

VALIDACIJA ELEKTRONSKIH SERTIFIKATA U SAVREMENIM PKI SISTEMIMA

Đuro Alfirević, *Vojna akademija – Odsek logistike, Beograd,*
djalfirevic@gmail.com

Rezime: *Zaštićena komunikacija preko nesigurnog medijuma, kakav je Internet, predstavlja jednu od ključnih komponenti u domenu obezbeđivanja neophodnih bezbednosno-kritičnih zahteva, kako bi se tok informacija odvijao nesmetano.*

Ključne reči: PKI, kriptografija, S/MIME, digitalni sertifikat

ELECTRONIC CERTIFICATES VALIDATION IN MODERN PKI SYSTEMS

Abstract: *Secured communication across unsecured medium, such as Internet, presents one of the major component in a domain of providing necessary security-critical demands, so the flow of information could go undisturbed.*

Key words: PKI, cryptography, S/MIME, digital certificate

UVOD

Savremene računarske mreže se, skoro u potpunosti, zasnivaju na Internet tehnologijama i TCP/IP (*Transfer Control Protocol/Internet Protocol*) protokolima. Automatizovani informacioni sistemi zasnovani na Internet tehnologijama imaju brojne slabosti sa aspekta zaštite bezbednosti podataka, što je u velikoj meri prouzrokovano arhitekturom računarske mreže Internet/Intranet tipa:

- TCP/IP protokoli nisu projektovani da zadovolje zahteve za zaštitom informacija
- Internet je mreža sa komutacijom paketa u kojoj se relativno jednostavno pristupa informacijama koje se prenose i moguće je ubacivanje poruka uz nemogućnost kasnijeg određivanja njihovog porekla i sadržaja

Kriptografija je tehnika koja se bavi proučavanjem načina generisanja poruka takvih da je njihov informacioni sadržaj poznat samo ovlašćenim korisnicima. S tim u vezi, primenom kriptografije, omogućena je realizacija četiri osnovna bezbednosna servisa:

- tajnost podataka,
- provera autentičnosti,
- provera integriteta primljenih podataka, i
- neporecivost transakcija.

Zaštita tajnosti podataka se vrši primenom simetričnih kriptografskih algoritama, dok se ostali servisi realizuju primenom asimetričnih kriptografskih algoritama. Savremena rešenja sistema zaštite karakteriše višeslojna arhitektura, sa upotrebom hardverskih bezbednosnih modula (*Hardware Security Module*). Upotrebom hardverskih bezbednosnih modula se najčešće ostvaruje zaštita bezbednosno kritičnih podataka, kao što su kriptografski ključevi, korisničke šifre i privatni algoritmi zaštite, bezbedna realizacija kriptografskih algoritama i drugih funkcija zaštite nezavisno od ostalih programa na PC računaru i ubrzavanje izvršavanja kriptografskih algoritama u odnosu na sisteme bazirane na isključivo softverskim postupcima zaštite.

U ovom radu je istaknut značaj realizacije infrastrukture sistema sa javnim ključevima, što je osnovni preduslov za uspostavljanje pouzdanog digitalnog identiteta na nivou računarske mreže. Zatim su objašnjeni pojam i primena digitalnih sertifikata u okviru infrastrukture sistema sa javnim ključevima. Dat je i osnovni koncept Java kriptografskog provajdera, i konačno, realizovana je aplikacija koja pruža mogućnost slanja kriptografski zaštićenih poruka elektronske pošte, uz pomoć programskog jezika Java™, firme Sun Microsystems, Inc.

1. DIGITALNI SERTIFIKATI

Asimetrični kriptografski algoritmi se zasnivaju na postojanju para ključeva: javnog i privatnog. Privatni ključ je strogo čuvana tajna poznata samo vlasniku para ključeva, dok je njegov javni ključ dostupan svim subjektima komunikacije. Jednoznačnost veze između javnog ključa i njegovog vlasnika se ostvaruje primenom digitalnih sertifikata, na bazi tehnologije digitalnog potpisa i tehnologija koje omogućuju pouzdano funkcionisanje infrastrukture sistema sa javnim ključevima. Struktura digitalnog sertifikata je prikazana na slici 1.

