Razvoj servisa za digitalni potpis sa sopstvenim modulom za generisanje ključeva i digitalnih sertifikata

The development of services for the digital signature with its own module to generate keys and digital certificates

Milenko Đurić, Saša Adamović, Univerzitet Sinergija, Bijeljina

***Sažetak* – U ovom radu fokus je stavljen na razvoj sopstvene aplikacije za generisanje digitalnih sertifikata potrebnih za digitalno potpisivanje, na razvoj same funkcije digitalnog potpisivanja, kao i na verifikovanje digitalnog potpisa uz pomoć digitalnih sertifikata. U aplikaciji će biti implementirani moduli za generisanje skladišta ključeva, digitalnih sertifikata koji se sastoje od osnovnih informacija o vlasniku sertifikata i para asimetričnih kriptoloških ključeva (javni i privatni). Ključevi su generisani pomoću DSA[1] i RSA[2] algoritama, a koriste se i za digitalno potpisivanje i verifikaciju digitalnog potpisa.**

***Ključne riječi* – digitalno potpisivanje; verifikovanje digitalnog potpisa; generisanje digitalnih sertifikata; generisanje asimetričnih kriptoloških ključeva; skladište ključeva**

***Abstract* – In this paper, the focus is on the development of our own application for the creation of digital certificates required for digital signing, on the development of the digital signature function, as well as on the verification of a digital signature with the help of digital certificates. Modules for the creation of key store, the creation of digital certificates that consist of basic information about the certificate owner and the creation of a pair of asymmetric cryptographic keys (public and private) will be implemented within this application. The keys are generated using the DSA and RSA algorithms, and are also used for digital signing and the verification of a digital signature.**

***Keywords* – digital signature; verifying a digital signature; creation of digital certificates; creation of asymmetric cryptographic keys; key store**

I. UVOD

Integritet poruke u savremenoj komunikaciji predstavlja imperativ svih učesnika u komunikaciji, bilo da se radi o privatnim ili poslovnim korisnicima. Bez obzira o kakvoj komunikaciji se radi, moramo biti sigurni da poruke koje šaljemo i poruke koje primamo nisu kompromitovane, odnosno da njihov integritet nije narušen, te da se komunikacija odvija između dva ili više identifikovanih, verifikovanih, korisinika. Itegritet poruke obezbjeđuje digitalni potpis.

Digitalni potpis je kompjuterska verzija vašeg svojeručnog potpisa. Takav potpis verifikuje da su podaci koji su poslati od strane te osobe ili kompanije važeći, tj. da je navedena osoba potpisala dokument. Ovi potpisi su sigurni i legalni, te značajno povećavaju bezbjednost svih učesnika u komunikaciji. Digitalni potpis ima ogroman značaj u ulozi zaštite integriteta i autentičnosti u svim vrstama elektronske komunikacije. U komunikaciji između dva ili više učesnika, najvažnije je da sadržaj poruke nije kompromitovan.

Da bismo bili u mogućnosti da digitalno potpisujemo dokumente potrebni su nam digitalni sertifikati. Digitalne sertifikate izdaju sertifikaciona tijela. Sertifikaciono tijelo (eng. *Certification authority*) izdaje digitalne sertifikate organizacijama ili pojedincima poslije potvrde njihovog identiteta. Kada su podaci potvrđeni, sertifikaciono tijelo potpisuje javni ključ svojim privatnim ključem.

Istraživanjem stanja u ovoj oblasti došlo se do zaključka da je potrebno razviti sopstveno rješenje za generisanje digitalnih sertifikata kao i modula za digitalno potpisivanje svih vrsta fajlova i verifikovanje digitalnog potpisa jer postojeća rješenja nisu od povjerenja.

Razvijena aplikacija će imati modul za generisanje skladišta u kojem će biti čuvani svi digitalni sertifikati. Iz skladišta će biti moguće, pomoću aplikacije, izvesti, uvesti ili izbrisati digitalni sertifikat, koji će služiti za digitalno

[1] U avgustu 1991. godine Američki nacionalni institut za standarde i tehnologiju (eng. *National Institute of Standards and Technology* - NIST) je predložio algoritam za digitalno potpisivanje (eng. *Digital* Signature Algorithm - DSA). Od tada je DSA postao standardni algoritam za digitalno potpisivanje (eng. *Digital Signature Standard* - DSS) [2].

[2] RSA algoritam je dobio ime od početnih slova imena svojih kreatora, Rivest, Shamir i Adleman.

DOI: 10.7251/ZRSNG1501109DJ

potpisivanje svih vrsta fajlova asimetričnim šifarskim algoritmima. Korisnik će imati mogućnosti odabira digitalnog sertifikata kojim želi da digitalno potpiše, odnosno da verifikuje digitalni potpis.

