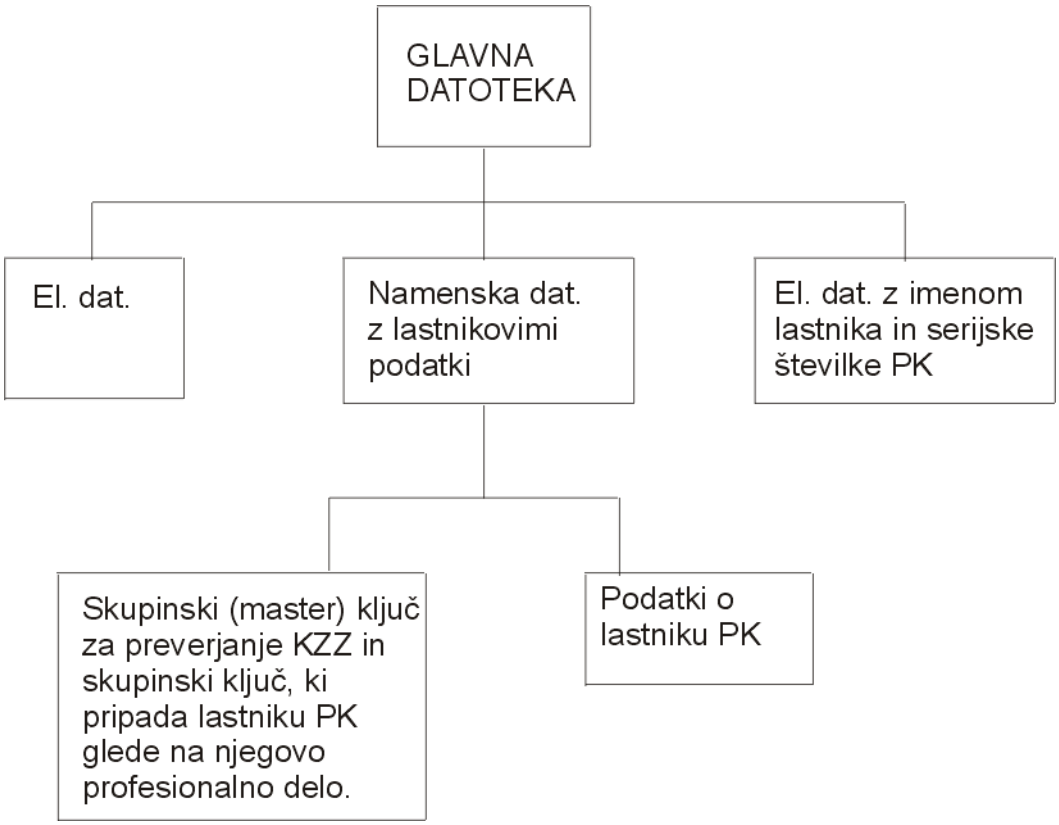
- uslužbenci ZZZS,
- uslužbenci prostovoljnega zdravstvenega zavarovanja 1,
- uslužbenci zdravstvenega prostovoljnega zavarovanja 2,
- izbrani osebni zdravnik s pogodbo,
- ostali zdravniki,
- medicinske sestre,
- ostali zdravstveni delavci (fizioterapevti),
- zdravnik intenzivne nege,
- farmacevti,
- farmacevtsko osebje,
- dobavitelji tehnične pomoči,

- uslužbenci obveznega zavarovanja in
- samopostrežni terminal

Ti kriptografski ključi so dolgi 16 bytov = 16*8 bitov = 128 bitov in se uporabljajo v 3DES enkripciji - dekripciji v CBC načinu. 3DES se izvaja po protokolu ANSI X9.17 (v zaporedju enkripcija - dekripcija - enkripcija). Ti ključi so izbrani implicitno, kakor tudi kriptografski algoritem (3DES).

c) PIN uporabnika PK in koda za odblokiranje. PIN je sestavljen iz štirih cifer, koda za odblokiranje pa je sestavljena iz osmih cifer.

Struktura datotek v PK je prikazana na spodnji sliki:



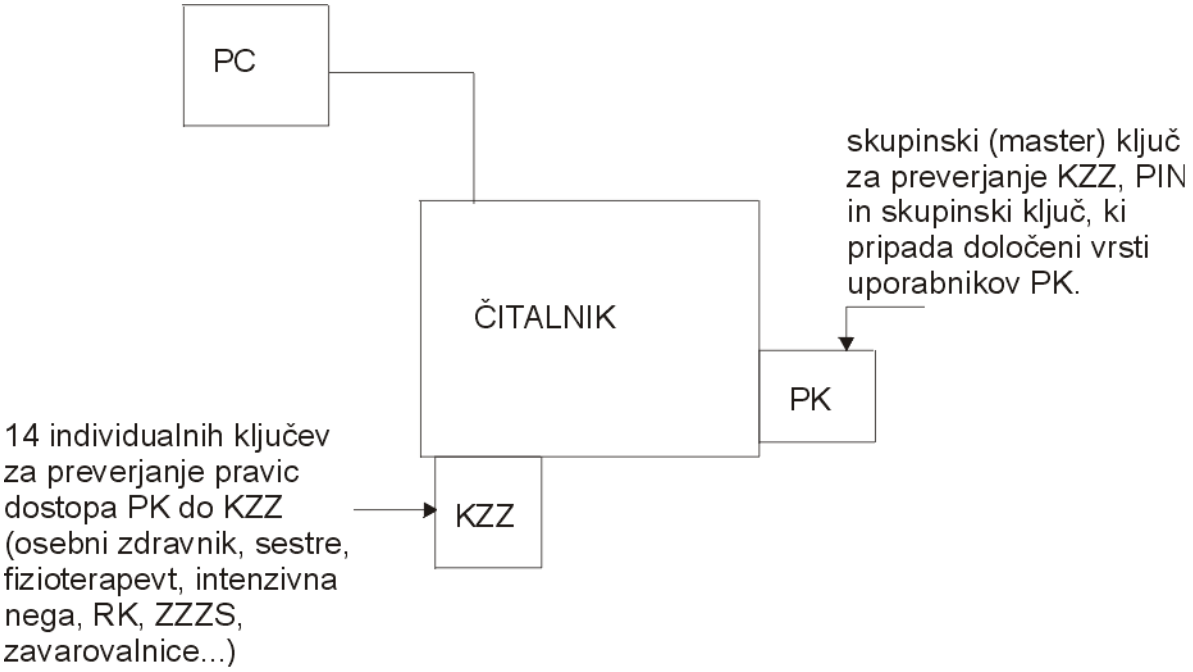
V prihodnosti bo profesionalna kartica tudi nosilec elektronskega podpisa imetnika kartice (za izdajo receptov, ...).

Čitalniki kartic

V sistemu KZZ nastopa več vrst čitalnikov:

- čitalnik kartic v zdravstveni ustanovi, priključen na lokalni informacijski sistemi,
- prenosni čitalnik kartic za delo zdravnikov na terenu,
- čitalniki kartic v samopostrežnih terminalih.

Čitalnik kartic ima dve vtični mesti: za KZZ in za PK. Ima dvovrstični prikazni zaslon s po 16 znaki v vrsti, tipkovnico z 16 tipkami, LED diode za prikaz stanj oziroma napak.



Samopostrežni terminali

Samopostrežni terminali primarno služijo za ažuriranje podatkov o zavarovanju na KZZ. Terminali so nameščeni v zdravstvenih ustanovah in izpostavah ZZZS, tako zavarovanci podaljšanje zavarovanja opravijo ob samem obisku zdravstvene ustanove.

Poleg primarne funkcije ažuriranja kartic nudijo terminali tudi možnosti širših rab, npr. kot večpredstavni informacijski kioski. Terminali so dostopni vsem zavarovancem ves delovni dan (od 6h do 22h).

Posebna funkcija samopostrežnih terminalov pa je tudi nalaganje novih naborov podatkov in aplikacij na že izdane kartice ob širjenju funkcij sistema.

V sistemu nastopata dva tipa samopostrežnih terminalov, zmogljivejša SST1 in enostavnejša verzija terminala SST2.

