BEZBEDNOST PODATAKA U SISTEMU ELEKTRONSKOG BANKARSTVA

Goran Pantelić, Željko Škrnjug, *NetSeT, Beograd*

Sadržaj – *U radu je opisan jedan primer realizacije sistema bezbednosti podataka u Web aplikaciji elektronskog bankarstva. Predstavljeni su neki elementi aplikativne zaštite zasnovani na softverskom kriptografskom modulu i primeni smart kartica kao pouzdanom nosiocu identiteta korisnika .*

1. UVOD

Sistem elektronskog bankarstva, kao paket usluga koje pruža svojim korisnicima putem javnih servisa Interneta, zahteva pouzdanu kontrolu autorizovanog pristupa i siguran prenos dozvoljenog skupa podataka. Zato je neophodno primeniti bezbednosne mehanizme zaštite podataka, imajući u vidu značaj i osetljivost informacija koje se razmenjuju.

Koristeći pojednostavljeni model jednog sistema koga čine korisnik (klijent), server (aplikativni server, web server ...) i baza podataka, potrebno je osigurati svaki segment sistema pojedinačno, ali i kao deo jedne funkcionalne celine. Rešenje koje će biti predstavljeno odnosi se na zaštitu podatka na relaciji klijent – server. Ono treba da obezbedi autentičnost korisnika, osigura integritet i tajnost podataka, i spreči svaku mogućnost eventualne zloupotrebe. Oslanjajući se na PKI (*Public Key Infrasturcture*) sistem infrastrukture javnih ključeva, rešenje je zasnovano je na RSA asimetričnom algoritmu [1] i simetričnim kriptografskim algoritmima [2]. Sve zahtevane funkcije grupisane su u aplikativnom programskom interfejsu, realizovanom u obliku klijentske i serverske *ActiveX* komponente koja se jednostavno integriše u *Web* aplikaciju elektronskog bankarstva.

Digitalni identitet korisnika, izražen u njegovom digitalnom certifikatu i odgovarajućem paru javnog i privatnog asimetričnog ključa, smešten je na *smart* kartici kao bezbednom nosiocu poverljivih podataka.

Pored tehničke podrške, neophodno je i odgovarajućim zakonskim aktima stvoriti sve pravne preduslove za funkcionisanje elektronskog poslovanja. Usvajanjem Zakona o elektronskom potpisu [3] očekuje se dalje širenje sistema elektronskog bankarstva, pri čemu njegova bezbednost dobija na većem značaju.

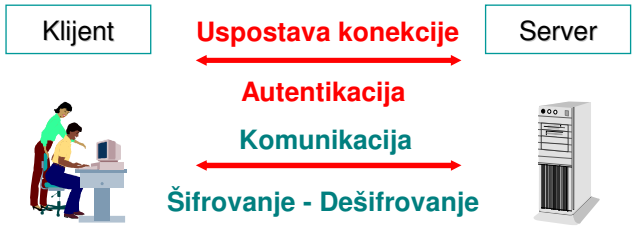
2. OPIS REŠENJA

Svaki korisnik sistema poseduje jedinstvenu *smart* karticu sa specifičnim kriptološkim parametrima. Ovi kriptološki podaci (par javnog i privatnog ključa dužine 1024 bita, digitalni certifikat po standardu X.509 verzija 3) generisani su u posebnom certifikacionom telu [4], zaduženom za PKI podršku, koje je sastavni deo višestepenog sistema zaštite podataka. Server takođe poseduje odgovarajuću *smart* karticu koja se aktivira na samom početku rada aplikacije.

Podržan je rad sa nekoliko različitih tipova kartica (*GemPlus, Authentic, StarCos, Java*) kapaciteta 16 KB ili 32 KB. To su mikroprocesorske kartice koje u sebi imaju ugrađen PKI koprocesor i mogu da izvršavaju kriptografske funkcije (digitalno potpisivanje , šifrovanje i dešifrovanje standardnim algoritmima, npr. DES...).

Softverski modul [5], pozivan na odgovarajućim stranama (htm, asp, jsp...) *Web* aplikacije, realizuje sve neophodne elemente zaštite. To su funkcije prijave i čitanja *smart* kartice, digitalnog potpisivanja i verifikacije potpisa, šifrovanja i dešifrovanja simetričnim algoritmima, digitalne koverte.

Imajući u vidu specifičnost bankarskog sistema i redosled operacija u eksploataciji, potrebno je (Sl.1): obezbediti autentikaciju korisnika, zaštititi vezu između klijenta i servera, izdati digitalnu potvdu izvršene aktivnosti (neporecivost).

