Đuro Alfirević,
potporučnik, dipl. inž.
Uprava za kadrove MO,
Beograd

ZAŠTIĆENA KOMUNIKACIJA PUTEM INFRASTRUKTURE SA JAVNIM KLJUČEVIMA

UDC: 004.773.3 : 621.391.7

Rezime:

Jedan tok informacija u okviru računarskih sistema ostvaruje se slanjem elektronske pošte. Međutim, da bi se ispunili zahtevi za kvalitativnost informacije koju ta pošta prenosi, neophodno je da računarska mreža ispunjava osnovna četiri bezbednosna servisa: zaštitu tajnosti, integritet podataka, autentikaciju i neporecivost. Ovaj rad predstavlja jedno od mogućih rešenja zaštićene komunikacije, primenom zaštićenog e-mail klijenta, sa prednostima koje donosi PKCS standard.

Ključne reči: PKI, kriptografija, S/MIME, kriptografski ključ, digitalni sertifikat.

SECURE COMMUNICATION VIA PUBLIC KEY INFRASTRUCTURE

Summary:

One of the information flows in a computer communication domain is accomplished by sending an e-mail, but in order to accomplish demands for information qualitativity that the e-mail contains, it's necessary for a computer network to provide the major four security services: confidentiality, data integrity, authentication and non-repudiation. This work represents one of the possible solutions of secured communication, applying a secured e-mail client with advantages that PKCS standard brings.

Key words: PKI, cryptography, S/MIME, cryptographic key, digital certificate.

Uvod

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

– 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.

Dakle, savremene računarske mreže ne pružaju odgovarajući nivo zaštite i upravo zbog toga predloženo rešenje zalazi u domen kriptografije. Ona predstavlja tehniku koja se bavi proučavanjem načina transformisanja poruka čiji je informacioni sadržaj poznat samo ovlašćenim korisnicima, kako bi se poruke načinile bezbednim i imunim na napade. 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 najčešće se, ali ne i obavezno, vrši primenom simetričnih kriptografskih algoritama, dok se ostali servisi realizuju primenom asimetričnih kriptografskih algoritama. Savremena rešenja sistema zaštite karakteriše višeslojna arhitektura koja inkorporira razne hardverske i softverske module.

Analiza zahteva

Jedna od najčešćih potreba za zaštićenom komunikacijom javlja se u domenu elektronskog poslovanja, gde se elektronskim putem prenose bezbednosno-kritične informacije, kakve su brojevi kreditnih kartica, zatim poverljivi podaci i sl. Dakle, posmatrano sa aspekta krajnjih korisnika, potrebno je obezbediti zaštićen e-mail klijent koji će obezbediti dovoljan nivo zaštite pri slanju elektronske pošte, ali je potrebno i da takav sistem bude nezavisan od platforme, kako bi rešenje bilo prenosivo.

Iz analize prethodno navedenih potreba da se komunikacije zaštite može se zaključiti da:

– sopstveno rešenje treba da integriše rad sa promenljivim tokenima, kakva je smart kartica;

– sama aplikacija treba da bude realizovana u programskom jeziku Java™, kako bi se obezbedila platformska nezavisnost samog sistema i

– sam sistem treba optimizovati radi boljih performansi.

Infrastruktura sa javnim ključevima

Infrastruktura sa javnim ključevima predstavlja skup hardverskih i softverskih elemenata, ljudi, politika i procedura neophodnih za generisanje, upravljanje, skladištenje, distribuciju i opoziv sertifikata. Postoji više mogućih načina da se realizuje infrastruktura sa javnim ključevima – PKI (Public Key Infrastructure), a 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 značajna autentičnost subjekata koji komuniciraju. Drugim rečima, uspostavljanje infrastrukture sa javnim ključevima osnovni je preduslov za realizaciju sistema zaštite. Servisi PKI koriste se na svim nivoima zaštite računarskih resursa i mreža. Primeri aplikacija zasnovanih na PKI 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 sa javnim ključevima sastoji se od sledećih komponenti:

– sertifikacionog autoriteta (Certification Authority, CA), koji izdaje digitalne sertifikate i reguliše način njihove upotrebe,

– registracionih autoriteta (Registration Authority, RA), koji predstavljaju interfejs za podnošenje zahteva za izdavanje sertifikata,

– komunikacionog sistema za razmenu podataka između registracionog i sertifikacionog autoriteta – distribuciju zahteva za izdavanje sertifikata i slanje digitalnih sertifikata,

– kriptografskih aplikacija za realizaciju funkcija PKI,

– subjekata koji komuniciraju u mrežnom okruženju, na bazi izdatih digitalnih sertifikata.

Sertifikacioni autoritet je telo sa najvećim stepenom poverenja u okviru PKI. Svojim digitalnim potpisom garantuje asocijaciju odgovarajućeg subjekta i njegovog javnog ključa, i upravo zbog toga je potpuna i pouzdana zaštita tajnog ključa sertifikacionog autoriteta, jedan od najvažnijih zadataka koji se postavlja pred PKI, jer ako se kompromituje privatni ključ asimetričnog šifarskog sistema sertifikacionog autoriteta, čitav sistem je kompromitovan.

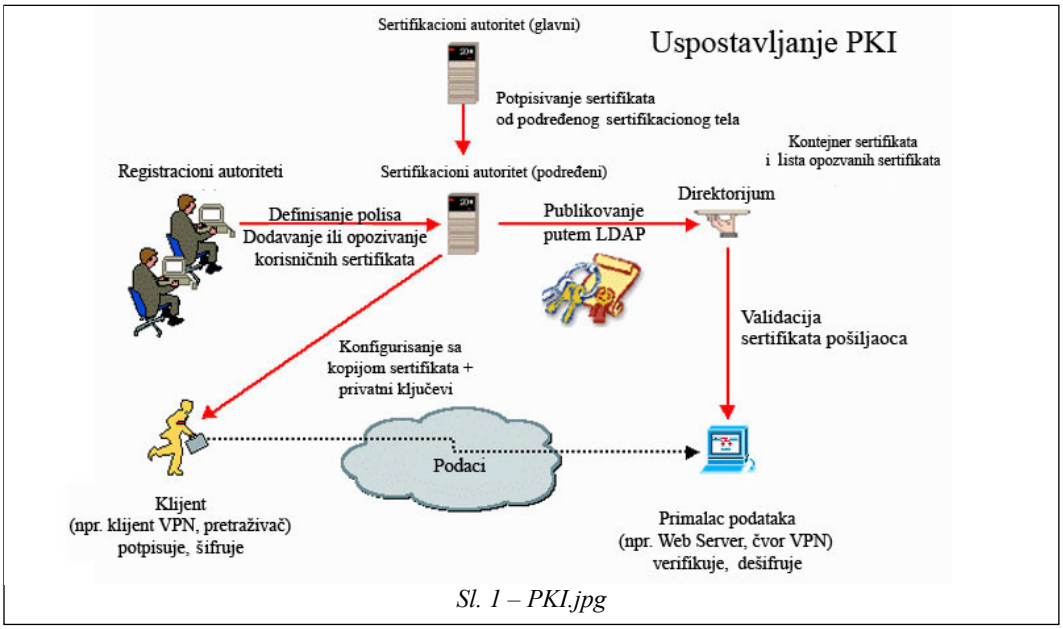
Neke od osnovnih funkcije CA su: izdavanje digitalnih sertifikata, upravljanje rokom važnosti, upravljanje procedurom povlačenja sertifikata, publikovanje sertifikata na X500/LDAP direktorijumu, i sl.

Na slici 1 prikazan je PKI.

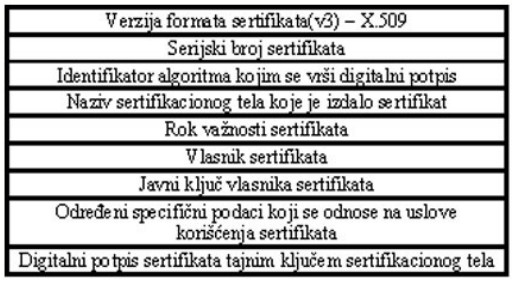
Ključni koncept zaštićene komunikacije u okviru PKI se, pre svega, oslanja na digitalne sertifikate.