Konfiguracija terminala SST1 je naslednja:

- Strojna oprema: PC kompatibilni računalnik, 32 MB RAM, disk 1,2 GB, 17-palčni ekran občutljiv na dotik, ločljivost 1024x768 pik, zvočna kartica in zvočniki, MMX tehnologija za predvajanje video filmov, 2 serijska priključka, komunikacijska kartica, sistem UPS avtonomije za 5 minut.
- Programska oprema: programsko nastavljivi WDOG, operacijski sistem Windows NT, komunikacijska oprema za povezavo z vgrajenim čitalnikom kartic, programska oprema za povezavo s centralnim strežnikom, programska oprema za upravljanje zaslona, programska oprema za nadzor delovanja terminala in statistične obdelave.

Konfiguracija terminala SST2 je v osnovi enaka. Terminal SST2 je namenjen izključno ažuriranju KZZ.

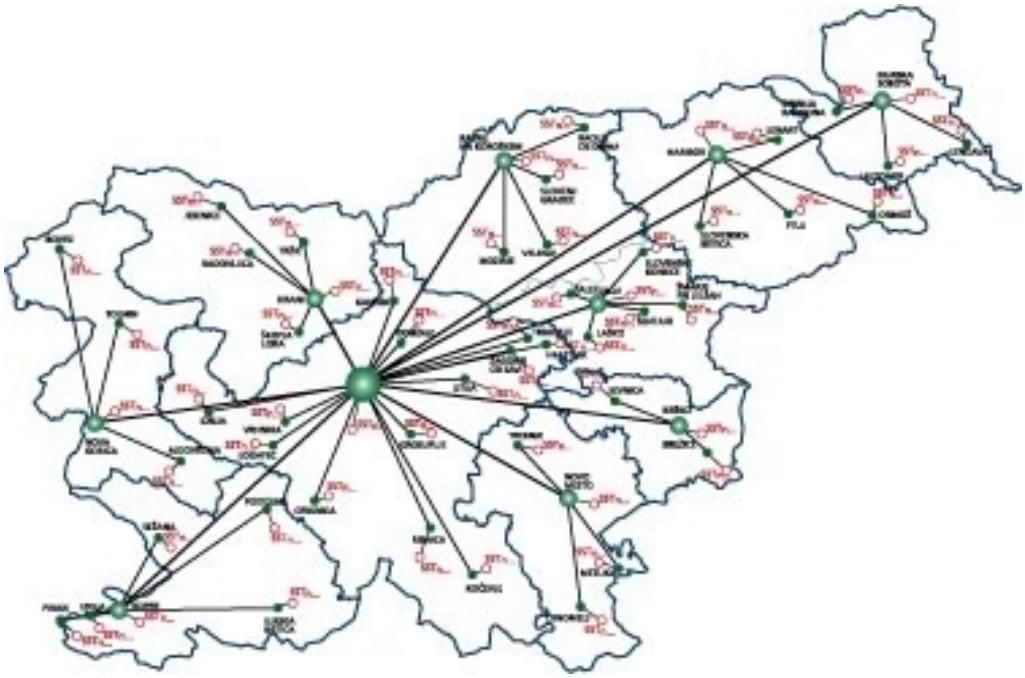
Centralni transakcijsko-komunikacijski strežnik in omrežje

Centralni transakcijsko-komunikacijski strežnik upravlja delovanje omrežja samopostrežnih terminalov in služi kot čelno vozlišče tega omrežja za povezavo s podatkovnimi strežniki zavarovalnice.

Na ZZZS je ta strežnik večprocesorski računalnik interoperabilnega tipa, s protokoli za komuniciranje z omrežnimi okolji TCP/IP, Intranet, Internet, SNA, OSI, ATM, X.25, FR, ter operacijskimi sistemi MVS, UNIX, OS/2, Windows NT in Windows 95. Strežnik deluje neprekinjeno (režim 24 x 365).

Omrežje samopostrežnih terminalov je zgrajeno na komunikacijski infrastrukturi ZZZS (povezave med izpostavami, območnimi enotami in informacijskim centrom ZZZS v Ljubljani) ter infrastrukturi Centra Vlade za informatiko.

Mreža samopostrežnih terminalov v Sloveniji (275 terminalov):



Zaščita sistema KZZ in PK

Simetrični algoritem 3DES v CBC načinu

Pri varovanju podatkov na KZZ je uporabljen simetrični algoritem 3DES.

Simetrični algoritem je kriptografski algoritem, ki uporablja isti ključ za šifriranje in za odšifriranje. Primer: Anita in Bojan se dogovorita za skupni ključ, ki ga ne pozna nihče drug (pogoj je, da si zaupata). Če Bojan s skupnim ključem zašifrira pismo, je prepričan da ga lahko odšifrira le Anita. Hkrati pa je tudi Anita zadovoljna, saj je prepričana da pismo izvira od Bojana.

DES (Data Encryption Standard) je najbolj znan in sploh prvi komercialni simetrični kriptosistem. Zasnovan je bil v šestdesetih letih pri IBMu.
Dolžina ključev je 64 bitov. Od teh 64-tih bitov je vsak osmi bit parity check bit, teh osem bitov služi za preverjanje ključa. Torej so ključi dolgi 56+8 bitov. DES deluje na 64-bitnih blokih čistopisa.

Simetričen algoritem DES je blokovni simetrični šifrirni sistem. Sporočilo (čistopis) razbije na določeno dolžino blokov (pri DESu so bloki dolgi 64 bitov), nato pa vsak blok preoblikuje in kombinira s ključem. Permutacije, substitucije in kombinacije bloka s ključem morajo zagotoviti, da so v izhodnem bloku (tajnopisu) zabrisani vsi vzorci iz vhodnega bloka čistopisa.

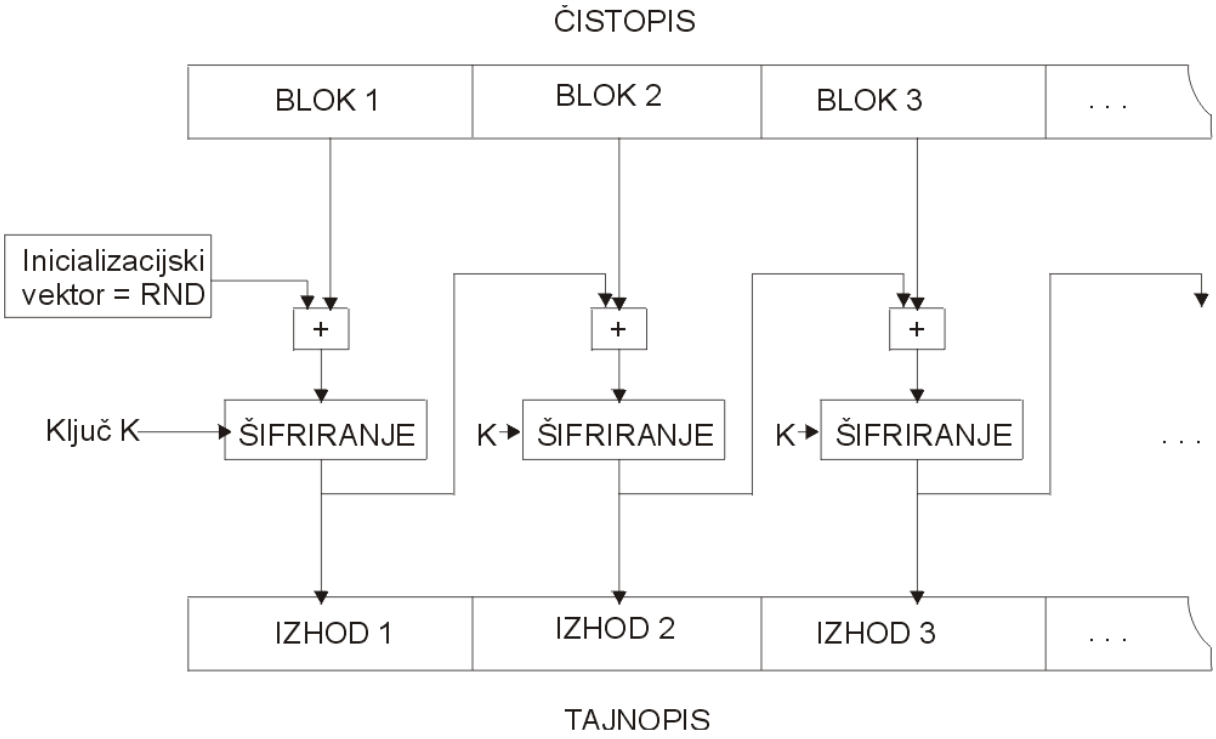
Algoritem DES lahko deluje na štiri različne načine (načini povezovanja blokov):

- EBC način (elektronska kodirna knjiga),
- CBC način (kodirno blokovno veriženje),
- CFB način (kodirna povratna zanka) in
- OFB način (izhodna povratna zanka).

