Zaštita sigurnosti i povjerljivosti podataka u aplikativnim rješenjima u ordinacijama primarne zdravstvene zaštite

Galibedin Galijašević, dr. med.
ABA informatika, Zagreb

Osobni podaci, a posebno medicinski podaci o zdravlju osobe iznimno su štićeni kroz legislativnu strukturu modernih država. Zloporaba tih podataka zakonski je kažnjiva i može imati dalekosežne osobne, društvene i političke posljedice. Stoga je neobično važno pitanje organizacije sigurnosti podataka i pitanje zaštite povjerljivosti u zdravstvenim informacijskim sustavima, koji se postižu najmodernijim tehnološkim i organizacijskim sustavima kontrole pristupa na svim razinama: na razini osobe, na razini aplikacije i organizacije informacijskog sustava i na razini informatičke opreme

Postupkom provjere vjerodostojnosti utvrđuje se identitet korisnika koji želi koristiti aplikacijski softver u ordinaciji primarne zdravstvene zaštite. Svaki zdravstveni djelatnik posjeduje pametnu karticu (engl. *Smart Card)* koja mu omogućuje dokazivanje identiteta prilikom postupka provjere vjerodostojnosti, šifriranje podataka i elektroničko potpisivanje medicinske dokumentacije. Uporaba pametne kartice temelji se na sustavu javnih i tajnih ključeva odnosno digitalnih certifikata izdanih od državne certifikacijske agencije (FINA). Pametna kartica korisnika informacijskog sustava primarne zdravstvene zaštite sadržava:

- privatni ključ za šifriranje podatka,
- privatni ključ za generiranje digitalnog potpisa.

Digitalni certifikati koji su izdani od certifikacijske agencije i sadrže javne ključeve korisnika informacijskog sustava pohranjeni su u Registru resursa u zdravstvu u Središnjem integracijskom zdravstvenom informacijskom sustavu – SIZIS (G1: ISPZZ). Svaka pametna kartica zaštićena je od neovlaštenog korištenja osobnim identifikacijskim brojem, tj. PIN-om (engl. *Personal Identification Number)*. Korisnik aktivira pametnu karticu korištenjem čitača kartice i pristupa informacijskom sustavu. SIZIS korištenjem PKI tehnologije (engl. *Public Key Infastructure)* utvrđuje identitet korisnika i omogućuje mu korištenje informacijskog sustava i njegovih usluga ukoliko je postupak provjere vjerodostojnosti potvrdio identitet. Pojednostavljeno govoreći, aplikacijski softver u ordinaciji može pokrenuti samo osoba koja posjeduje pametnu karticu s valjanim i važećim certifikatom i poznaje osobni identifikacijski broj (PIN) dotične kartice.

Autorizacija korisnika je sljedeća razina zaštite povjerljivosti podataka. Obavlja se prilikom zahtjeva korisnika za određenom uslugom i/ili podacima koje pruža informacijski sustav primarne zdravstvene zaštite. Postupkom autorizacije provjeravaju se prava koje korisnik ima prema točno definiranim ulogama koje mogu imati pojedini korisnici sustava (liječnik, sestra, itd.). Uloge korisnika su definirane u organizacijskoj strukturi zdravstvenog sustava i pohranjene u registru resursa u zdravstvu. Dakle, dopušta se samo kontrolirani pristup onim podacima i uslugama koje su odobrene korisničkoj ulozi koja je dodijeljena certifikatu pohranjenom na pametnoj kartici. Drugim riječima, i liječnik i medicinska sestra svojim karticama mogu pokrenuti aplikacijski softver, no za razliku od korisnika s dodijeljenom ulogom liječnika, korisnik s ulogom medicinske sestre ne može pristupiti zdravstvenom kartonu u cijelosti, već određenom, definiranom segmentu istog. SLIKA 1 prikazuje postupak provjere vjerodostojnosti i autorizacije liječnika korištenjem pametne kartice.

Sve dok ne dođe do zamjene sadašnjih zdravstvenih iskaznica pametnom karticom, identifikacija osiguranika i provjera statusa zdravstvenog osiguranja obavlja se pomoću postojećih magnetskih kartica za osnovno i dopunsko zdravstveno osiguranje (SLIKA 2). Uvođenjem pametnih kartica, osiguranici/pacijenti će moći svojim digitalnim potpisom na pametnoj kartici dodatno kontrolirati pristup svojim medicinskim podacima davanjem suglasnosti za pristup podacima. Zbog svog velikog memorijskog kapaciteta, pametna kartica osiguranika bi također mogla biti nositelj važnih medicinskih informacija o pacijentu.[1,2,3]

Struktura elektroničkog zdravstvenog kartona

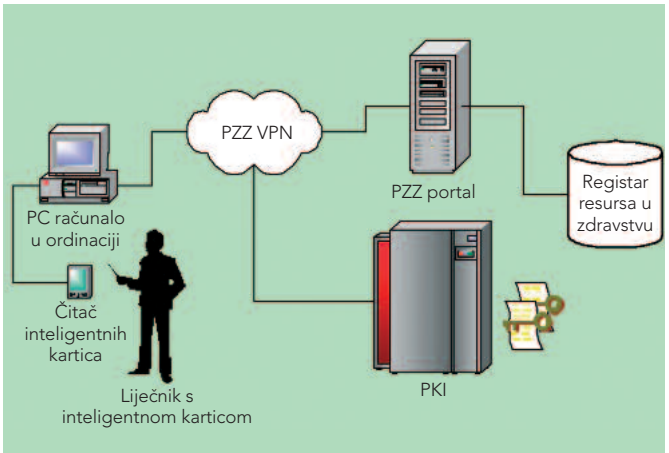
Struktura elektroničkog zdravstvenog kartona Središnjeg integracijskog zdravstvenog informacijskog sustava (ISPZZ), a koju nasljeđuju i aplikacijski softveri u ordinacijama, dodatno s više razine kontrolira pristup bazama podataka korištenjem PKI tehnologije i tehnologije pametne kartice (SLIKA 3). Sustav bilježi sve pristupe i pokušaje pristupa podacima, pa je uvijek moguće rekonstruirati i pokušaj neovlaštenog pristupa podacima.[4,5]

