1. Uvod

Razvoj elektronskih komunikacija doveo je do toga da se razmena informacija poverljive sadržine odvija svakodnevno. Da li je u pitanju razmena elektronske pošte između partnera ili korišćenja usluga elektronskog bankarstva, bitno je da ne dođe do neovlašćenog pristupa podacima koji se šalju. Da bi se prenos ovakvih informacija učinio sigurnijim, one se modifikuju na takav način da osoba kojoj one nisu namenjene ne može da ih protumači u slučaju da dođe u njihov posed.

Tema diplomskog rada iz predmeta Elektronsko bankarstvo odnosi se na problematiku sigurnosti u sistemu elektronskog bankarstva i primenu PKI – a (public key infrastructure). Infrastruktura javnog ključa (engl. ***Public Key Infrastructure - PKI***), je vrlo složen sistem temeljen na asimetričnoj kriptografiji. PKI objedinjuje sertifikate, sertifikacijsku ustanovu (sertifikator), bazu sertifikata i opozvanih sertifikata, korisnike sertifikata, kao i sve njihove međusobne interakcije (interakcije između pojedinih elemenata sistema).

Sigurnost predstavlja najveću brigu banaka koje nude usluge elektronskog bankarstva i najčešće je definisan kao kombinacija tehnologija, mera i postupaka zaštite informacija od neovlašćenog eksploatisanja. Sprečavanje zloupotreba informacija paralelan je zadatak zadatku razvoja elektronskog bankarstva. Danas, možemo konstatovati da postoji nekoliko sistema i nivoa zaštite podataka, počevši od najjednostavnijih kao što je lozinka, koji danas sam po sebi više ne predstavlja dovoljan sistem zaštite i mora se kombinovati sa određenim dodacima (na primer, PIN kodovi), preko TAN kartica pa sve do savremenih sistema enkripcije podataka koji za sada onemogućavaju zloupotrebu informacija. Naravno, osnovni zadatak pružalaca usluga elektronskog poslovanja, svakako jeste zaštita podataka, s` obzirom na sve veći broj mogućnosti i načina da se „zaobiđu“ klasični sistemi zaštite i da se dođe do informacija. Ipak, najveću odgovornost za sprečavanje zloupotrebe informacija iz elektronskog bankarstva snosi sam korisnik, jer se u njegovom posedu nalaze pojedinačni

elementi zaštite sistema. Banka mora voditi računa pored sigurnosnih sistema i o zaštiti mreže banke i kontroli pristupa.

Sama ideja o PKI-u nastala je sedamdesetih godina prošlog veka. U to vreme je postojala simetrična kriptografija odnosno kriptografija temeljena na tajnom ključu. Glavni problem simetrične kriptografije bio je sigurna razmena tajnog ključa preko nesigurnog kanala. 1976. godine, Whitfield Diffie i Martin Hellman u svojoj publikaciji „*New Directions in Cryptography*" su predstavili ideju razmene tajnog ključa temeljenu na asimetričnoj kriptografiji (kriptografija temeljena na javnom i privatnom ključu). Asimetrična kriptografija omogućila je i digitalno potpisivanje podataka. Dve godine posle uveden je pojam digitalnog sertifikata kao digitalno potpisanog dokumenta koji povezuje javni ključ sa osobom kojoj taj ključ pripada. Sve ovo, kao i pojava savremene komunikacije preko medija (ponajviše pojava Interneta) kao nesigurnog kanala, dovelo je do realizacije PKI-a kao sistema koji omogućuje sigurnu komunikaciju preko nesigurnog kanala.

2. PKI sistem

PKI sistem predstavlja najvažniji aspekt sistema elektronskog poslovanja, kao i savremenih finansijskih i korporacijskih računarskih mreža. PKI sistem obezbeđuje pouzdano okruženje za realizaciju četiri osnovne funkcije zaštite komercijalnih i poslovnih transakcija - auteničnost strana u komunikaciji, integritet podataka, nemogućnost naknadnog poricanja sadržaja poslatih podataka i zaštitu tajnosti podataka. Prve tri funkcije realizuju se na bazi tehnologije digitalnog potpisa primenom asimetričnih kriptografskih sistema, dok se funkcija zaštite tajnosti realizuje primenom simetričnih kriptografskih sistema.

Srce PKI sistema predstavlja Sertifikaciono telo (CA – certification authority) čija je osnovna funkcija pouzdano uspostavljanje zaštićenog digitalnog identiteta ovlašćenih učesnika u datoj računarskoj mreži. Pomenuta funkcija se postiže primenom digitalnog sertifikata koji jednoznačno povezuje identitet ovlašćenog učesnika sa javnim ključem asimetričnog šifarskog sistema. Autentičnost i jednoznačnost svakog digitalnog sertifikata dokazuje se digitalnim potpisom svakog digitalnog sertifikata od strane Sertifikacionog tela. Na taj način sertifikaciono telo postaje treća strana od poverenja za bezbednu komunikaciju bilo koja dva ovlašćena učesnika u datoj računarskoj mreži.

PKI sistem predstavlja infrastrukturu sistema sa javnim ključevima odnosno kombinaciju hardverskih i softverskih proizvoda, politika i procedura. Obezbeđuju sigurno okruženje za poslovanje i komunikaciju korisnika bez obzira na njihovu fizičku lokaciju. PKI sistemi se baziraju na elektronskim identitetima korisnika (elektronski sertifikati) koji povezuju ime vlasnika datog sertifikata sa njegovim javnim ključem asimetričnog kriptografskog sistema i omogućavaju mu delovanje shodno njegovim ovlašćenjima.

-------- CEO RAD MOŽETE PREUZETI NA SAJTU --------

http://www.maturskiradovi.net/eshop/

POGLEDAJTE VIDEO UPUTSTVO SA TE STRANICE I PORUČITE RAD PUTEM ESHOPA , REGISTRACIJA JE OBAVEZNA.

MOŽETE NAS KONTAKTIRATI NA E-MAIL: maturskiradovi.net@gmail.com