Ker se v varovanju prenosa podatkov iz KZZ v PK uporablja algoritem 3DES v CBC načinu, si bomo podrobneje ogledali delovanje CBC načina.

Pri CBC načinu se čistopis razbije na 64 bitov dolge bloke, nato pa se vsak blok posebej preoblikuje in kombinira s ključem.

Začetni blok sporočila se z logično operacijo XOR sešteje z naključnim številom (pravimo mu inicializacijski vektor). Dobljen blok algoritem 3DES zašifrira in ga postavi na začetek zašifriranega sporočila (tajnopisa). Vsak naslednji blok čistopisa se sešteje z zašifriranim prejšnjim blokom in se zašifrira s 3DES algoritmom ter postavi na drugo mesto v tajnopisu itd.



Šifriranje z DESom je zasnovano na dveh splošnih konceptih: produktni tajnopisi in Feistelovi tajnopisi.

- Produktni tajnopis dobimo s komponiranjem več enostavnih operacij, z namenom, da povečamo varnost. Te operacije so: transpozicije, XOR, tabele, linearne transformacije, aritmetične operacije, modularno množenje, enostavne substitucije.
- Feistelov tajnopis pa dobimo tako, da v večih krogih (rundah) obdelujemo začetni blok.

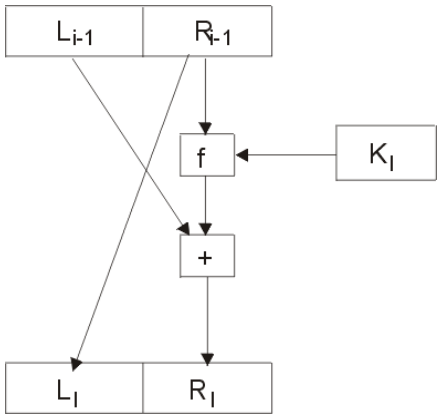
Pri šifriranju z DESom uporabljamo enostavne operacije, kot so permutacije, razširitvene funkcije. Algoritem DES se izvaja v 16-tih krogih. Iz danega ključa K, dolgega 56 + 8 bitov, s permutacijami generira šestnajst podključev K_1, K_2, …, K_{16}., dolgih 48 bitov. Algoritem DES v i-tem krogu uporabi podključ K_i.

Algoritem DES čistopis razdeli na bloke, dolge 64 bitov. DES blok čistopisa najprej permutira z inicializacijsko permutacijo IP in ga nato razdeli na dva bloka po 32 bitov, na L_0 in R_0. Nato opravi 16 krogov šifriranja (v zadnjem krogu ni zamenjave strani blokov, ni tako kot na sliki) in dobljeni blok (L_{16}, R_{16}) premutira z inverzno permutacijo IP^{-1}.

V i-tem krogu DESa izgleda takole:

$$(L_{i-1}, R_{i-1}) \rightarrow (L_i, R_i)$$
$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

Funkcija f je produktni tajnopis, ki ni nujno obrnljiv.



Leta 1996 so kriptografi M. Blaze, R. Rivest, B. Schneier, T. Shimomura, E. Thompson in M. Wiener predlagali minimalne dolžine ključev, potrebnih za varen simetričen (recimo DES) kriptosisteme. Da bi zagotovili ustrezno zaščito pred najbolj resnimi grožnjami (npr. velike komercialne ustanove ali vladne agencije) mora biti ključ dolg vsaj 75 bitov. Da bi zagotovili ustrezno zaščito za naslednjih 20 let, morajo biti ključi dolgi vsaj 90 bitov. Torej so ključi, ki se uporabljajo pri DES algoritmu (56 bitov) prekratki, če želimo zagotoviti dobro varnost sistema.

V spodnji tabeli je predstavljen povprečen čas za napad z grobo silo (ocene so glede na tehnologijo leta 2000).

dožina ključa v bitih	posameznik z enim PC	majhna skupina, 16 PC-jev	raziskovalna omrežja, 256 PC-jev	veliko podjetje	vojaške obveščevalne službe
40	dnevi	ure	minute	milisekunde	mikrosekunde
56	leta	tedni	dnevi	minute	milisekunde
64	tisočletja	stoletja	desetletja	ure	sekunde
80	∞	∞	tisočletja	stoletja	dnevi
128	∞	∞	∞	∞	∞

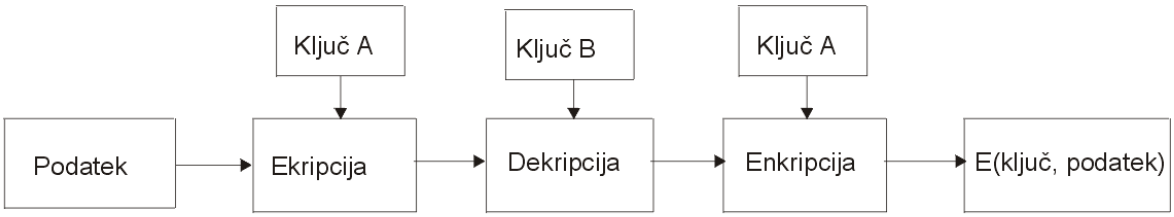
Posameznik, ki ima en sam PC in programsko opremo lahko na sekundo preveri 2^{20} do 2^{28} možnih ključev. Z majhno skupino PC-jev (recimo 16) lahko na sekundo preverimo 2^{24} do 2^{32} možnih ključev. Raziskovalna omrežja (256 PC-jev) lahko na sekundo preverijo 2^{28} do 2^{36} možnih ključev. Veliko podjetje z milijon dolarjev vredno opremo lahko preveri 2^{48} možnih ključev na sekundo. Velike vojaške obveščevalne organizacije pa lahko preverijo 2^{60} možnih ključev na sekundo.
Za dobro varnost mora biti dolžina ključa več kot 80 bitov, idealno okoli 120 bitov.

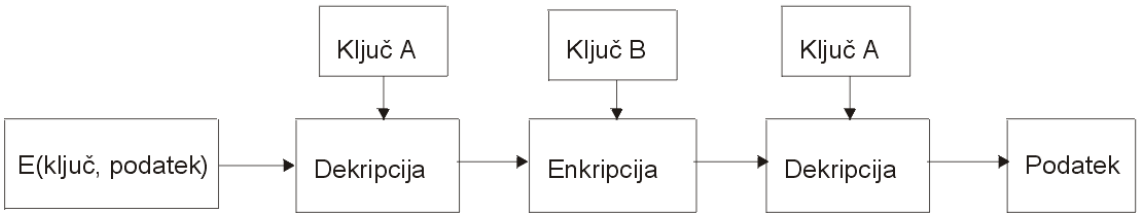
Problem prekratkega ključa simetričnega algoritma DES rešimo tako, da uporabimo DES trikrat zapored (šifriranje – odšifriranje – šifriranje) in dobimo trojni DES oz. 3DES algoritem.

Obstaja več variant 3DES algoritma, ki se razlikujejo glede na število porabljenih ključev.

- Pri vsaki ponovitvi DESa lahko uporabimo drugi ključ, v tem primeru je dejanska dolžina ključa 168 bitov, to je 3 * 56 bitov.
- Najbolj pogosta metoda pa je, da se prvi ključ uporabi za šifriranje, drugi ključ za odšifriranje in nato zopet prvi ključ za šifriranje, pri tem je dejanska dolžina ključa 112 bitov, to je 2 * 56 bitov.

