UPRAVLJANJE X.509 SERTIFIKATIMA U PKI SISTEMU

Xxxxx Xxxxx M.S.c
Univerzitet Singidunum
Danijelova 32, Beograd
Telefon: +38111xxxxxxxx
E-mail: xxxxxxxxxxx@singidunum.ac.rs

Saša Adamović M.S.c
Univerzitet Singidunum
Danijelova 32, Beograd
Telefon: +38111xxxxxxx
E-mail: xxxxxxxx@singidunum.ac.rs

Xxxxx Xxxxxxx M.S.c
Univerzitet Singidunum
Danijelova 32, Beograd
Telefon: +38111xxxxxxx
E-mail: xxxxxx@singidunum.ac.rs

Mr Xxxxxx Xxxxxx
Univerzitet Singidunum
Danijelova 32, Beograd
Telefon: +38111xxxxxx
E-mail: xxxxxxxxxx@singidunum.ac.rs

Sažetak – U ovom radu opisana je infrastruktura javnog ključa, njeni sastavni delovi, kao i prednosti i mane ovakvog sistema. Korisnici u elektronskom poslovanju svakodnevno izvršavaju hiljade transakcija razmenjujući svoje privatne i poslovne podatke. S' obzirom na nemogućnost tradicionalne provere identiteta korisnika (provera ličnih dokumenata) otvorena su vrata mnogim problemima kada je u pitanju sigurnost informacija. Ovaj rad analizira upravo moguća rešenja takvih problema zasnovana na izdavanju i upravljanju digitalnim sertifikatima.

Abstract - This paper describes a public key infrastructure, its components, as well as advantages and disadvantages of such a system. Users in the electronic business daily perform thousands of transactions by exchanging their private and business data. The inability of traditional user authentication (verification of identity documents) opened the door to many problems when it comes to information security. This paper precisely analyzes possible solutions to such problems based on the issuing and managing of digital certificates.

1 UVOD

Tema ovog rada jeste razmatranje rešenja koje postoje i koriste se danas, a odnose se na probleme identifikacije korisnika prilikom razmene osetljivih podataka i informacija. Neki od najčešćih sigurnosnih problema su izmena podataka, izmišljanje podataka, prisluškivanje podataka, prekidanje komunikacionih kanala, kao i lažno predstavljanje korisnika. Svi ovi problemi mogu dovesti do krađe brojeva kreditnih kartica, kreditnih računa, jedinstvenih matičnih brojeva ili izmene brojeva bankovnih računa. Lažno predstavljanje podrazumeva lažiranje samog izvora informacije da bi se primaocu dostavile izmišljene ili stare poruke. Sistem javnih ključeva (*eng. Public Key Infrastructure* ili skraćeno PKI) osmišljen je da bi ponudio rešenje ovih problema.

U ovom radu posebna pažnja usmerena je na digitalni sertifikat, dokument koji povezuje javni ključ sa njegovim vlasnikom. Izdavanje i upotreba digitalnih sertifikata pomaže učesnicima u komunikaciji da razmenjuju dokumenta ili informacije, sigurni u identitet svog sagovornika. Validan sertifikat mora biti digitalno potpisan da bi se osigurao njegov integritet, za koji je odgovoran potpisnik takvog sertifikata. Sve ovo kao i pojava savremene komunikacije preko Interneta kao nesigurnog kanala, dovelo je do realizacije PKI sistema koji omogućuje sigurnu komunikaciju preko nesigurnog kanala.

2 KRIPTOGRAFIJA SA JAVNIM KLJUČEM

Sigurnost simetričnih kriptosistema zavisi od tajnosti ključa, što može da predstavlja i njihov veliki nedostatak. Pošiljalac i primalac pre samog šifrovanja podataka moraju razmeniti tajni ključ putem komunikacionih kanala što predstavlja veliki izazov i potencijalni problem. Sigurnost sistema koji koriste jedan ključ za šifrovanje i dešifrovanje opada povećanjem broja poruka koje treba šifrovati, jer podrazumeva čestu razmenu tajnih ključeva. Rešenje ovih problema ponudili su 1976 godine Whitfield Diffie i Martin Hellman. Njihovo rešenje je podrazumevalo uspostavljanje metode koja je postala poznata pod nazivom „razmena ključeva Difi-Helman“, i bila je prva praktična metoda uspostavljanja sigurne veze preko nezaštićenih kanala bez unapred dogovorene lozinke. Od 1970 tih godina do danas, razvijen je veliki broj različitih načina kriptovanja, digitalnog potpisivanja, usaglašavanja ključevima i drugih tehnika na polju kriptografije sa javnim ključem. Kriptosistemi zasnovani na konceptu javnog ključa podrazumevaju šifrovanje osnovnog teksta gde se ključ za šifrovanje razlikuje od ključa za dešifrovanje. Drugim rečima, u upotrebi su javni i privatni ključ. Funkcija šifrovanja algoritmom sa javnim ključem, na osnovu javnog ključa i ulaznih podataka proizvodi šifrat. Funkcija dešifrovanja na osnovu privatnog ključa i šifrata proizvodi originalnu poruku. Javni ključ je poznat onim osobama sa kojima korisnika želi da komunicira, dok je tajni ključ poznat samo korisniku koji dešifruje poruku.