Ključnu ulogu u aplikaciji ima Java modul *KeyTool* koji će biti implementiran u našu aplikaciju. *KeyTool* služi za generisanje skladišta za digitalne sertifikate, kao i za samu manipulaciju digitalnim sertifikatima. Ovaj modul koristi DSA i RSA, jedne od najpopularnijih asimetričnih kriptoloških algoritama za generisanje para ključeva (javni i privatni).

Posebnu pažnju ćemo posveti što boljoj implementaciji programskih modula radi pravilne upotrebe i onemogućiti bezbjednosne propuste.

II. METODI

Da bismo bili u mogućnosti da digitalno potpišemo, odnosno verifikujemo digitalni potpis potrebni su nam digitalni sertifikati. Za generisanje digitalnih sertifikata koristimo Java modul *KeyTool* koji je implementiran u našu aplikaciju.

Komande korištene za genirisanje digitalnog sertifikata	
Komanda	Opis
-genkey	Pozivanje funkcije za generisanje digitalnog sertifikata
-alias	Funkcija za dodjeljivanje imena generisanom digitalnom sertifikatu
-v	Funkcija za prikaz povratnih informacija nakon izvršavanja komandi
-keystore	Funkcija kojoj se prosljeđuje lokacija skladišta u kojem će biti sačuvan generisani digitalni sertifikat

Tabela 1 – *KeyTool* komande za generisanje digitalnog sertifikata

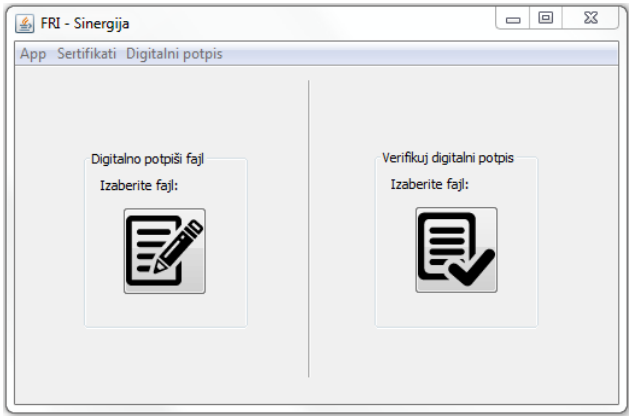
Takođe su nam potrebne i jednosmijerne heš funkcije. U aplikaciji ćemo koristiti dvije jednosmijerne heš funckije a to su SHA-1 i SHA-256. Jednosmijerne heš funkcije relativno lako izračunavaju heš vrijednosti podataka, ali je izuzetno teško od heš vrijednosti izračunati početni podatak. To znači da je za dati x veoma je lako izračunati $f(x)$ ali za dati $f(x)$ je teško izračunati x. Kada u ovom kontekstu kažemo da je nešto teško izračunati, mislimo da bi bili potrebni milioni godina da se izračuna x za dati $f(x)$ čak i kada bi se svim kompjuterima na svijetu dalo da rješavaju taj zadatak [1].

Servis integriteta poruke postižemo tako što ćemo našu poruku digitalno potpisati, odnosno našoj poruci izračunati heš vrijednost i zatim šifrovati tu vrijednost sa privatnim ključem koristeći jedan od algoritama, DSA ili RSA. Šifrovanu heš vrijednost zajedno sa originalnim fajlom šaljemo ostalim učesnicima u komunikaciji.

Integritet i autentičnost poruke se provjeravaju tako što drugi učesnici u komunikaciji primljenu poruku provjeravaju izračunavajući njenu heš vrijednost, zatim dešifruju potpisanu heš vrijednost koju su primili pomoću javnog ključa od pošiljaoca i jednog od algoritama, DSA ili RSA. Da bismo utvrdili integritet i autentičnost poruke, dvije heš vrijednosti moraju biti jednake. Itegritet i autentičnost se kompletno zasnivaju na tajnosti privatnog ključa pošiljaoca.