Slika 1: Struktura digitalnog sertifikata

Verzija formata sertifikata(v3) - x.509
Serijski broj sertifikata
Identifikator algoritma kojim se vrši digitalni potpis
Naziv certifikacionog tela koje je izdalo certifikat
Rok važnosti sertifikata
Vlasnik sertifikata
Javni ključ vlasnika sertifikata
Određeni specifični podaci koji se odnose na uslove korišćenja sertifikata
Digitalni potpis sertifikata tajnim ključem certifikacionog tela

Digitalni sertifikati praktično predstavljaju jednoznačne identifikacione parametre subjekata u komunikaciji – “digitalnu ličnu kartu.”

Elementi koji čine strukturu digitalnog sertifikata su:

- format sertifikata predstavlja oznaku strukture digitalnog sertifikata. Jedan od najzastupljenijih formata digitalnih sertifikata je definisan X509 standardom. Poslednja verzija ovog standarda je v3.
- Svaki digitalni sertifikat izdat od strane nekog certifikacionog tela ima svoj jedinstveni serijski broj. Sertifikat je jedinstveno određen nazivom certifikacionog tela koje ga je izdalo i svojim serijskim brojem.
- Rok važnosti sertifikata predstavlja vremenski period u kome je izdati sertifikat validan. U sistemima visoke sigurnosti, digitalni sertifikati se izdaju na period od šest meseci ili kraći, sprečavajući na taj način napad primenom kriptanalize.
- Vlasnik sertifikata je predstavljen složenom strukturom koja obuhvata nekoliko ličnih podataka:
 - o Ime vlasnika,
 - o Naziv organizacije u kojoj je zaposlen,
 - o Naziv niže organizacione celine,
 - o Naziva mesta u kome stanuje,
 - o Dvoslovni niz koji označava državu,
 - o Region u okviru države.
- javni ključ matematičkog para ključeva (javni-privatni kojeg poznaje samo vlasnik).
- sertifikat je digitalno potpisan od strane certifikacionog tela koje ga je izdalo. Ovim potpisom se garantuje integritet sertifikata.
- Radi mogućnosti provere digitalnog potpisa, jedno od polja digitalnog sertifikata je identifikator algoritma korišćenog za kreiranje digitalnog potpisa.

Uloga digitalnog sertifikata je da dovede u jednoznačnu vezu fizički identitet subjekta sa njegovim javnim ključem. Kreiranje i digitalno potpisivanje sertifikata vrši “treća strana od poverenja” (*trusted third party, TTP*). Ukoliko prijemna strana uspešno verifikuje dobijeni sertifikat, onda je ona sigurna u autentičnost pošiljaoca poruke – vlasnika odgovarajućeg tajnog ključa.

2. INFRASTRUKTURA SISTEMA SA JAVNIM KLJUČEVIMA

Osnovna funkcija sistema sa javnim ključevima je pouzdano uspostavljanje digitalnog identiteta subjekata u okviru računarske mreže. U savremenim sistemima zaštite, osnovni nosioci digitalnog identiteta su digitalni sertifikati.

Već je napomenuto da digitalni sertifikati predstavljaju jednoznačne identifikacione parametre subjekata u komunikaciji.

Infrastruktura sistema za primenu javnih ključeva predstavlja kombinaciju hardverskih i softverskih elemenata za realizaciju funkcija sistema sa primenom javnih ključeva. Postoji više mogućih načina da se realizuje PKI (*Public Key Infrastructure*). Njegova osnovna uloga je pouzdano uspostavljanje digitalnog identiteta subjekata u okviru mreže, baziranog na upotrebi digitalnih sertifikata. Time se stvara bezbedno okruženje za realizaciju drugih bezbednosnih servisa, prvenstveno onih kod kojih je od značaja autentičnost subjekata koji komuniciraju. Drugim rečima, uspostavljanje infrastrukture sistema sa javnim ključevima je osnovni preduslov za realizaciju sistema zaštite. Usluge PKI sistema se koriste na svim nivoima zaštite računarskih resursa i mreža. Primeri aplikacija zaštite zasnovanih na PKI sistemima su:

- Formiranje virtualne privatne mreže (*VPN - Virtual Private Network*);
- Formiranje pouzdanog sistema zaštite na transportnom nivou u računarskoj mreži;
- Zaštićen *E-mail* servis;
- Bezbedna razmena dokumenata.