Sigurnost asimetričnih algoritama zasniva se na vrlo teškoj mogućnosti izračunavanja privatnog ključa iz javnog kjuča. Ovi algoritmi se ne koriste pri šifrovanju velikog broja poruka. Njihova glavna uloga je razmena ključeva pre početka komunikacije između pošiljaoca sa jedne strane i primaoca sa druge. Iz ovog razloga kriptografija sa javnim ključem nije zamena za simetrične kriptosisteme. U ovom radu analiziraćemo sve delove kriptosistema sa javnim ključem, a posebnu pažnju posvetiti upravljanju digitalnim sertifikatima.

2.1 INFRASTRUKTURA JAVNOG KLJUČA

Infrastruktura javnog ključa ili PKI (*eng. Public Key Infrastructure*) je celokupan sistem koji povezuje korisnike, digitalne sertifikate, sertifikacioni autoritet kao i bazu važećih i nevažećih sertifikata. Centralno mesto sistema predstavlja sertifikacioni autoritet ili CA (*eng. Certificate authority*) koji vrši proveru identiteta svih strana u komunikaciji poređenjem para ključeva. Svaki korisnik u komunikaciji ima svoj par ključeva. Identitet korisnika je jedinstven unutar sertifikacionog autoriteta. Registracija i izdavanje sertifikata koje se odvija u okviru sertifikacionog centra, omogućava povezivanje korisnika sa njegovim identitetom. U nastavku rada prikazan je primer korišćenja PKI sistema za autentifikaciju korisnika:

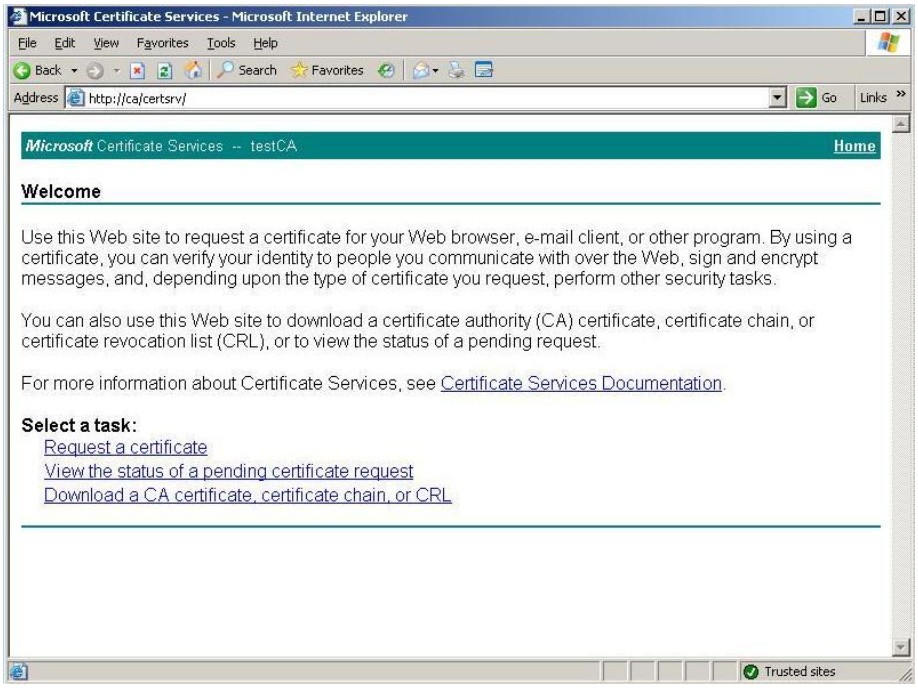
- osoba A dostavlja osobi B svoj identifikator u poruci M_1
- po prijemu poruke osoba B generiše slučajan broj N i šalje ga osobi A u poruci M_2
- osoba A po prijemu poruke M_2 šifruje svojim privatnim ključem generisani broj N i vraća poruku M_3
- poruku M_4 osoba B će poslati sertifikacionom centru sa kodom kojim se zahteva sertifikat osobe A pomoću njenog identifikatora
- administracija sertifikacionog centra odgovara porukom M_5 u kojoj šalje osobi B šifrovanu poruku sa podacima osobe A pomoću svog privatnog ključa
- poruku M_5 osoba B će dešifrovati javnim ključem administracije sertifikacionog centra i na taj način saznati ključ osobe A kojim može dešifrovati raniju poruku M_3, odnosno generisani slučajni broj N
- dobijeni rezultat se upoređuje sa originalom čime komunikacija sa osobom A može biti prihvaćena ili odbačena