Uporaba certificiranih softvera u ordinacijama

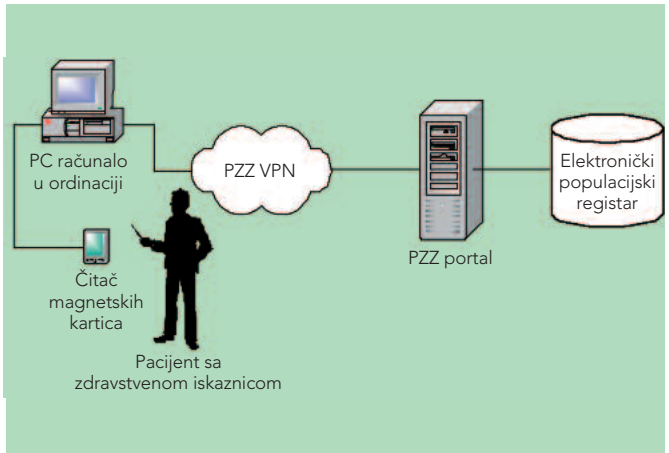
Aplikacijska rješenja za ordinacije primarne zdravstvene zaštite bi trebala dobiti certifikate od državne certifikacijske agencije (FINA) putem kojih bi Središnji integracijski zdravstveni sustav (ISPZZ) kontrolirao softverski pristup. Ovakvom kontrolom bi se onemogućio pokušaj pristupa sustavu neovlaštenim softverskim rješenjima.[1,2]

Sigurnosni sustavi računalne opreme

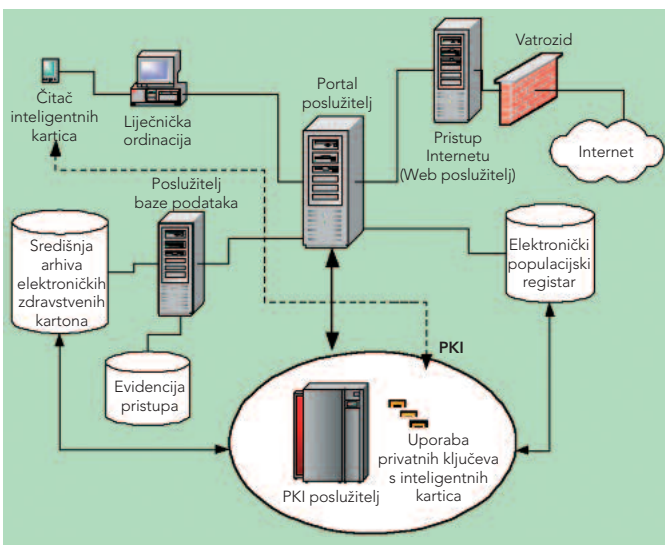
Računalna oprema kojom će biti opremljene ordinacije primarne zdravstvene zaštite treba slijediti najviše trenutačno postojeće sigurnosne standarde. Oprema treba uključiti čitače pametnih kartica za korisnike, a u perspektivi i za osiguranike/pacijente, kao i strukturne hardverske elemente koji podižu razinu sigurnosti opreme i informacijskog sustava i podataka u njemu pohranjenih (nadzor perifernog pristupa, sigurnosni čip).



Slika 1. Provjera vjerodostojnosti i autorizacija liječnika



Slika 2. Provjera statusa zdravstvenog osiguranja pacijenta



Slika 3. Pristup bazama podataka

Zaključak

Zahtjev za sigurnošću zdravstvenih informacijskih sustava i podataka u njima jedan je od osnovnih prioriteta. Visoki stupanj zaštite sigurnosti i povjerljivosti podataka u aplikativnim rješenjima za ordinacije primarne zdravstvene zaštite, kao i u cjelokupnom Informacijskom sustavu primarne zdravstvene zaštite postiže se najmodernijim tehnološkim i organizacijskim sustavima kontrole pristupa na svim razinama: na razini osobe, na razini aplikacije i organizacije informacijskog sustava i na razini informatičke opreme. M

LITERATURA

1. Vegoda PR, ed. Integrating the Healthcare Enterprise. Chicago, IL: Healthcare Information and Management Systems Society, 2001; 20-5.
2. Slakey DP, Nowfar S. Factors Affecting Patient – Physician Communication Via the Internet. Healthcare Information Management 2004; 18:30-5.
3. Chan W, Centiu C, Morris JA, Kurtz M. Uniform Data Standards for Capturing Patient Medical Record Information at the Point of Care. Journal of Healthcare Information Management 2002; 14(3):85-95.
4. Carlon GC. The Electronic Medical Record and the Oath of Hippocrates. How the EMR Helps "Do No Harm." Health Management Technology 2000; 21:16.
5. Erstad TL. Analyzing Computer based Patient Records: A Review of Literature. Journal of Healthcare Information Management 2003; 17(4):51-7.