Infrastruktura sistema za primenu javnih ključeva sastoji se iz sledećih funkcionalnih komponenti:

- sertifikacionog tela (*Certification Authority, CA*), koje izdaje digitalne sertifikate i reguliše način njihove upotrebe,
- registracionih tela (*Registration Authority, RA*), koja predstavljaju interfejs za podnošenje zahteva za izdavanje sertifikata,
- komunikacionog sistema za razmenu podataka između registracionog i sertifikacionog tela – distribuciju zahteva za izdavanje sertifikata i slanje digitalnih sertifikata,
- kriptografskih aplikacija za realizaciju funkcija PKI sistema,
- subjekata koji komuniciraju u mrežnom okruženju, na bazi izdatih digitalnih sertifikata,

Sertifikaciono telo je autoritet sa najvećim stepenom poverenja u PKI sistemu. Sertifikacioni autoritet svojim digitalnim potpisom garantuje asocijaciju odgovarajućeg subjekta i njegovog javnog ključa. Neke od osnovnih funkcija CA su:

- Izdavanje digitalnih sertifikata,
- Publikovanje sertifikata na X500/LDAP serveru,
- Upravljanje rokom važnosti,
- Upravljanje procedurom povlačenja sertifikata, itd.

3. S/MIME PROTOKOL

Danas, verovatno jedan od najkorišćenijih protokola na aplikativnom nivou je S/MIME (*Secure Multipurpose Internet Mail Extension*). S/MIME aplikacije se ugrađuju u softverske pakete koji su danas najdominantniji na tržištu, od kojih su neki: *Netscape Communicator, Microsoft Outlook, Mozilla Firefox*, itd.

S/MIME je baziran na popularnom Internet MIME (*Multipurpose Internet Mail Extension*) standardu i on obezbeđuje sledeće kriptografske usluge po pitanju sigurnosti za aplikacije tipa elektronskih razmena poruka: autentifikacija, integritet poruke i neporecivost (koristeći digitalni potpis), i tajnost podataka (digitalnu envelopu).

S/MIME može biti korišćen od strane tradicionalnih korisničkih poštanskih agencija (*Mail User Agents*, MUA) kako bi se pošti koja je poslata, dodale kriptografske bezbednosne usluge i kako bi se interpretirale kriptografske bezbednosne usluge u pošti koja je primljena.

Međutim, S/MIME nije ograničen samo na elektronsku poštu; može se koristiti sa bilo kojim transportnim mehanizmom koji transportuje MIME podatke, kao što je HTTP (*HyperText Transfer Protocol*). Osim toga, S/MIME može biti primenjen u agentima automatizovanog prenosa poruka koji koriste kriptografske bezbednosne usluge koje ne zahtevaju bilo kakvu intervenciju čoveka, kao što je potpisivanje softverski generisanih dokumenata i šifrovanje fax poruka koje se šalju preko Interneta.

MIME standard pruža generalnu strukturu sadržaja Internet poruka i odobrava ekstenzije za aplikacije novog sadržaja.

4. REALIZACIJA SOPSTVENOG REŠENJA

Programska rešenja su realizovana u programskom jeziku Java, što ima svojih dobrih i loših osobina.

Specifikacija Jave obuhvata dve relativno nezavisne celine: specifikaciju Java programskog jezika i specifikaciju Java Virtuelne Mašine (JVM). Specifikacija Java programskog jezika se značajnije ne razlikuje od specifikacija drugih objektno orijentisanih jezika, dok specifikacija JVM predstavlja novinu u odnosu na druge objektno orijentisane jezike opšte namene. Specifikacija Java Virtuelne Mašine predstavlja platformu za izvršavanje programa u čijoj osnovi se nalazi programski model imaginarnog – Java procesora. Programi napisani programskim jezikom Java se prevode za izvršavanje na Java platformi. Tačnije, izlaz iz procesa prevođenja Java programa predstavlja odgovarajuća sekvenca *bytecode* instrukcija – asemblerskih direktiva Java procesora. Za izvršavanje na konkretnoj računarskoj platformi, neophodno je postojanje odgovarajućeg interpretera, koji ostvaruje funkcionalnost zamišljenog procesora tako što preslikava skup *bytecode* instrukcija, u skup instrukcija karakterističnih za ciljnu platformu.