PKI omogućuje sigurnu komunikaciju za korisnike koji se ne poznaju ili razmenjuju poruke sa udaljenih lokacija. Poverenje prilikom komunikacije između korisnika se ostvaruje kroz sertifikacioni centar. Ovakva komunikacija može da predstavlja i problem za korisnike koji u njoj učestvuju. Prvi problem koji se može pojaviti otvara pitanje kom centru odnosno trećoj strani se može verovati. Svaka izmena koju korisnik želi da napravi na svom sertifikatu povlači stavljanje tog sertifikata na listu nevažećih. U tom slučaju mora se izdati novi sertifikat. Dugačke liste opozvanih sertifikata (*eng. Certificate Revocation List*) takođe mogu biti potencijalni problem. Uprkos navedenim problemima PKI sistem ima veliku ulogu u kriptografiji danas. Kombinovanjem sistema (simetrični i asimetrični) može se unaprediti sigurnost sistema. Kada je reč o sigurnosti informacija, jako teško se ostvaruje apsolutna zaštita podataka koji moraju biti tajni. Na dizajnerima sigurnosnih sistema je da sve njegove delove maksimalno obezbede, a da bi u tome uspeo kombinacija više šifarskih sistema može dovesti do zadovoljavajućih rezultata.

2.1.1 SERTIFIKACIONI CENTAR

Sertifikacioni centar (*eng. Certificate authority*, CA) predstavlja centralni deo infrastrukture javnih ključeva. CA generiše, izdaje i poništava sertifikate. CA ima i ulogu potpisivanja sertifikata svojim privatnim ključem. Korišćenjem javnog ključa sertifikacionog centra, svako može proveriti integritet sertifikata. Zbog velike važnosti ove komponente, u slučaju napada CA se brani metodom samouništenja.To podrazumeva uništenje svih ključeva.

Na Windows serverskim operativnim sistemima moguće je instalirati poseban servis koji bi predstavljao sertifikaciono telo. Pitanje koje se postavlja je ko bi verovao takvom sertifikacionom telu. Za potrebe ovog rada implementirano je rešenje koje je podržano u okviru Windows platforme. Na taj način sagledaćemo primer sertifikacionog centra i upravljanje digitalnim sertifikatima. Međutim u realnom okruženju postoje kompanije koje izdaju sertifikate, kojima se može verovati i koji su podržani od strane intenet browsera. Neke od najpoznatijih kmpanija iz ove oblasti su: VeriSign, Entrust Authority i Comodo inc.



Slika 1. Postupak izdavanja sertifikata od strane CA implementiranog na Windows platformi

2.2 DIGITALNI POTPIS

Verodostojnost neke poruke se može dokazati upotrebom digitalnog potpisa. U nastavku rada dajemo primer upotrebe digitalnog potpisa:

- osoba A šalje poruku osobi B i pri tom želi da osoba B bude sigurna da poruka nije promenjena.
- osoba A prvo izračunava heš vrednost poruke. Ta vrednost se zatim šifruje privatnim ključem osobe A i dodaje poruci koja se u tom obliku šalje osobi B.
- Posle ovih koraka osoba B je u mogućnosti da proveri validnost poruke. Potpis se dešifruje javnim ključem osobe A.
- Dobijeni rezultat predstavlja heš vrednost poruke koju je izračunala osoba A. Zatim osoba B izračunava heš vrednost poruke.
- Dobijena heš vrednost iz prethodnog koraka se upoređuje sa rezultatom koji je posledica izračunavanja heš vrednosti osobe A. Ukoliko su te vrednosti iste, dolazi se do zaključka da poruka nije menjana na putu do osobe B.