Pri varovanju sistema KZZ se uporablja 3DES z dvema ključema K_a in K_2 , v zaporedju K_a, K_2 in K_1, ki imata skupno dolžino 112 bitov. Ta dolžina ključa pa že zagotavlja dovolj zgledno varnost.

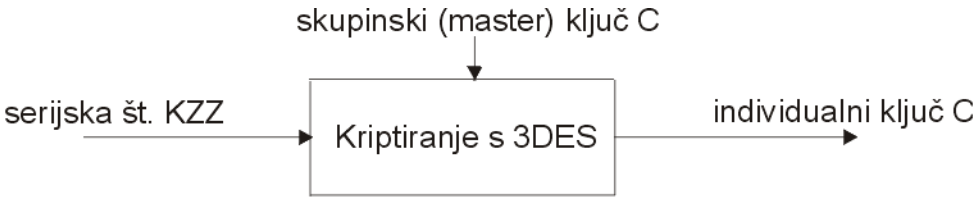


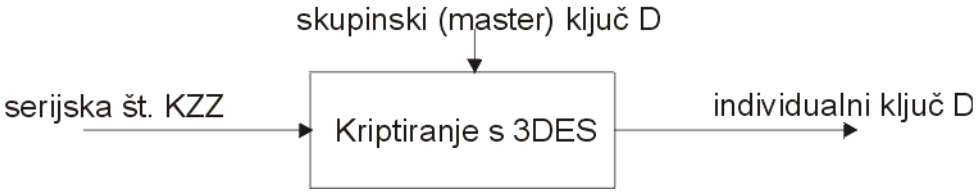


Pri vpeljavi simetričnega sistema 3DES v sistem kartice KZZ pa se pojavi problem prevelike količine dogovorjenih tajnih ključev.

V Sloveniji približno dva milijona potencialnih imetnikov PK in imetnikov KZZ. Simetrični algoritmi (med njimi tudi DES) temeljijo na dogovorjenih tajnih ključih med dvema uporabnikoma (imetnikom PK in imetnikom KZZ). Število vseh možnih dogovorjenih tajnih ključev za preverjanje pravic dostopa imetnika PK do kartice KZZ bi bilo zelo veliko. In vse te dogovorjene tajne ključe bi morala imeti shranjene vsaka kartica KZZ, za kar pa na kartici KZZ z 16 kB spomina ni dovolj prostora.

Zaradi problema s shranjevanja vseh dogovorjenih ključev, uporabnike PK kartic razdelimo na več skupin. Vsak uporabnik KZZ ima svoj ključ za preverjanje avtentičnosti KZZ in individualne ključe vseh skupin uporabnikov PK. Vsaka skupina uporabnikov PK kartice pa ima ključ za svojo skupino in t.i. skupinski ključ (master key), s katerim lahko iz serijske številke KZZ izračuna individualni ključ na kartici KZZ.





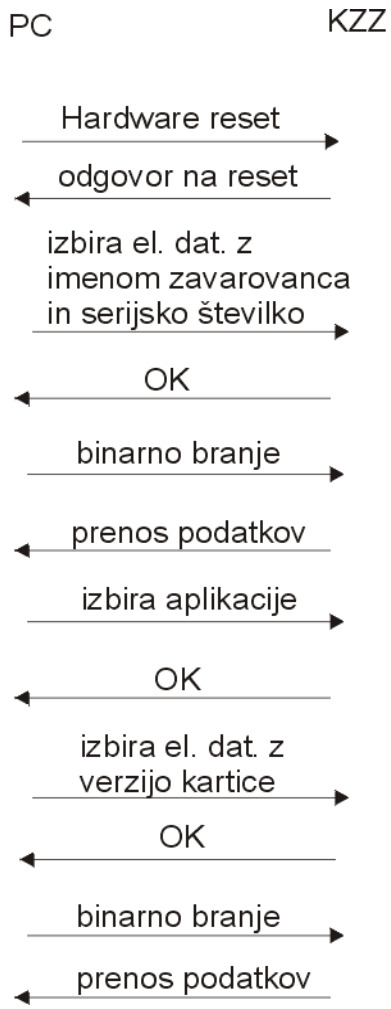
S temi ključi se uporabnik KZZ in uporabnik PK medsebojno overita s protokolom vrste izziv-odgovor.

Protokol inicializacije in izmenjave podatkov med KZZ in PK

Postopek dostopanja do podatkov na KZZ se vrši v naslednjih fazah:

1. inicializacija,
2. preverjanje pristnosti (KZZ in PK),
3. avtentifikacija lastnika kartice KZZ z uporabo PIN kode za dostop do določenih elementarnih datotek,
4. pristop do podatkov kartice KZZ,
5. vzdrževanje PIN na PK.

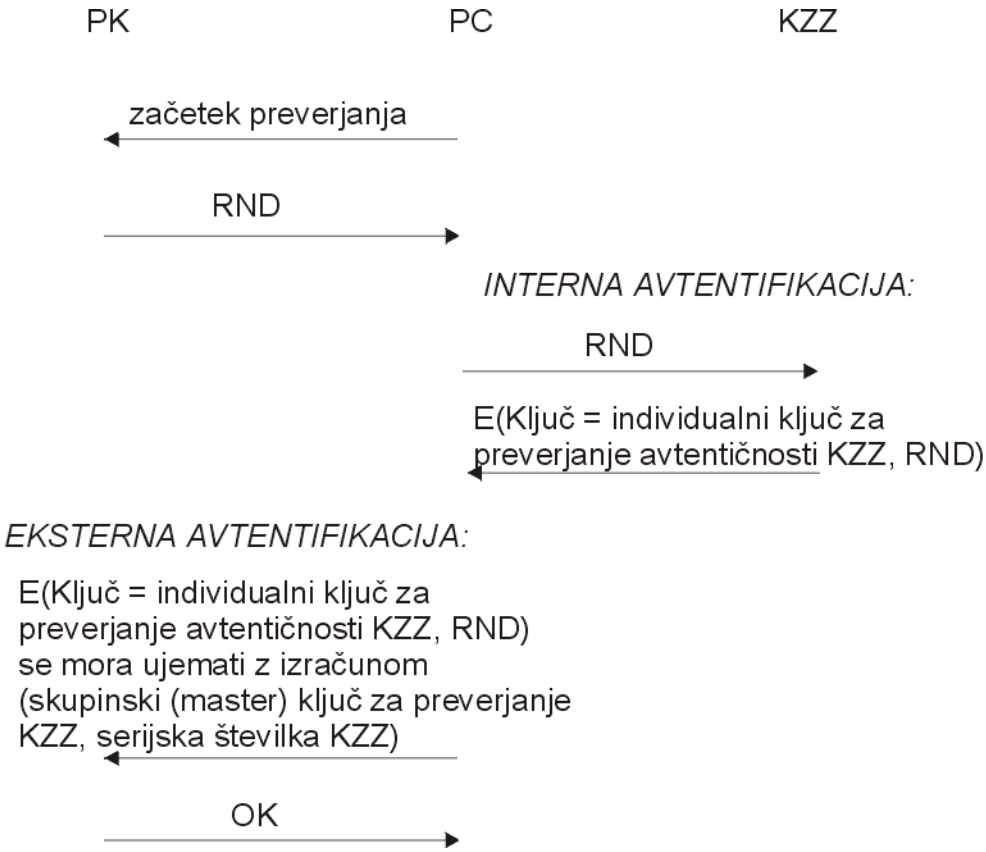
Inicializacija se izvrši implicitno enkrat pri vstavitvi KZZ v bralno zapisovalno napravo in je nekakšna nastavitev strojne opreme (reset). V tej fazi se preberejo tudi nekateri osnovni podatki kot npr. serijska številka kartice. Izvrši se tudi izbira aplikacije. Kartica je lahko namreč nosilec več različnih aplikacij. Za sistem KZZ se predvideva v naslednji fazi projekta razširitev z aplikacijo elektronskega recepta.