Posledica ovakve politike je smanjena efikasnost Java programa, uz obezbeđenu prenosivost na sve računarske platforme za koje postoji realizovana JVM. Za povećanje efikasnosti Java programa koriste se takozvani JIT (*Just-In-Time*) kompajleri, koji pod izvesnim okolnostima mogu da ubrzaju izvršavanje programa 10 do 50 puta [2]. Osnovna ideja upotrebe JIT tehnika je da se prilikom prvog poziva neke metode, izvrši prevođenje Java *bytecode* instrukcija koje je čine, u sekvencu instrukcija koje se neposredno izvršavaju na konkretnoj platformi (*native code*). Svaki sledeći poziv ove metode se direktno preslikava u sekvencu instrukcija koje se neposredno izvršavaju [2].

Uvođenje originalnog koncepta prenosivosti programa na nivou izvršnog kôda je imalo brojne posledice. Ovaj koncept je, zahvaljujući pogodnostima koje pruža, veoma brzo našao veliku primenu u svetu proizvođača smart kartica i mobilnih telefona, omogućavajući da se za veliki broj mikroracunara različitih proizvođača (sa podrškom za Javu), softver razvija na identičan način, upotrebom istog programskog jezika.

Osnovni cilj u dizajnu arhitekture kriptografskog podsistema u Javi bio je da se razdvoje kriptografski postupci i metode od svoje algoritamske implementacije. Osmišljena je tako da omogućava različitim subjektima da obezbede sopstvene realizacije kriptografskih algoritama i funkcija. Providerska arhitektura ima za cilj definisanje standardnog interfejsa prema programeru koji koristi kriptografske funkcije, nezavisno od konkretnog algoritma ili njegove implementacije.

Klasa koja praktično čini kostur kriptografskog podsistema je klasa *Provider*.

Provider je klasa iz paketa **java.security** koja povezuje nazive algoritama sa nazivima klasa koje ih realizuju. Izvedena je iz klase *Properties* definisane u paketu **java.util** i predstavlja asocijativni niz u kome je ključ – naziv algoritma, vrednost kojoj se pristupa – puno ime klase koja realizuje dati algoritam.

Security je klasa iz paketa **java.security**, koja sadrži listu provajdera i metode karakteristične za liste – za dodavanje i brisanje elemenata, itd., čije su sve metode statičke. Time je omogućeno da u jednoj instanci Java virtuelne mašine postoji samo jedan objekat klase *Security*. Da bi se koristile implementacije algoritama koje pruža određeni provajder, neophodno je da se dati provajder registruje – doda u listu objekta *Security*.

5. IMPLEMENTACIJA

Pre svega, potrebno je napomenuti da aplikacija predstavlja *stand-alone* Java program, za slanje poruka elektronske pošte, putem SMTP (*Simple Mail Transfer Protocol*) servera. Korisniku sistema je praktično omogućeno slanje tri tipa e-mail poruka. To su:

- *Data*,
- *SignedData*,
- *EnvelopedData* i
- *SignedAndEncryptedData*.

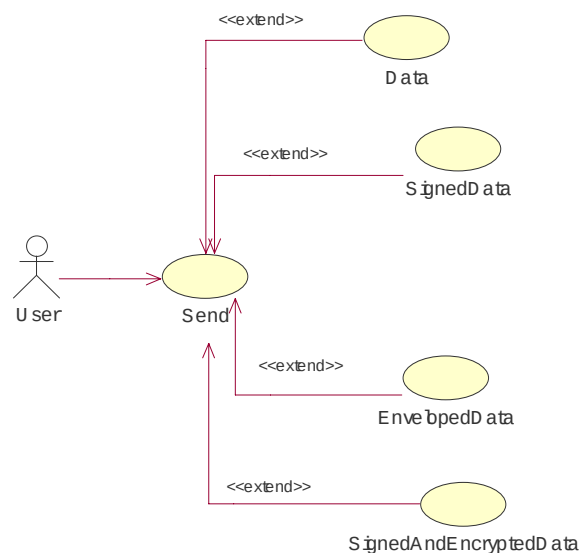
Radi konciznije predstave implementacije softverskog rešenja primenjeni su dijagrami unifikovanog jezika za modelovanje (*Unified Modeling Language, UML*).

Na slici 2 je prikazan dijagram slučajeva upotrebe (*Use Case Diagram*), dijagram koji prikazuje slučajeve upotrebe i aktere, kao i njihove relacije. Ovim dijagramom se predstavlja statički pogled na funkcionalnost (ponašanje) sistema. Takođe, preko ovih dijagrama se može modelovati kontekst sistema: granice sistema i akteri koji sa njime interaktivno deluju, zatim funkcionalni zahtevi sistema, sa aspekta šta sistem treba da radi, nezavisno od toga kako to iznutra treba da radi [3].