Iz prethodnog primera sledi da se uz pomoć digitalnog potpisa može utvrditi identitet pošiljaoca poruke kao i integritet iste.

2.3 DIGITALNI SERTIFIKAT

Digitalni sertifikat (*eng. certificate*) je potpisan dokument koji omogućava korisnicima i organizacijama proveru identiteta učesnika u komunikaciji. Sertifikat se digitalno potpisuje da bi se utvrdila veza između korisnika i javnog ključa. Javni ključ, korisnički identitet, informacije o vlasniku sertifikata i digitalni potpis su sastavni delovi sertifikata. Upotrebom digitalnih sertifikata obezbeđuju se sledeći sigurnosni parametri:

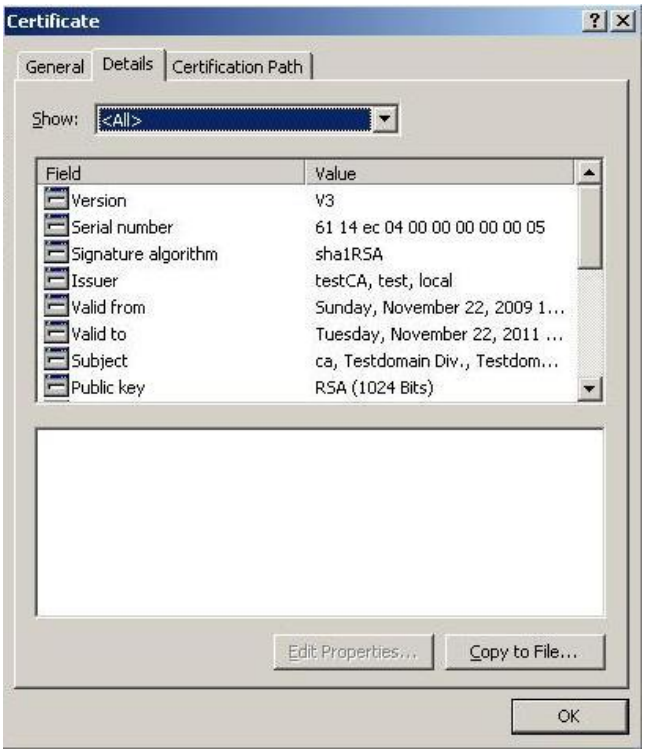
- Identitet korisnika
- Integritet poruke
- Autorizacija
- Neporicanje

Upotreba digitalnih sertifikata rešava neke od ključnih problema zaštite informacija. Ukoliko nam poruka stiže od korisnika čiji identitet utvrđujemo potpisom treće strane kojoj se veruje, nema razloga da sumnjamo da je takva poruka kompromitovana, odnosno da je stigla od osobe koje je neovlašteno presrela komunikaciju. U nastavku rada pažnja se posvećuje formi odnosno standardu digitalnih sertifikata koji se koristi danas.

2.3.1 DIGITALNI SERTIFIKAT U SISTEMU JAVNIH KLJUČEVA PREMA STANDARDU X.509

Format X.509 određuje format zapisa i definiše polja sertifikata. Ovaj standard takođe predviđa načine povlačenje sertifikata kao i algoritme za šifrovanje. Prvi PKI projekat je podrazumevao upotrebu upravo X.509 standarda. Mnoge kompanije u svetu svoje poslovanje temelje na ovom standardu. VISA i MasterCard kao u svojim elektronskim transakcijama primenjuju X.509 standard. U nastavku rada dajemo pregle strukture X.509 sertifikata verzje 3.

- Verzija sertifikata – označava verziju sertifikata koji se upotrebljuje.
- Serijski broj – jedinstveni broj koji izdaje CA. Pravi razliku itmeđu sertifikata.
- Identifikator algoritma – identifikuje algoritma kojim je CA potpisao sertifikat.
- Izdavač sertifikata – označava potpisnika sertifikata (CA).
- Validnost sertifikata – svaki sertifikat je validan u određenom vremenskom periodu. Taj vremenski period je propisan datumom početka i datumom kraja validnosti sertifikata.
- Naziv entiteta – povezuje privatni ključ sa javnim ključem iz sertifikata.
- Podaci o javnom ključu entiteta – sadrži javni ključ entiteta zajedno sa identifikatorom kriptografskog algoritma.
- Identifikator izdavača – jedinstveno polje koje identifikuje ime izdavača prema X.500 standardu
- Identifikator entiteta – jedinstveno polje koje identifikuje entitet.
- Proširenja – propisana u verziji 3 digitalnih sertifikata. Definiše standarde proširenja verzije 2 digitalnih sertifikata.
- Digitalni potpis sertifikata – identifikuje potpis sertifikata privatnim ključem sertifikacionog centra.