Inicializaciji KZZ in PK se razlikujeta v tem, da se pri inicializaciji PK zahteva vpis osebne identifikacijske številke PIN, s čimer se potrjuje lastništvo nad uporabljeno PK (avtentifikacija PK).

Po uspešno izvedeni inicializaciji se vzpostavi komunikacija med KZZ in PK. V tej fazi obe vrsti v komunikacijo vključenih kartic s posebnimi komandami kartičnega operacijskega sistema, med katerimi sta bistveni interna avtentifikacija (v nadaljevanju IA) in eksterna avtentifikacija (v nadaljevanju EA), medsebojno preverita pristnost. Z IA se v bistvu zunanjemu svetu dokazuje da je kartica pristna. Z EA pa zunanji svet preverja pristnost kartice. Zunanji svet je enkrat PK in drugič KZZ. Sam postopek je sledeč:

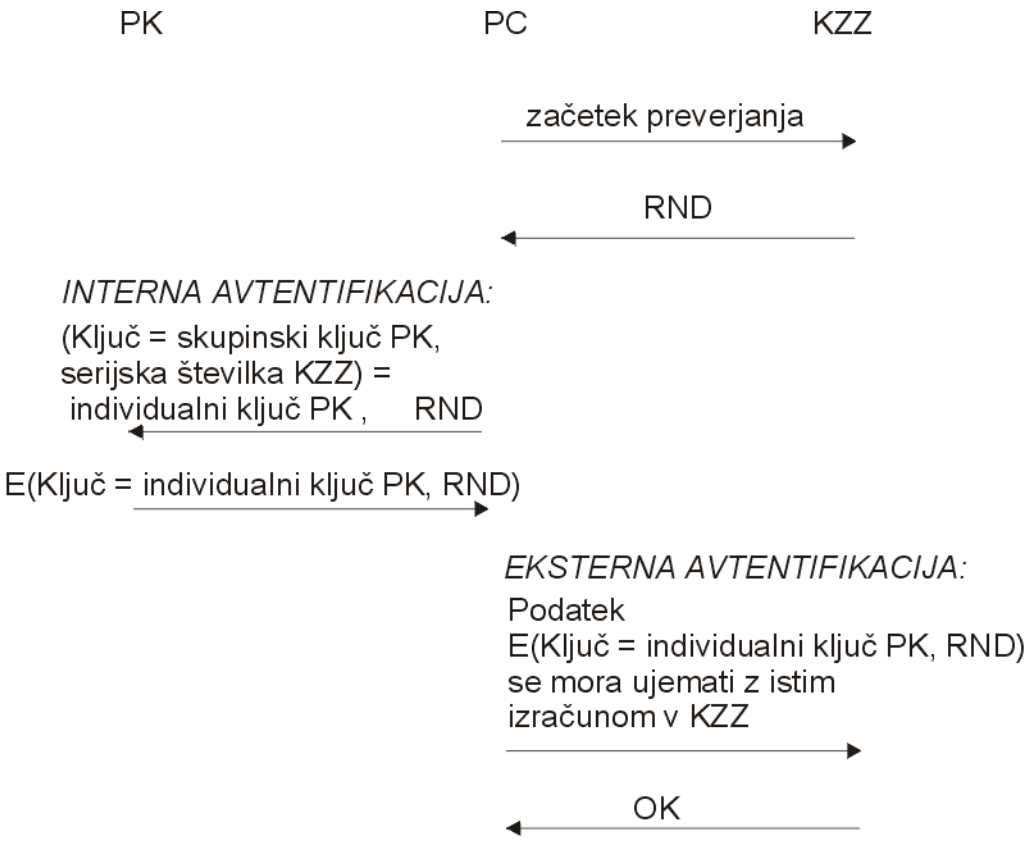
PK preveri pristnost KZZ:



Postopek:

1. programska komanda zahteva od PK naključno število (RND),
2. PK pošlje KZZ RND,
3. na KZZ se RND in individualni ključ za preverjanje avtentičnosti KZZ kriptirata s 3DES algoritmom,
4. kriptogram se prenese na PK,
5. Enkripcija serijske številke KZZ s pomočjo skupinskega (master) ključa za preverjanje KZZ se mora ujemati s prejetim kriptogramom iz KZZ,
6. identičnost obeh vrednosti potrjuje pristnost KZZ.

Po enakem postopku le v obratnem vrsten redu poteka preverjanje pristnosti PK. Na osnovi vrste skupinskega ključa, ki je zapisan na PK, KZZ odpre dostop do ustreznih elementarnih datotek.



Ta faza se lahko ponovi večkrat v okviru dostopanja do podatkov iz iste KZZ.

S tretjo fazo ima lastnik kartice KZZ možnost, da zavaruje dostop do določenih datotek na KZZ. Vnesti mora svoj PIN, preden se lahko preberejo ali spreminjajo podatki v datoteki. Za enkrat je ta možnost le pri datoteki o izdanih zdravilih.

Četrta faza je sam pristop do podatkov, ki ni dovoljen brez druge faze, ker faza preverjanja pristnosti PK poveže tudi ustrezne pristopne pravice PK. V tej fazi se KZZ pošljejo komande za izbiro datotek in njihovo branje oz. ažuriranje.

Pri komuniciranju s PK obstaja dodatno še faza vzdrževanja identifikacijske številke PIN. V njej se izvaja postopek menjave identifikacijske številke PIN oz. njeno deblokiranje. PK namreč omogoča vnos napačne identifikacijske številke samo trikrat. Po tretjem neuspešnem poskusu operacijski sistem kartice blokira njeno nadaljnjo uporabo. Deblokada je možna z deblokacijskim ključem. Po treh zaporednih neuspelih poskusih deblokade je PK neuporabna. Izdati se mora nova PK. Z PK, ki ima blokirano identifikacijsko številko ni možno izvajati postopka ugotavljanja pristnosti.

Dostop do podatkov na KZZ je zaščiten s ključi in omogočen z uporabo PK kakor prikazuje spodnja tabela.

Ime datoteke	**ZZŠ**	**VER**	**IDZ**	**PZ**	**OZ**	**PZ1**	**PZ2**	**IOZ**	**RZ**	**TPR**	**KIR**	**DIZ**	**PT**	**DIT**	**DO**
Uporabnik ključa															
uslužbenec ZZZS			B+P	B+P	B+P			B+P		B+P				B+P	
prost. zdrav. zav. 1			B		B	B+P									
prost. zdrav. zav. 2			B		B		B+P								
izbrani oseb. zdravnik			B	B	B	B	B	B+P	B+P	B+P	B+P	B+P	B+P	B+P	
ostali zdravniki			B	B	B	B	B	B	B+P	B+P	B+P	B+P	B+P	B+P	
medicinsko osebje			B	B	B	B	B		B+P	B+P	B+P	B+P	B	B+P	
fizioterapevti			B	B	B	B	B								
zdravnik inten. nege			B	B	B		B								B
farmacevt			B	B	B	B	B		B	B	B+P	B+P	B	B+P	
farmacevtsko osebje			B	B	B	B	B		B	B	B+P	B+P	B	B+P	
dobavitelj teh. opreme			B	B	B	B	B			B				B+P	
obvezno zavarovanje			B+P	B+P	B+P	B+P		B+P		B+P				B+P	
samopostr. terminal			B+P	B+P	B+P	B+P	B+P								B+P
PIN												*			

Legenda:
ZSŠ datoteka z imenom zavarovanca in serijske številke,
VER datoteka z verzijo kartice,
IDZ datoteka z identifikacijo zavarovanca,
PZ datoteka s podatki o zavarovancu,
OZ datoteka s podatki o obveznem zavarovanju,
PZ1 datoteka s podatki o prostovoljnem zdravstvenem zavarovanju 1,
PZ2 datoteka s podatki o prostovoljnem zdravstvenem zavarovanju 2,
IOZ datoteka s podatki o izbranem osebnem zdravniku,
RZ datoteka s podatki o predpisanih receptih za zdravila,
TPR datoteka s podatki o predpisanih tehničnih pripomočkih na recept,
KIR datoteka s kontrolnimi informacijami o izdaji receptov,
DIZ datoteka z dokumentacijo o izdanih zdravilih,
PT datoteka v kateri so opisana pacientova tveganja,
DIT datoteka z dokumentacijo o izdanih tehničnih pripomočkih,
DO datoteka z izjavo o darovanju organov,
B branje,
P pisanje.