Asimetrični kriptografski algoritmi zasnivaju se 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 fizičkog identiteta subjekta i javnog ključa ostvaruje se primenom digitalnih sertifikata, na bazi tehnologije digitalnog potpisa i tehnologija koje omogućuju pouzdano funkcionisanje infrastrukture sa javnim ključevima. Struktura digitalnog sertifikata prikazana je na slici 2.

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



Sl. 1 – PKI.jpg



Sl. 2 – Struktura digitalnog sertifikata.jpg

Elementi koji čine strukturu digitalnog sertifikata su:

– format sertifikata, koji predstavlja oznaku strukture digitalnog sertifikata. Jedan od najzastupljenijih formata digitalnih sertifikata definisan je X509 standardom;

– jedinstveni serijski broj. Sertifikat je jedinstveno određen nazivom sertifikacionog tela koje ga je izdalo i svojim serijskim brojem;

– rok važnosti, koji predstavlja period u kojem je izdati sertifikat validan;

– vlasnik sertifikata, koji je predstavljen složenom strukturom koja obuhvata nekoliko ličnih podataka: ime vlasnika, naziv organizacije u kojoj je zaposlen, naziv niže organizacione celine, naziv mesta u kojem stanuje, dvoslovni niz koji označava državu, region u okviru države;

– digitalni potpis sertifikacionog tela koje ga je izdalo, kojim se garantuje integritet sertifikata;

– identifikator algoritma koji se koristi za kreiranje digitalnog potpisa.

Uloga digitalnog sertifikata je, dakle, da dovede u jednoznačnu vezu fizički identitet subjekta (vlasnika sertifikata) sa javnim ključem. Kreiranje i digitalno potpisivanje sertifikata vrši „treća strana od poverenja“ (trusted third party, TTP). Ukoliko prijemna strana uspešno verifikuje dobijeni sertifikat, ona je sigurna u autentičnost pošiljaoca poruke, tj. sigurna je da javni ključ stvarno pripada subjektu sertifikata.

Rešenje slanja zaštićenog e-maila

Realizacija sopstvenog rešenja se, pre svega, oslanja na programski jezik Java™-u, firme Sun Microsystems, Inc., i na standard kriptografskih sistema sa javnim ključem.

Specifikacija Jave obuhvata dve relativno nezavisne celine: specifikaciju programskog jezika Java i specifikaciju Java Virtuelne Mašine (JVM) [3]. Specifikacija programskog jezika Java ne razlikuje se značajnije 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 prevode se 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 programa napisanih u programskom jeziku Java, 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 [4]. Osnovna ideja upotrebe JIT tehnika je da se pri prvom pozivu 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 direktno se preslikava u sekvencu instrukcija koje se neposredno izvršavaju [4].

Uvođenje originalnog koncepta prenosivosti programa na nivou izvršnog koda imalo je 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 mikroračunara različitih proizvođača (sa podrškom za Javu) softver razvija na identičan način, upotrebom istog programskog jezika [5], [6], [7]. Time je ostvarena ogromna razlika u odnosu na vreme kada je svaki proizvođač definisao skup asemblerskih instrukcija karakterističnih za svoje familije mikroračunara.

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. Provajderska arhitektura ima za cilj definisanje standardnog interfejsa prema programeru koji koristi kriptografske funkcije, nezavisno od konkretnog algoritma ili njegove implementacije.

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 kojem je ključ – naziv algoritma, vrednost kojoj se pristupa – puno ime klase koja realizuje dati algoritam.