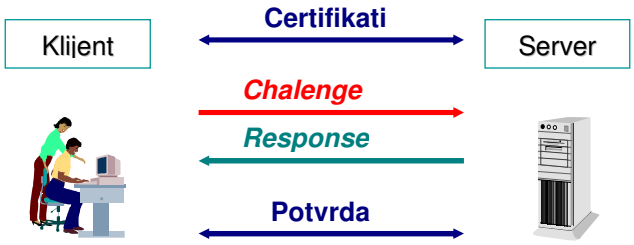


Sl.1. *Šema veze klijent – server*

Postupkom autentikacije neophodno je da se pouzdano utvrdi i proveri identitet korisnika. Korisnik se prijavljuje sistemu na osnovu onoga šta poseduje (kartica) i što zna (korisničko ime i lozinka). Unošenjem korisničkog imena i lozinke započinje proces dvostruke provere. Najpre se lokalno, preko klijentske *ActiveX* kontrole proverava prisustvo kartice korisnika i unetih podataka, i čitaju podaci sa nje. Korisničko ime i lozinka se, posebno razvijenim postupkom, transformišu u PIN kod (*Personal Identification Number*), koji dozvoljava pristup funkcijama i privatnim podacima na kartici. U slučaju neispravnog unosa tri puta zaredom, kartica se blokira i ne može se dalje koristiti. Na ovaj način se sprečava zloupotreba kartica neprestanim pokušajima predstavljanja (*brute force attack*). Blokirana kartica se mora prijaviti ovlašćenoj službi za deblokiranje, nakon čega se može nastaviti sa njenom upotrebom.

Posle uspešnog predstavljanja *smart* kartice, server nastavlja proceduru dalje provere. Pri tome se, zbog sigurnosti postupka, primenjuje višefazna "*challenge-response*" razmena podataka između klijenta i servera. U osnovi ove procedure (Sl.2.) je da

obe strane formiraju sopstveni deo poverljivih podataka koji se obostrano proveravaju. Na strani klijenta se generiše slučajan podatak ("*challenge*") i prosledi serveru. Server obrađuje "*challenge*", generiše svoj slučajan podatak i vraća transformisani odgovor ("*response*") klijentu. Obe strane proveravaju prispele podatke, na osnovu čega utvrđuju njihovu ispravnost i potvrđuju da mogu nastaviti dalji rad. U slučaju bilo koje neispravnosti, postupak se prekida i korisniku se onemogućava pristup sistemu.



Sl.2. *Autentikaciona "challenge - response" procedura*

Svi podaci su digitalno potpisani čime se garantuje njihova verodostojnost. Potpisani podaci se verifikuju digitalnim certifikatima učesnika, koji su razmenjeni i provereni na samom početku autentikacije.

Na ovaj način ostvaren je postupak jake autentikacije u toku koga su učesnici međusobno potvrdili svoj identitet. Server je nedvosmisleno utvrdio da je klijent zaista onaj za koga se izdaje, ali je i klijent utvrdio da je server upravo taj kome se prijavio.

Nakon izvršene autentikacije, korisnik zahteva usluge servera, pri čemu se prenos svih značajnih informacija (npr. transfer novca, nalozi za plaćanje, razne transakcije i izveštaji) odvija kroz bezbedni kripto tunel. Kripto tunel se uspostavlja na kraju autentikacije, kada se u toku višefazne razmene formira jedinstveni sesijski ključ koji se koristi u daljem toku komunikacije. Tako se svaki put kada se korisnik prijavi, obrazuje novi ključ koji se koristi samo u toj sesiji. Na ovaj način postignuta je tajnost podataka šifrovanjem i dešifrovanjem sesijskim ključem i simetričnim algoritmima, standardnim (AES, IDEA...) ali po zahtevu i namensko razvijanim.

Kako kvalitet primenjene zaštite zavisi od pouzdanosti ključeva, pored sesijskog ključa nastalog tokom autentikacije, generišu se i novi ključevi prilikom slanja osetljivih podataka. Za distribuciju novih ključeva koristi se metod digitalnog koverta. Tako je svaka poruka šifrovana različitim ključem.

Pored tajnosti podataka, neophodno je osigurati verodostojnost tj. integritet podataka. Integritet podataka je obezbeđen primenom metoda digitalnog potpisa, zasnovanom na RSA asimetričnom algoritmu. Digitalno potpisani podaci se šalju zajedno sa svojim potpisom, dok se na prijemnoj strani verifikuje njihov potpis, tako da se može jednoznačno utvrditi da poruka odgovara originalu i nije promenjena u toku prenosa. Svaki pokušaj nedozvoljene promene podataka ili njihovog potpisa, detektuje se i uzrokuje sprovođenje posebnih mera.