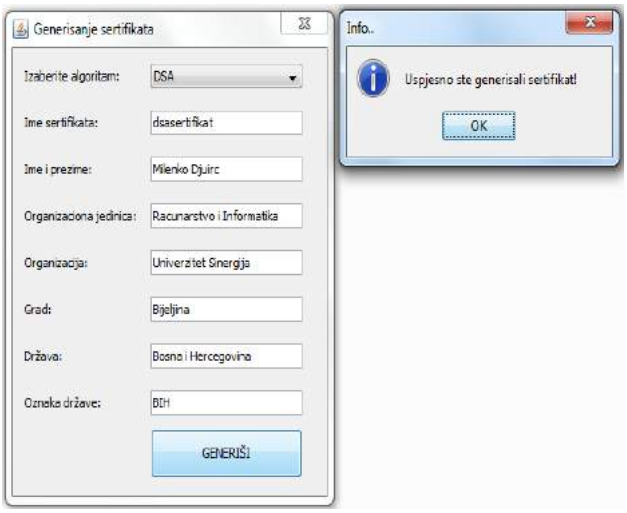
III. PREDLOŽENO PROGRAMSKO REŠENJE

Zbog nepovjerenja u postojeća rješenja koja su nam dostpuna, komercijalna ili besplatna, odlučili smo se za razvijanje sopstvenog softverskog rješenja.



Slika 1 – Glavni ekran aplikacije

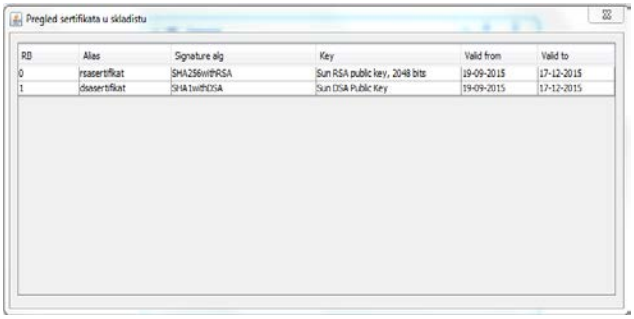
Na glavnom ekranu aplikacije (Slika 1.) korisniku je ponuđen meni i dvije opcije da digitalno potpiše ili da verifikuje digitalni potpis. Korisnički interfesjs ne treba da bude prenatrpan raznim funkcionalnostima iz razloga što ovakvi interfejsi olakšavaju upotrebu aplikacije i smanjuju mogućnosti za nastajanje grešaka. Na ovom prozoru su ponuđene dve osnovne funkcije, potpiši i verifikuj.



Slika 2 – Ekran za generisanje digitalnih sertifikata

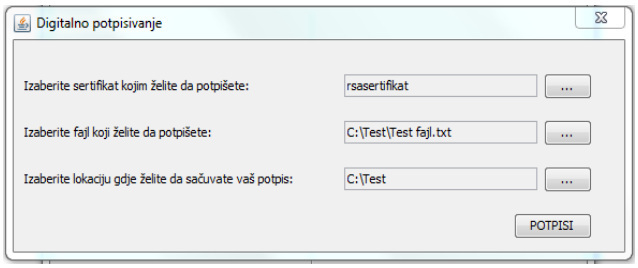
DOI: 10.7251/ZRSNG1501109DJ

Odabirom „Generiši“ opcije iz menija otvara nam se novi ekran za generisanje digitalnih sertifikata (Slika 2.) gdje se od korisnika očekuje da odabere algoritam koji će biti zadužen za generisanje para ključeva, da unese ime sertifikata koje mora biti duže od osam karaktera, ime i prezime vlasnika sertifikata, organizacionu jedinicu, organizaciju, grad, državu i skraćenicu te države. Ako su svi parametri pravilno unešeni, aplikacija generiše digitalni sertifikat i smiješta ga u skladište.



Slika 3 – Pregled skladiška

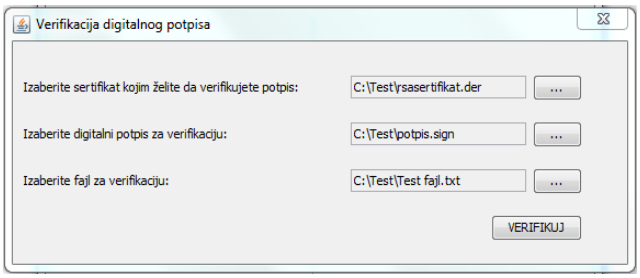
Pregledom skladišta vidimo koji se sve digitalni sertifikati nalaze u njemu, kao i osnovne informacije vezane za te sertifikate (Slika 3).



Slika 4 – Ekran za digitalno potpisivanje

Kada želimo da digitalno potpišemo fajl, kliknemo na „Izaberite fajl“ (Slika 2) i otvara nam se novi ekran za digitalno potpisivanje fajla (Slika 4). Od korisnika se traži da izabere digitalni sertifikat iz skladišta kojim želi digitalno da potpiše fajl. Takođe, od korisnika se traži da izabere fajl koji želi da digitalno potpiše i lokaciju na kojoj će biti sačuvan digitalni potpis.