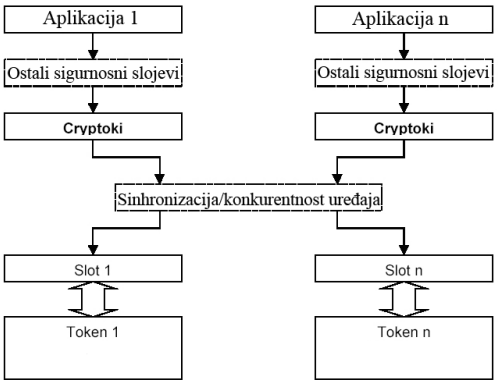
Security je klasa iz paketa java.security, koja sadrži listu provajdera i metode karakteristične za liste – za dodavanje i brisanje elemenata, itd., čije su sve metode statičke. Time je omogućeno da u jednoj instanci Java virtuelne mašine postoji samo jedan objekat klase Security. Da bi se koristile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

Jedna od vodećih firmi u svetu o oblasti kriptografije – RSA Data Security, Inc., čiji su osnivači kreatori RSA algoritma (Rivest, Shamir, Adleman), izdala je nekoliko standarda čiji je naziv Public Key Cryptography Standard (PKCS) sa rednim brojevima u sufiksu, koji se odnose na kriptografiju i koji su postali široko prihvaćeni. Jedan od tih standarda je i PKCS#11, koji propisuje način pristupa prenosivim kriptografskim uređajima kao što su smart kartice, hardverski bezbednosni moduli, PCIMCIA kartice i ostali hardverski uređaji koji imaju mogućnost čuvanja kriptografskih parametara i obavljanja kriptografskih operacija. Trenutno aktuelna verzija ovog standarda je PKCS#11 v2.20. Postoje i drugi standardi koji propisuju način pristupa ovakvim uređajima, kao što

je ISO 7816, ali ovaj standard, za razliku od ostalih, propisuje programski interfejs na višem nivou, koji je kompatibilan sa standardnim programskim jezikom C, za korišćenje ovakvih uređaja.

Prvi cilj standarda bio je da se svi tipovi kriptografskih uređaja apstrahuju pod kategorijom kriptografski token, a drugi cilj bio je deljenje resursa. Današnji operativni sistemi su, uglavnom, multi-tasking, što znači da su resursi računara u jednom trenutku deljeni između više aplikacija. Drugo, na jednom računaru može se naći više od jednog kriptografskog tokena u jednom trenutku. Generalni model na koji se standard oslanja prikazan je na slici 3.

Standardom su opisane strukture podataka i funkcije, pomoću kojih je moguće kreirati objekte i izvoditi kriptografske operacije sa podacima koji se mogu prosleđivati tokenu ili koji se već nalaze na tokenu, kao što je privatni asimetrični ključ. Na kriptografskom tokenu mogu se čuvati objekti koji pripadaju nekoj klasi objekata kao što je sertifikat, ključ, običan podatak i biometrijski podaci. Standard definiše funkcije pomoću kojih se može



Sl. 3 – Generalni model na koji se PKCS#11 oslanja.jpg

vršiti kriptovanje i dekriptovanje podataka, digitalno potpisivanje i verifikacija digitalnog potpisa. Takođe, standardom je propisan i pristup do objekata koji se nalaze na tokenu. Tako postoje javni (public) i privatni (private) objekti. Pristup do privatnih objekata koji se nalaze na tokenu dozvoljen je samo pod uslovom da se odgovarajući PIN (Personal Identification Number) predstavi tokenu. Ovaj standard omogućio je ponovnu iskoristivost klijentskog koda, tako da će jednom napisan klijentski kod koji se oslanja na PKCS#11, moći da radi sa bilo kojim kriptografskim uređajem koji ovaj standard podržava. Proizvođači kriptografskih uređaja dostavljaju biblioteku koja implementira ovaj standard, za ciljnu platformu (Windows, Linux,...), a programeri je koriste kao i svaku drugu biblioteku pisanu u programskom jeziku C.