Možni napadi na sistem KZZ

Šibkosti sistema KZZ se kažejo že v sami izbiri simetričnega algoritma 3DES (in s tem tajnih ključev). Smo namreč v dobi asimetrične kriptografije, to je kriptografije z javnimi ključi. Simetrični algoritmi se zaradi pomanjkljive varnosti uporabljajo bodisi v zaprtih okoljih, bodisi tam, kjer ni velike potrebe po varnosti.

Eden izmed možnih napadov na sistem KZZ je prisluškovanje postopkom za ugotavljanje pristnosti med PK in KZZ.

Če s prisluškovanjem uspemo dobiti del čistopisa *a* in njegov tajnopis *b*, potem z zelo zmogljivo opremo poskusimo dobiti ključ s katerim je bil zašifriran. Ključi pri 3DESu so dolgi 112 bitov. Torej poskušamo zašifrirati čistopis *a* z 2^{112} različnimi ključi K, dokler ne dobimo danega tajnopisa *b*.

$$3DES_K(a)=b$$

Ta napad z grobo silo bi bil zelo uspešen, če bi uporabili DES (dolžina ključa je 56 bitov; potrebno bi bilo preveriti le 2^{56} različnih ključev) in manj uspešen za 3DES (dolžina ključa 112). Če bi v nekaj urah lahko ugotovili kateri od 2^{56} različnih ključev je pravi, bi potrebovali z isto opremo potrebovali stoletja, da bi brez velike sreče ugotovili, kateri izmed 2^{112} različnih ključev je pravi ključ za 3DES algoritem. (Pri tem uporabljamo veliko število PCjev.) Velike obveščevalne službe pa tudi 3DES algoritem razbijejo v razmeroma kratkem času.

Če s prisluškovanjem dobimo del tajnopisa *b*, potem moramo uporabiti dekripcijo DESa, njegov inverz, da pridemo do ključa K. Z uporabo vseh možnih ključev K, ki se pojavijo lahko pri 3DESu, z obratom 3DESa dobimo različne čistopise *a*.

$$3DES^{-1}_K(b)=a$$

Pri vseh možnih ključih K, teh je 2^{112}, dobimo prav toliko možnih čistopisov *a*. Z uporabo lastnosti jezika (frekvenca črk, parov črk …), v katerem je pisan čistopis, lahko ugotovimo, kateri čistopis *a* je pravi čistopis za dani tajnopis *b*.
Ocena časovne zahtevnosti tega napada je enaka oceni zgornjega napada.

Možen je tudi t.i. DFA-napad (Differential Fault Analysis), ki namenoma povzroči izolirane napake pri kriptografskem računanju in so ga predlagali proti asimetričnim kriptosistemom leta 1996, še istega leta pa so ga prilagodili vsem kriptosistemom (torej tudi DESu). Napad DFA na DES potrebuje le 200 blokov tajnopisa, da izračuna vrednost tajnega ključa. Za 3DES se število potrebnih blokov tajnopisa ne poveča bistveno.

Imetniki PK kartice morajo za dostop do KZZ uporabiti svojo osebno identifikacijsko številko PIN. PIN je dolg 4 cifre. Če dobi napadalec v roke kartico PK, jo lahko izkoristi, če ugotovi pravi PIN. Vseh možnih PINov je 10*10*10*10=10000. Napadalec pa lahko v čitalnik le trikrat zapored vtipka PIN, v četrtem poskusu pa se kartica zablokira. Torej je verjetnost za uspešnost takega vdora 3/10000 =0.0003.

Na sistem KZZ so možni tudi čisto mehanski (fizični) napadi. Pri taki vrsti napadov napadalec poskuša kartici spremeniti delovno napetost, temperaturo, frekvenco itd. in tako zmesti njeno normalno delovanje, delovanje generatorja naključnih števil ali spremeniti kak števec. Vendar je tehnologija pametne kartice taka, da imajo

procesorji pametnih kartic senzorje, ki zaznajo nenormalne delovne pogoje in čip se pri takih napadih samodejno uniči. Možni so tudi napadi z »odpiranjem« čipa in z ustrezno nanotehnologijo ugotoviti njegovo notranjo zgradbo. Ker nanotehnologija neprestano napreduje, se da kartice, starejše od dveh let, z novo tehnologijo že odpirati, vendar so stroški takih napadov precejšnji.

Šibkost sistema KZZ se kaže tudi v skupinskih ključih. Obstajajo namreč napadi, ki ne posegajo v neposredno delovanje kartice. Med te sodi analiza porabe moči. Pri napadu z analizo moči merimo tok, ki ga procesor potrebuje, da izvrši določen ukaz. Na ta način lahko napademo večino kriptosistemov, ki niso ustrezno zaščiteni, med njimi so tako simetrični kot asimetrični kriptosistemi. Kako bi izvedli napad z merjenjem moči na sistemu KZZ?
Vsaka skupina uporabnikov PK ima skupinski (master) ključ, s katerim lahko iz serijske številke KZZ izračuna individualni ključ na kartici KZZ. Če prisluškujemo (merimo tok) temu šifriranju, lahko s pomočjo dane serijske številke KZZ dobimo večino bitov tajnega skupinskega (master) ključa 3DES algoritma. Za ostale neznane bite tajnega ključa pa uporabimo napad z grobo silo (za katero ne porabimo veliko časa). S tem, ko smo prišli do tajnega skupinskega (master) ključa, pa lahko dobimo vse ostale skupinske ključe sistema KZZ.
Kako bi se sistem KZZ lahko zaščitil pred takim napadom? Poraba elektrike bi morala biti podobna za vse strojne ukaze in ne bi smela biti odvisna od podatkov, ki jih obdeluje čip, da ni mogoče ugotoviti določene količine tajnih informacij. Uporabljati je torej potrebno zaslepljevalne metode, s katerimi poskušamo prikriti, katere operacije opravljamo.

Sedaj smo podrobneje opisali napade pri prenosih podatkov med PK in KZZ, ker smo podrobneje obravnavali povezave in zaščito med tema dvema karticama.
Obstajajo tudi zaščite pri prenosu podatkov iz kartic v centralno bazo ZZZS in samoposrežnimi terminali. Menda se pri teh prenosih za zaščito uporablja javna kriptografija (asimetrični algoritem RSA, ki temelji na velikih praštevilih). Napadi na javno kriptografijo so težji. Lahko pa izvajamo zgoraj opisan napad z merjenjem moči.

Ovrednotenje uvedbe KZZ

Ocena pilotske uvedbe KZZ v Posavju

Zavod za zdravstveno zavarovanje Slovenije je 6. aprila 1998 začel pilotni poskus uvajanja kartice zdravstvenega zavarovanja v posavski regiji, v občinah Krško, Brežice in Sevnica. Uvedba kartice KZZ, ki se je zaključila v mesecu juniju 1998, je potekala postopoma. V treh mesecih je bilo razdeljenih približno 440 profesionalnih kartic (4 kB) in 70.000 kartic zdravstvenega zavarovanja (8 kB) , ki so s tem postale veljavni dokument za vse obiske pri zdravniku in leto kasneje v lekarni. V posavski regiji je bilo nameščenih 21 samopostrežnih terminalov.

V Zavodu so se za pilotni projekt odločil zato, da s čim manjšimi posledicami in stroški preverijo delovanje sistema kartice zdravstvenega zavarovanja v praksi in odpravijo morebitne pomanjkljivosti in napake. Vseh postopkov, kot so na primer uvedba kartice, preizkušanje posebnih primerov (varnost v sistemu KZZ, nedelovanje čitalnikov, izguba kartice, nedelovanje terminalov, sprejemljivost sistema za zdravstveno osebje itd.) namreč v laboratorijskih preizkusih ni bilo mogoče predvideti.