Kada je korisnik unio sve potrebne podatke, pritiskom na dugme „POTPISI“ (Slika 4) aplikacija digitalno potpisuje fajl. Kada je aplikacija završila digitalno potpisivanje fajla, o tome obavještava korisnika.



Slika 5 – Ekran za verifikaciju digitalnog potpisa

Kada korisnik želi da verifikuje digitalni potpis, on klikne na drugo dugme na ekrenu, „Izaberi fajl“, i otvara se novi ekran (Slika 5) gdje se od korisnika očekuje da popuni podatke na tom ekranu. Od korisnika se očekuje da aplikaciji proslijedi digitalni sertifikat kojim želi da verifikuje digitalni potpis, digitalni potpis i fajl za koji se provjerava digitalni potpis.

Klikom na dugme „VERIFIKUJ“ (Slika 5), aplikacija vrši verifikaciju digitalnog potpisa. Ukoliko je digitalni potpis verifikovan, aplikacija ispisuje poruku korisniku o uspješnoj verifikaciji, a ukoliko verifikovanje digitalnog potpisa nije uspješno, aplikacija obavještava korisnika da digitalni potpis nije verifikovan.

IV. ZAKLJUČAK

U ovom radu razvijena je sopstvena aplikacija za digitalno potpisivanje i generisanje digitalnih sertifikata. Aplikaciju je moguće koristiti u privatne ili poslovne svrhe. Glavni doprinos predloženog rješenja je sopstveni razvoj kripto-mehanizma u koji ćemo imati povjerenje. Na mjestima gde je bezbjednost neizoztavna, bitno je posjedovati sopstvena kripto rješenja i tako sistem učiniti bezbjednijim. Aplikacija je razvijena i implementirana prema visokim standardima za razvoj kriptografskih mehanizama sa preporučenim dužinama ključeva od strane NIST-a. Aplikacija je dobro optimizovana, ne zauzima mnogo resursa, te se ne zahtijeva mnogo resursa za njeno pokretanje, odnosno izvršavanje. Važno je napomenuti da se prilikom razvoja vodilo se računa o platformskoj nezavisnosti, pokretanje je moguće na svim operativnim sistemima sa Java virtuelnom mašinom. Sa aspekta ergonomije aplikativnog interfejsa, doprinijeli smo jednostavnijoj upotrebi ove aplikacije i tako smanjili potencijalne greške koje prosečan korisnik može da izazove.

Korištenjem ove aplikacije, privatni i poslovni korisnici obezbjeđuju servis integriteta, autentičnosti i neporecivosti, a navedni servisi su ključni elementi savremenog poslovanja preko Interneta.

ZAHVALNICE

Zahvaljujem se Univerzitetu Sinergija za obezbjeđivanje svih potrebnih uslova za kvalitetno akademsko obrazovanje, kao i svim profesorima koji su doprineli mom akademskom obrazovanju.

Posebna zahvalnost ide dr Saši Adamoviću koji je najviše i na pravi način znao da doprinese mom obrazovanju i koji je sve studente motivisao da se bave programiranjem.

LITERATURA

[1] A. Saša, Zaštita informacionih sistema, Beograd, 2015.

[2] V. Mladen i A. Saša, Kriptologija 1, Osnove za analizu i sintezu, Univerzitet Singidunum, 2013.

[3] S. William, Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall, 2005.

DOI: 10.7251/ZRSNG1501109DJ

[4] C. Suranjan, B. Katrik, H. Wasim i NIIT, Public Key Infrastructure Implementation and Design, John Wiley & Sons, 2002.

[5] O. Rolf, Contemporary Cryptography, Artech House, 2005.

[6] Oracle, „Tools,“ 31 Jul 2015. [Na mreži]. Available: https://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html. [Poslednji pristup 31 Jul 2015].

[7] Oracle, „Security,“ 7 Jully 2015. [Na mreži]. Available: http://docs.oracle.com/javase/7/docs/api/java/security/KeyStore.html. [Poslednji pristup 7 Jully 2015].

[8] B. K. Jonathan, Java Cryptography, O'Reilly, 1998.

[9] S. Douglas, Cryptography: Theory and Practice, CRC Press, CRC Press LLC, 1995.

[10] S. Bruce, Applied Cryptography, Second Edition; Protocols, Algorthms, and Source, John Wiley & Sons, Inc., 1996.

[11] J. M. Alfre, C. v. O. Paul i A. V. Scott, A Handbook of Applied Cryptography, CRC Press, 1996.

[12] W. D. Alexander i J. M. Chris, A Companion to User’s Guide to Cryptography and Standards, Artech House, 2005.

DOI: 10.7251/ZRSNG1501109DJ