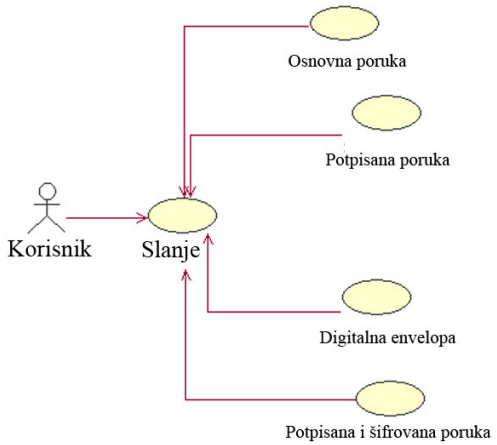
Implementacija

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

Radi konciznije predstave implementacije softverskog rešenja, kao i jake hijerarhijske dekompozicije samog problema, primenjeni su dijagrami unifikovanog jezika za modelovanje (Unified Modeling Language, UML).

Na slici 4 prikazan je dijagram slučajeva upotrebe (Use Case Diagram), dijagram koji prikazuje slučajeve upotrebe

i aktere, kao i njihove relacije. Ovim dijagramom predstavlja se statički pogled na funkcionalnost (ponašanje) sistema. Takođe, preko njih može se modelovati kontekst sistema: granice sistema i akteri koji sa njime interaguju, zatim funkcionalni zahtevi sistema (šta sistem treba da radi, nezavisno od toga kako iznutra funkcioniše) [9].

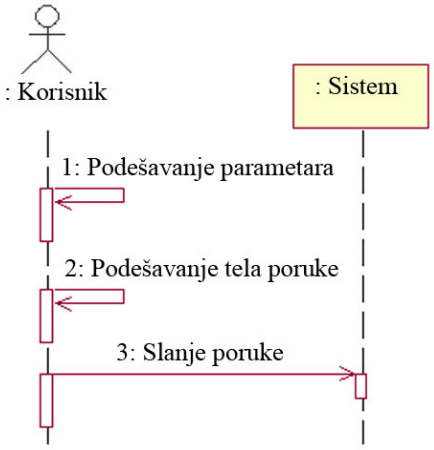


Sl. 4 – Dijagram slučajeva upotrebe sopstvenog rešenja.jpg

Dakle, kao što dijagram pokazuje, korisniku je omogućeno slanje osnovnih, potpisanih i šifrovanih poruka, kao i slanje digitalne envelope. Puna funkcionalnost sistema realizovana je upotrebom provajdera BouncyCastle, koji pruža servise neophodne za slanje S/MIME (Secure/Multipurpose Internet Mail Extensions) tipova poruka, gde S/MIME predstavlja bezbednosno proširenje standardnih MIME tipova podataka.

Opis realizacije pojedinačnih slučajeva upotrebe prikazan je pomoću dijagrama interakcije, i to preko dijagrama sekvence (Sequence Diagram), koji naglašava vremenski redosled poruka, gde su objekti poređani po x osi, dok se poruke ređaju u vidu horizontalnih linija po y osi, pri čemu vreme raste nadole [9].

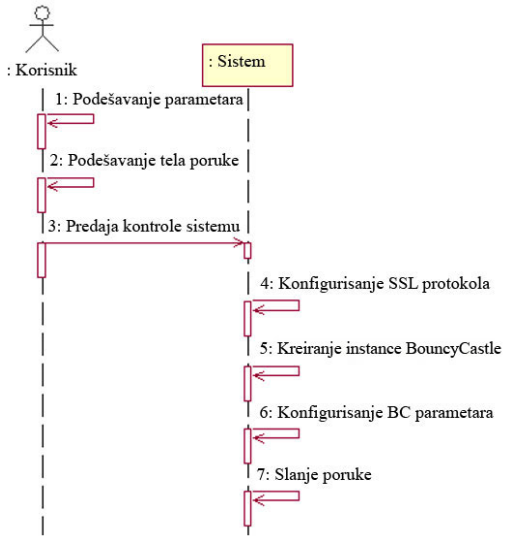
Ukoliko korisnik odabere slanje osnovnih poruka (slika 5) aplikacija se ne oslanja na BouncyCastle provajder, tj. na sam sadržaj poruke ne primenjuju se kriptografske tehnike zaštite podataka. Suština se svodi na konfigurisanje osnovnih parametara poruke (SMTP Server, From, To, Subject, User name, Password), definisanje sadržaja poruke i, konačno, slanje poruke.