U zavisnosti od važnosti podataka, digitalno potpisivanje se obavlja na samoj kartici ili u softveru. Potpisivanje na kartici se primenjuje za aktivnosti koje zahtevaju lični potpis korisnika, jer tada njegov privatni ključ ne napušta karticu pa samim tim takav potpis dobija na većem značaju.

Kombinovanom primenom metoda digitalnog potpisivanja i šifrovanja, korisnik ostvaruje bezbednu komunikaciju i pristup raspoloživim resursima.

Drugi aspekt sigurnosti, specifičan za sistem elektronskog bankarstva, odnosi se na arhiviranje i potvrdu izvršenih aktivnosti (neporecivost). Neporecivost se u tim uslovima može posmatrati kao skup mera koje imaju za cilj da utvrde izvršavanje određenih elektronskih aktivnosti, kao i da provere identitet izvršioca i sam sadržaj. Zato je potrebno sve poverljive podatke digitalno potpisati, i sačuvati zajedno sa njihovim digitalnim potpisom. Tako se i posle dužeg vremena može izvršiti njihova verifikacija i proveriti identitet izvršioca. Na ovaj način sistem obezbeđuje da se ne može poreći obavljena aktivnost, niti tvrditi da je njen sadržaj drugačiji od verifikovanog.

Ovaj postupak je naročito važan u slučaju spora, i ima za cilj da pruži uslugu arbitriranja kako bi se utvrdilo pravo stanje. Zato je zbog velike osetljivosti podataka i odgovornosti koja se preuzima, neophodna podrška izražena odgovarajućim zakonskim regulativima, koje će precizno formulisati i definisati postupke, prava i obaveze svih učesnika sistema.

Klijenti mogu koristiti usluge sistema samo u periodu važenja njihovog digitalnog certifikata (obično 1 godina). U slučaju isteka certifikata, prijava korisnika se odbija. Tada se mora obratiti nadležnoj službi koja će ga uputiti kako da produži svoj digitalni certifikat. Najpre se formira zahtev za zanavljanjem certifikata, koji se prosleđuje certifikacionom telu. Certifikaciono telo obrađuje zahtev i generiše novi certifikat. Upisivanjem zanovljenog certifikata na karticu, korisnik može nastaviti sa radom u sistemu.

Kompleksnost opisanih procedura i složenost primenjenih algoritama, unose izvesno vremensko kašnjenje. Međutim, rezultati u svakodnevnoj praksi su pokazali da to ne utiče značajno na rad i ne ometa karakteristike sistema ni u slučajevima istovremenog pristupa većeg broja klijenata.

4. ZAKLJUČAK

Predstavljeno rešenje aplikativne zaštite podataka u *Web* aplikaciji elektronskog bankarstva, zasniva se na tehnologijama simetričnih i asimetričnih kriptografskih algoritama i digitalnog potpisivanja. *Smart* kartice se koriste kao bezbedan nosilac digitalnog identiteta korisnika, generisanog u certifikacionom telu.

Kriptografske funkcije implementirane u softverskom modulu, obezbeđuju pouzdanu autentičnost korisnika, sigurnu razmenu podataka i neporecivost izvršenih aktivnosti. Opisano rešenje predstavlja osnovu koja se može dalje razvijati u pravcu obezbeđivanja ostalih segmenata sistema i podrške novim servisima.

LITERATURA

[1] RSA Laboratories, *PKCS#1: RSA Encryption standard, Version 2*, 1999.

[2] B.Schneier, *Applied Cryptography*, Wiley & Sons, 1996.

[3] *Zakon o elektronskom potpisu*, Službeni glasnik RS, 135/04, 21.12.2004.

[4] G.Pantelić, Ž.Škrnjug, *Certifikaciono telo u PKI sistemu zaštite podataka,* XLVIII Konferencija ETRAN, Čačak, jun 2004.

[5] Ž.Škrnjug, G.Pantelić, *Kriptografski API –Softverski modul za zaštitu podataka,* XLVIII Konferencija ETRAN, Čačak, jun 2004.

Abstract – In this paper one data security system in electonic banking Web application is presented. Some elements of application data protection based on software cryptographic module and smart card usage as reliable carrier of digital user identity are described.

DATA SECURITY IN ELECTRONIC BANKING SYSTEM

Goran Pantelić, Željko Škrnjug