Kao što dijagram pokazuje, korisniku je omogućeno slanje osnovnih poruka, potpisanih poruka, šifrovanih i potpisanih poruka, i slanje digitalne envelope.

Uz upotrebu **javax.swing** i **java.awt** paketa, realizovan je grafički korisnički interfejs (*Graphical User Interface, GUI*) koji je prikazan na slici 3.

Slika 2: Dijagram slučajeva upotrebe sopstvenog rešenja

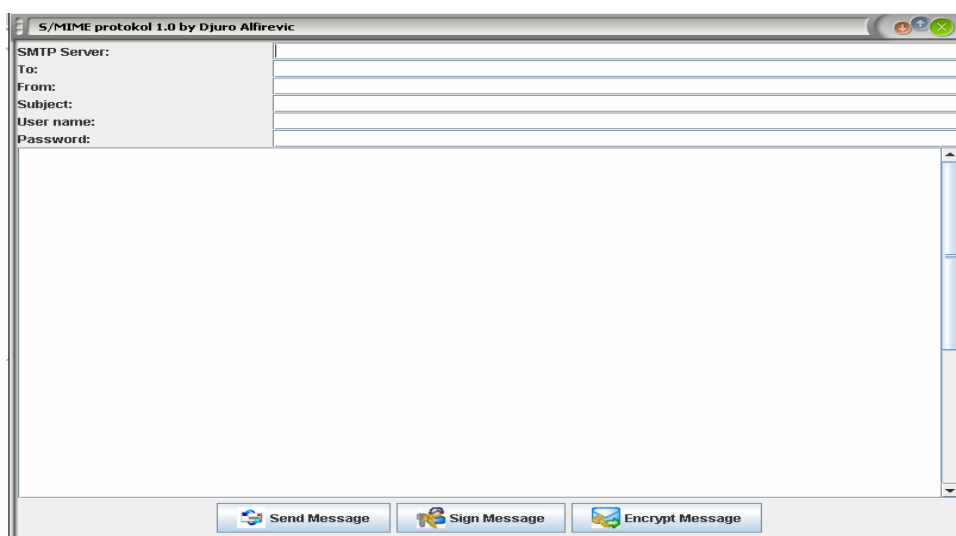


Puna funkcionalnost sistema, realizovana je upotrebom *BouncyCastle* provajdera, koji pruža servise neophodne za slanje S/MIME tipova poruka.

Osnovne klase *BouncyCastle* provajdera za realizovanje bezbednosnih proširenja standardnih poruka elektronske pošte, MIME tipa, su *SMIMESignedGenerator* i *SMIMEEnvelopedGenerator*.

BouncyCastle provajder je zasnovan na postojećim PKCS (*Public Key Cryptography Standard*) standardima vezanim za tipove podataka na koje se mogu primeniti bezbednosna proširenja.

Slika 3: Grafički korisnički interfejs



Sa slike se vidi da je korisniku omogućeno slanje potpisanih i šifrovanih poruka, odabirom obe opcije *Sign Message* i *Encrypt Message*, zatim omogućeno mu je slanje digitalno potpisanih poruka i slanje digitalne envelope, odabirom opcija *Sign Message* i *Encrypt Message*, respektivno.

6. ZAKLJUČAK

Ovim radom je praktično izložen koncept pouzdane arhitekture za prenos informacija kakva je neophodna u današnjim poslovnim sistemima. Sistem koji je realizovan pruža mogućnost slanja kriptografski zaštićenih poruka elektronske pošte, međutim s obzirom da sistem obezbeđuje skalabilnost i fleksibilnost, u daljoj nadogradnji sistema, predviđena je implementacija POP3 (*Post Office Protocol*) protokola za primanje elektronske pošte.

7. LITERATURA

1. Marković M. (2004), "Tehnike zaštite podataka i kriptografski protokoli u savremenim računarskim mrežama", skripta
2. Pistoia M., Reller D., Gupta D., Nagnur M., Ramani A. (1999), "Java 2 Network Security", Redbook, United States of America
3. Milićev D. (2001), "Objektno orijentisano modelovanje na jeziku UML", Mikro knjiga, Beograd