Sl. 5 – Dijagram sekvence slanja osnovnih poruka.jpg

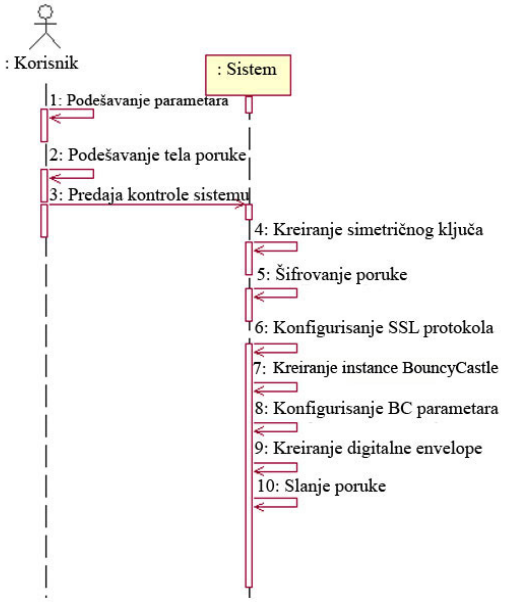
Odabirom slanja potpisanih poruka (slika 6) uključuju se kriptografski parametri i na sadržaj poruke primenjuju kriptografske tehnike. Korisnik konfiguriše osnovne parametre poruke (SMTP Server, From, To, Subject, User name, Password), definiše njen sadržaj, zatim se kontrola predaje provajderu BouncyCastle, koji primenom odgovarajuće kriptografske kompresione funkcije kreira kriptografski otisak poruke, zatim je

privatnim ključem potpisnika, upotrebom RSA algoritma, potpisuje i, konačno, šalje poruku, uz dodavanje i sertifikata i njenog potpisnika. Pri slanju kriptografski zaštićenih poruka (S/MIME poruka) sistem se oslanja na protokol SSL (Secure Sockets Layer), gde se umesto standardnih portova 80 i 8080 koristi port 465 radi zaštićene komunikacije.



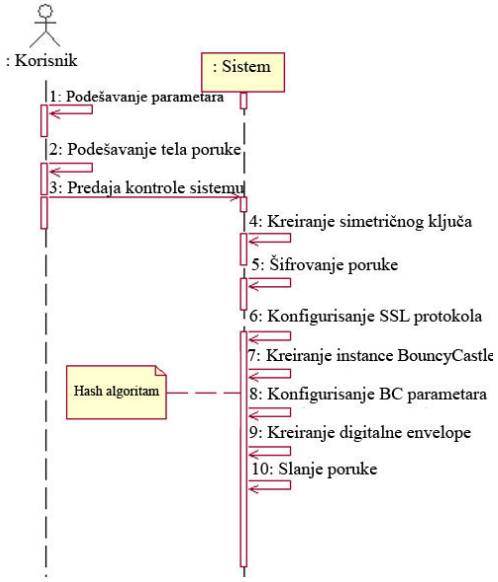
Sl. 6 – Dijagram sekvence slanja potpisanih poruka.jpg

U slučaju slanja digitalne envelope (slika 7) korisnik podešava osnovne parametre (SMTP Server, From, To, Subject, User name, Password) i definiše sadržaj poruke. Zatim, kreira se tajni ključ simetričnog kriptografskog algoritma i njime se šifruje sadržaj poruke. Zatim se, upotrebom javnog ključa RSA algoritma, šifruje simetrični ključ. Tako šifrovan sadržaj poruke i ključ kojim je poruka šifrovana predstavljaju digitalnu envelopu. Upotrebom digitalne envelope rešava se problem distribucije deljenog simetričnog ključa, kakav egzistira u simetričnim kriptografskim sistemima.