Slika 2. Struktura digitalnog sertifikata izdatog od strane CA implementiranog na Windows platformi

3 ZAKLJUČAK

U ovom radu cilj je bio analiza i sagledavanje prednosti i mana korišćenja digitalnih sertifikata pri utvrđivanju identiteta korisnika i integriteta poruka koje se šalju. Pre samog uspostavljanja PKI sistema potrebno je jasno definisati njegovu ulogu, okruženje u kojem će funkcionisati, kakvu sigurnost će pružiti u datim uslovima, kao i isplativost takvog rešenja. U veoma složenoj oblasti zaštite informacija sistem koji je opisan u radu daje zadovoljavajuća rešenja koja se koriste danas u realnom informatičkom okruženju. Da bi PKI sistem bio uspešan potrebno ga konstantno nadograđivati. Na taj način sistem postaje sigurniji, lakše se koristi, a učesnici u komunikaciji postaju bezbedniji prilikom razmene poverljivih informacija, ukoliko su naravno i oni sami registrovani u okviru PKI sistema. Rad i istraživanja u ovoj oblasti međutim upućuju na nove pravce kretanja u kriptografiji. U skladu sa tim pažnju je potrebno usmeriti ka kvantnoj kriptografiji i čini se nanovo razmotriti prednosti i mane simetričnih šifarskih sistema.

LITERATURA

[1] Alfred J. Menezes: *Handbook of Applied Cryptography,* P. C. 1996

[2] D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: *Sigurnost računarskih sistema i mreža.* Mikro knjiga, 2007

[3] Goldreich O: *Foundations of Cryptography.* Outside North America Publishers Inc. 2005

[4] Stamp M: *Information Security.* JohnWiley & Sons, Inc. 2006

[5] S. Vaudenay *A classical introduction to cryptography: application for communications security*. Springer Science Business Media Inc, 2006

[6] W. Stallings: *Cryptography and Network Security*. Pearson Education Inc, 2006

[7] http://os2.zemris.fer.hr

BESPLATNI GOTOVI SEMINARSKI, DIPLOMSKI I MATURSKI RAD.

RADOVI IZ SVIH OBLASTI, POWERPOINT PREZENTACIJE I DRUGI EDUKATIVNI MATERIJALI.

WWW.SEMINARSKIRAD.ORG

WWW.MATURSKIRADOVI.NET

WWW.MATURSKI.NET

WWW.SEMINARSKIRAD.INFO

WWW.MATURSKI.ORG

WWW.ESSAYSX.COM

WWW.FACEBOOK.COM/DIPLOMSKIRADOVI

NA NAŠIM SAJTOVIMA MOŽETE PRONAĆI SVE, BILO DA JE TO SEMINARSKI, DIPLOMSKI ILI MATURSKI RAD, POWERPOINT PREZENTACIJA I DRUGI EDUKATIVNI MATERIJAL. ZA RAZLIKU OD OSTALIH MI VAM PRUŽAMO DA POGLEDATE SVAKI RAD, NjEGOV SADRŽAJ I PRVE TRI STRANE TAKO DA MOŽETE TAČNO DA ODABERETE ONO ŠTO VAM U POTPUNOSTI ODGOVARA. U BAZI SE NALAZE GOTOVI SEMINARSKI, DIPLOMSKI I MATURSKI RADOVI KOJE MOŽETE SKINUTI I UZ NJIHOVU POMOĆ NAPRAVITI JEDINSTVEN I UNIKATAN RAD. AKO U BAZI NE NAĐETE RAD KOJI VAM JE POTREBAN, U SVAKOM MOMENTU MOŽETE NARUČITI DA VAM SE IZRADI NOVI, UNIKATAN SEMINARSKI ILI NEKI DRUGI RAD RAD NA LINKU IZRADA RADOVA. PITANjA I ODGOVORE MOŽETE DOBITI NA NAŠEM FORUMU ILI NA MATURSKIRADOVI.NET@GMAIL.COM