Ocena pilotne uvedbe:
Z oceno pilota so mednarodni strokovnjaki ugotovili, da je pilotni projekt kartice zdravstvenega zavarovanja v celoti potrdil vsebinske cilje iz zasnove projekta in je bil izveden v skladu z načrtom uvajanja sistema kartice zdravstvenega zavarovanja. Kartico so sprejeli zavarovanci, zdravstveno osebje, osebje Zavoda in delodajalci, saj je vsem prinesla obljubljene prednosti in izboljšave (razbremenitev zdravstvenega osebja pri administrativnih opravilih, enostavno potrjevanje preko samopostrežnih terminalov brez tretje osebe, več časa za strokovno delo zdravnikov in farmacevtov itd.). Zdravstveno osebje pa je izrazilo željo, da se na kartico čimprej uvedejo tudi drugi (medicinski) podatki.

Pilotni projekt je bil izveden v načrtovanih časovnih in finančnih okvirih. Tehnologija kartic se je izkazala za ustrezno, tako glede usklajenosti s standardi kot tudi glede načrtovanih funkcij. Varnost podatkov na kartici je po oceni strokovnjakov Inštituta Jožefa Stefana zagotovljena na ustrezni ravni. Organizacijski pristop k uvedbi v pilotni regiji se je izkazal kot uspešen in tako primeren za uvedbo v druge slovenske regije.

Ovrednotenje uvedbe KZZ v Sloveniji

Po zaključeni nacionalni uvedbi kartičnega sistema je bila oktobra 2000 organizirana mednarodna evalvacijska konferenca. Povzetek ugotovitev je naslednji:

Uvedba je potekala v skladu z načrtom, v predvidenih rokih, znotraj zastavljenih finančnih okvirov in z uspešno realizacijo objektivnih ciljev.

Kartico so dobro sprejele zavarovane osebe, zdravstveno osebje in poslovni subjekti zdravstvenega zavarovanja.
Sprejemanje kartice pri zavarovancih in zdravstvenem osebju je analizirala neodvisna zunanja agencija. Na področju celotne Slovenije je sprejemanje kartice med zavarovanci 82,9%.
Z uporabo kartičnega sistema rastejo pozitivne ocene tudi med zdravstvenimi delavci. Po dveh letih uporabe v pilotni regiji je 70,6% zdravnikov podprlo oceno, da je kartica poenostavila njihovo delo, 76,9% medicinskih sester se strinja, da se je njihov obseg dela zmanjšal, in 92,3%, da jih je kartica poenostavila delo.

Kartični sistem ima od svoje uvedbe dalje pozitivne učinke zaradi preglednosti in natančnosti podatkov, ponuja pa tudi nadaljnje potenciale za izboljšanje poslovanja.

Nadaljnji razvoj

Kartični sistem je bil oblikovan glede na potrebe in realno stanje v slovenskem zdravstvenem varstvu in zdravstvenem zavarovanju, upoštevajoč opremljenost z informacijsko tehnologijo, v okviru možnih finančnih okvirov ter v skladu z veljavno zakonodajo.

Informacijska tehnologija se hitro razvija, zato je pomembno, da je slovenski kartični sistem odprt za spremembe in omogoča nadaljnje nadgradnje podatkov storitev in tehničnih komponent.

Na kartici so zaenkrat samo zavarovalniški, identifikacijski in administrativni podatki. Kartični sistem pa je na voljo tudi za zapis medicinskih podatkov. Kartica nikoli ne bo postala prenosni karton s številnimi podrobnimi podatki, ampak naj bi bili na tem mediju zapisani stabilni nujni medicinski podatki.

Mrežna povezanost med večino izvajalci zdravstvenih storitev v slovenskem zdravstvu bo začela delovati čez nekaj let. Kartica bo s tem razvojem postala ključ za dostop podatkov v omrežju.

Že sedaj je možno izkoristiti široko mrežo samopostrežnih terminalov, preko katere lahko zavarovane osebe interaktivno iščejo informacije in naročajo storitve. Na samopostrežnih terminalih lahko naročamo konvencijska potrdila za zdravstveno zavarovanje med začasnim bivanjem v tujini. Poiskati in izvesti pa bo potrebno še druge možnosti.

Septembra 2001 je bil ustanovljen Projektni svet za uvedbo zdravstvenih podatkov na kartico, pod vodstvom Ministrstva za zdravje sodelujejo predstavniki Kliničnega centra, Združenja zdravstvenih zavodov, Zavoda za zdravstveno zavarovanje, Inštituta za varovanje zdravja, Zdravniške zbornice in Lekarniške zbornice. Zaradi pomembnosti izbranih medicinskih podatkov in medinstitucionalnega usklajevanja, zakonodajnih zahtev in postopkov je potrebno spremembe uvesti premišljeno in postopno.

Novi podatki na zdravstveni kartici v prihodnosti bodo:

1. Darovalec
   Ko bodo urejene pravne in tehnično-organizacijske podlage, bo stekla akcija obširnega informiranja slovenske javnosti o zbiranju prostovoljnih izjav glede posmrtnega darovanja organov in tkiv za presaditev. Ta podatek se bo zapisal v za to pripravljeno datoteko na kartici KZZ.

2. Zapis o medicinsko-tehničnih pripomočkih
   ZZZS pripravlja zapis na KZZ o izdanih in izposojenih medicinsko-tehničnih pripomočkih (predvideno v letu 2002). To so proteze, ortoze in ortopedski čevlji, vozički in drugi pripomočki za gibanje, stojo in sedenje, pripomočki za vid, sluh in govor, pripomočki pri težavah z odvajanjem seča, pripomočki pri zdravljenju sladkorne bolezni itd. Za velik del pripomočkov je določen čas, po katerem je zavarovana oseba upravičena do prejema novega. Zapis o izdaji

novega pripomočka bo omogočil potrebno evidenco pri predpisovanju novih pripomočkov, kar je pogoj za porazdelitev omejenih finančnih sredstev.

3. Zapis o alergijah in cepljenjih
   Podatke o alergijah in cepljenjih na kartici KZZ lahko pričakujemo od konca leta 2003.

4. Elektronski podpis.
   Pogoj za digitalno podpisovanje zdravstvenih podatkov je elektronski podpis. Elektronski (ali digitalni) podpis uporabljamo za ugotavljanje pristnosti elektronskega sporočila, dokumenta ali identitete. Elektronski podpis je dodan čitljivemu besedilu na tak način, da prestane preizkus le, če vsebina sporočila ostane nespremenjen. Preizkus je običajno izveden z asimetričnim algoritmom (npr. RSA, ElGamal): z zasebnim ključem se generira informacija, ki jo tretja oseba uporabi zato, da z javnim ključem preveri veljavnost.
   Pravna veljava elektronskega podpisa je določena z zakonom (Zakon o elektronskem poslovanju in elektronskem podpisu, UL RS 57/2000).
   Za elektronsko podpisovanje je potrebna programska in strojna oprema, potrdilo pristojne institucije in ključi za podpisovanje. Ustrezno infrastrukturo v sistemu KZZ se zagotovi z nadgradnjo profesionalnih kartic v obstoječem sistemu KZZ. Uvedbo elektronskega podpisa v zdravstvu pričakujemo leta 2003. Elektronski podpis bo omogočil elektronsko poslovanje z elektronskim receptom, elektronskim predpisovanjem medicinsko-tehničnih pripomočkov, kartični zapis stabilnih medicinskih podatkov (diabetes, epilepsija, hemofilija, pacemaker,…), kartični zapis podatkov o izdanih zdravilih itd.

Mednarodno sodelovanje

V Evropi in svetu potekajo številni projekti uvajanja kartic v zdravstvene sisteme. Evropska komisija želi spodbuditi razvoj skladnosti nacionalnih projektov zdravstvenih kartic in vzpostaviti model bodočega prenosa izkušenj, znanja, standardov in priporočil med projekti, ki že potekajo, ter tistimi, ki so v nastajanju, z namenom, da bi zdravstvene kartice v prihodnosti uporabljali tudi zunaj nacionalnih meja.