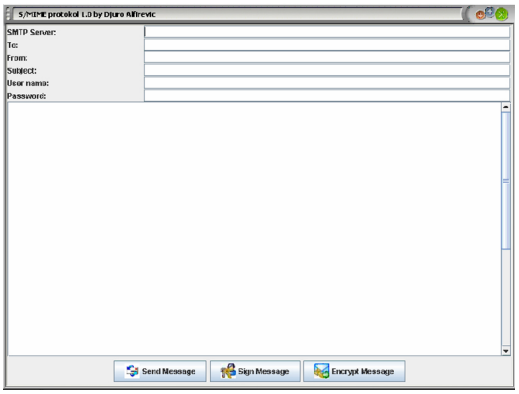
Sl. 7 – Dijagram sekvence slanja digitalne envelope.jpg

Slanje šifrovanih i potpisanih poruka praktično inkorporira tehnologije digitalnog potpisa i digitalne envelope. Dijagram sekvence prikazan je na slici 8.



Sl. 8 – Dijagram sekvence slanja potpisane i šifrovane poruke.jpg

Uz upotrebu javax.swing i java.awt paketa realizovan je grafički korisnički interfejs (Graphical User Interface, GUI) koji je prikazan na slici 9.



Sl. 9 – Grafički korisnički interfejs.jpg

Zaključak

Kao jedan od osnovnih preduslova zaštićene komunikacije subjekata u distribuiranom okruženju, predloženo rešenje oslanja se na višeslojnu arhitekturu zaštite kakva danas egzistira kao jedna od mogućih odbrana od potencijalnih napada na računarske sisteme. Od predloženih slojeva zaštite, realizovana je zaštita na aplikativnom nivou, koja se oslanja na sloj zaštite transportnog nivoa. Predočene su najosnovnije karakteristike i koncepti programiranja u programskom jeziku Java i njihove posledice. Pri realizaciji predloženog programskog rešenja primenjene su savremene metodologije projektovanja objektno orijentisanog softvera.

Pravci daljeg razvoja nastalog projekta mogu biti brojni, a uslovljeni su, prvenstveno, mogućnošću primene i konkretnim potrebama. Moguće smernice daljeg rada mogu biti:

– realizacija sopstvenog kriptografskog provajdera (možda i kriptografskog podsistema), sa sopstvenim implementacijama simetričnih i asimetričnih kriptografskih algoritama,

– detaljnije upoznavanje sa standardima asimetrične kriptografije – PKCS (Public Key Cryptography Standard) 1–15,

– kreiranje sertifikacionog autoriteta za izdavanje sertifikata, liste opozvanih sertifikata, kreiranje registracionih autoriteta sa odgovarajućim interfejsom za komunikaciju sa centralnim sertifikacionim autoritetom,

– realizacija predloženog protokola zaštite na aplikativnom nivou u jeziku C++, radi povećanja efikasnosti u odnosu na postojeću realizaciju,

– inkorporiranje servera POP3 (Post Office Protocol) za primanje poruka elektronske pošte,

– druge brojne primene, u skladu sa konkretnim potrebama.

Literatura:

[1] Carlisle Adams, Steve Lloyd, Understanding PKI: concepts, standards, and deployment considerations, Addison Wesley, 2002.

[2] David Hook, Beginning cryptography with java, Wrox Press, 2005.

[3] Branko Milosavljević, Praktikum za kurs java i internet programiranje, Vojna akademija, Beograd, 2001.

[4] Marco Pistoia, Duane F. Reller, Deepak Gupta, Milind Nagnur, Ashok K. Ramani, Java 2 network security, international technical support organization, http://www.redbooks.ibm.com, 1999.

[5] Java Card 2.1.1 Specifications, http://java.sun.com

[6] Java Card. 2.1.1 Runtime Environment (JCRE) Specification, http://java.sun.com

[7] Java Card. 2.1.1 Virtual Machine Specification, http://java.sun.com

[8] Jonathan Knudsen, Java cryptography, O'Reilly, 1998.

[9] Dragan Milićev, Objektno orijentisano programiranje na jeziku UML, Mikro knjiga, 2001.