V Evropski Uniji in v skupini G7 potekajo intenzivne aktivnosti usklajevanja raziskovalnih, razvojnih, tehnoloških in organizacijskih dejavnosti na področju zdravstvenih kartic. V dosedanjih etapah je bil zgrajen obsežen sistem standardov, pravil in priporočil za zagotavljanje poenotenja sistemov in zmožnosti za uporabo podatkov in tehnologije v širšem prostoru, ne le na območju enega samega sistema. V okviru usklajenih pilotnih preizkusov in operativnih sistemov je bilo do sedaj v Evropi izdanih že preko 100 milijonov kartic.

Netlink je eden ključnih razvojno-usklajevalnih projektov Evropske unije na področju zdravstvene informatike s poudarkom na kartičnih in mrežnih tehnologijah. Vanj so vključene Nemčija, Francija, Italija in Kanada. Namen Netlinka je razvoj kartičnih projektov v vseh sprejetih državah ob neposrednih stikih in sodelovanju z evropskimi institucijami kot tudi z izmenjavo izkušenj in znanja v državah Evropske Unije in G7.

S takim pristopom želi Evropska komisija spodbuditi razvoj skladnosti nacionalnih projektov zdravstvenih kartic in vzpostaviti model bodočega prenosa izkušenj, znanja, standardov in priporočil med projekti, ki že potekajo, in tistimi, ki so v nastajanju, z namenom, da bi zdravstvene kartice uporabljali tudi zunaj nacionalnih meja. V Evropi in v svetu potekajo številni projekti uvajanja kartic v zdravstveno varstvo, kot so CardLink (uvajanje večnamenske administrativne kartice z naborom nujnih medicinskih podatkov), DiabCard (zasnova kartice za bolnike z diabetesom) in TrustHealth (poskus uvajanja univerzalne profesionalne kartice) ter mnogi drugi.

V začetku leta 1998 sta se sestrskemu projektu Netlinka, imenovanem Netlink-CEE, ki povezuje vzhodnoevropske projekte z zahodnoevropskimi, pridružila Slovenija in Češka. Obe državi sta edini med srednjeevropskimi deželami svojo kartico zdravstvenega zavarovanja razvili do nivoja, skladnega s priporočili in rezultati projektov Evropske skupnosti. Kot izvajalca sta iz Slovenije v projekt vključena Zavod za zdravstveno zavarovanje Slovenije in Institut Jožef Stefan. Za slovenski projekt kartice zdravstvenega zavarovanja pomeni vključitev v Netlink formalizacijo že do sedaj razvejanega sodelovanja na strokovni ravni, potrditev visoke stopnje usposobljenosti in strokovnosti vseh izvajalcev projekta ter financiranje raziskovalno razvojne dejavnosti v okviru projekta kartice zdravstvenega zavarovanja.

V okviru konference Cartes 2000 so bile konec oktobra v Parizu podeljene nagrade za največje dosežke. Na področju zdravstva je nagrado prejel slovenski sistem kartic zdravstvenega zavarovanja z obrazložitvijo, da predstavlja projekt najbolj celovito obstoječo rešitev.

Slovenija se od jeseni 1999 s projektom kartice vključuje v delo združenja EHTEL, ki kot nevtralna in trajna asociacija za podporo razvoju informacijskih rešitev v zdravstvu združuje predstavnike zdravstvene politike in plačnikov (ministrstva, zdravstvene zavarovalnice), uporabnikov (zdravstvenih delavce in pacientov) ter industrije.

ZZZS je vključen tudi v delo skupine za razvoj kartic v zdravstvu v okviru programa eEurope (Smart Card Charter, Trail Blazer 11 Health). Prav tako je ZZZS vključen v mednarodno iniciativo za zagon dveh razvojnih projektov, HealthCards.Net (demonstracija in promocija sinergij med pametno kartico in mrežami v zdravstvu) in Prescribe (oblikovanje mreže za elektronsko posredovanje receptov na evropski ravni).

Zaključek

Informacije so eno izmed najbolj dragocenih in koristnih sredstev, zato jih je nujno zaščititi pred izgubo, nepooblaščenim spreminjanjem in odkrivanjem. Informacije so lastnina tistega, ki jih ima. Izguba informacije povzroči izgubo časa in denarja.

Uporaba tehničnih kontrol in nadzora služi preprečevanju nevarnih pojavov z odvračanjem zlonamernih uporabnikov, oziroma tako, da le-tem povzroča velike težave pri neavtoriziranem vstopanju v sistem. Primer tehnične kontrole predstavlja vsak postopek avtentifikacije uporabnika, na primer vstopno geslo, identifikacijska številka.

Varovanje ni enkratno opravilo, ampak je stalni posel. Razvijati, napredovati mora v skladu s potrebami in zahtevami poslovanja. Prav tako pa je potreben tudi stalni nadzor nad ustreznostjo zaščite. Sistem kartice zdravstvenega zavarovanja zagotovo posodablja sistem in izboljšuje zaščito podatkov, ki jih je imelo zdravstvo s staro zdravstveno izkaznico. Vendar pa bo potrebno tudi izboljšati varovanje sistema KZZ in iti v koraku s časom ter izbirati napredne ter uveljavljene kritografske algoritme.

Vsak proizvod, ki je rezultat človeškega dela, vsebuje določeno mero nenatančnosti in neučinkovitosti. Iz tega sledi, da je malo verjetno oziroma neverjetno, da bi bili ukrepi ali postopki absolutnega varovanja mogoči. Za vsak algoritem se v doglednem času najde ustrezen napad.

Literatura

1. Zavod za zdravstveno zavarovanje, domača stran (http://www.zzzs.si)
2. Gemplus, domača stran (http://www.gemlpus.si)
3. Motus technologies, domača stran (http://www.motus.qc.ca)
4. Pehani P.: *Mikroprocesorska kartica in kartični operacijski sistemi*. Uporabna informatika, 2 številka, letnik VII, 1999: 14-20.
5. Jurišič A., Trojar A.: *Pametna kartica*. Uporabna informatika, maj 1997, 37-45.
6. Sušelj M.: *Slovenska kartica zdravstvenega zavarovanja (1., 2., 3. in 4. del).* Glasilo zdravniške zbornice Slovenije ISIS, 1997.
7. Sušelj M.: *Sistem kartice zdravstvenega zavarovanja - uvajanje in prve izkušnje*. Uporabna informatika, posebna številka Maj 1998: 50-55.
8. Habjančič P.: *Pametne kartice*, seminarska naloga (http://www1.feri.uni-mb.si/~debevc/HCI/Izdelki/Marko-Habjanic/index.htm)
9. B. Berčic, M. Pikec, S. Slavec, I. Zelič, I. Zupan, Infonet d.o.o., Kranj, članek (http://www.infonet.si/html/body-medo.htm)
10. Denis Požar, Marjan Sušelj, *Varovanje podatkov v sistemu KZZ*, Zbornik referatov INDO `97, Informatika v državnih organih Portorož `97.
11. Health insurance card of Slovenia, *Technical specification of the health professional card*, Version 1.2, 20. 5. 1999
12. Health insurance card of Slovenia, *Technical specification of the health insurance card*} Version 1.2, 25. 5. 1999
13. Trček D., *Sistem kartice zdravstvenega zavarovanja in specifikacija SET*, IJS, članek.
14. T. Kalin, G. Kandus, D. Trček, B. Zupan, *Slovenian national health insurance card: The next step*., IJS, članek.
15. T. Kalin, G. Kandus, D. Trček, R. Novak, M. Sušelj, *Smart-card based infrastructure for a health-care information system in Slovenia*, IJS, članek.
16. A. Pernice, H. Doare, *Health Cards: An overview of the current key international issues*, Health Cards '97, 12.-14. 11. 1997 Amsterdam, 391-414.
17. A. Jurišić, J. Tonejc, *Pametne kartice in varnost*, revija Monitor **11**/6, junij 01, 66-75 str.
18. A. Jurišić, J. Tonejc, *Pametne kartice- 2. del: Zasebno življenje javnih ključev*, revija Monitor **11**/7-8, julij - avg 01, 44-53 str.
19. A. Jurišić, J. Tonejc, *Pametne kartice- 3. del: Napadi in obrambe: velike skrivnosti malih kartic*, revija Monitor **11**/9, sept 01, 54-64 str.