Digitalni potpis i digitalni sertifikat

Dejan Đorđević, major Vojske Srbije

Sadržaj — **U modernoj „eri informatike“, kada se podaci obrađuju, prenose i čuvaju u elektronskoj formi, informacije postaju izložene čitanju, kopiranju i neautorizovanoj promeni. Savremene računarske mreže se, skoro u potpunosti, zasnivaju na Internet tehnologijama. Slabosti koje su uočene u arhitekturi mreža Internet tipa sa aspekta bezbednosti su da protokoli na kojima se Internet zasniva (TCP/IP) nisu projektovani da zadovolje zahteve za zaštitom informacija koje se preko njih prenose.**
Rešenje ovog problema donekle pruža kriptologija, nauka koja razmatra različite aspekte obezbeđivanja tajnosti informacija.

Ključne reči — **digitalni potpis, digitalni sertifikat, infrastruktura sa javnim ključevima.**

I. UVOD

Kriptologija je termin koji potiče od grčkih riječi kriptos (skriven, tajan) i logos (nauka), i označava naučnu disciplinu koja se bavi sigurnim (tajnim) komunikacijama.
Dve osnovne, tesno povezane grane kriptologije su: kriptografija i kriptoanaliza.

Predmet kriptografije je, pre svega, sinteza postupaka za obezbeđivanje tajnosti informacija, tzv. kripto-zaštitu informacija.
Predmet kriptoanalize je razmatranje metoda kojim se kompromituju ("razbijaju" od strane neovlašćenih korisnika) postupci kripto-zaštite informacije.

Primenom kriptografije realizuju se četiri osnovna bezbednosna zahteva (servisa):
• tajnost – obezbeđuje da informacioni sadržaj poruke bude dostupan samo ovlašćenim korisnicima
• integritet – obezbeđuje otkrivanje neovlašćene izmene informacionog sadržaja poruke
• autentičnost – omogućava proveru identiteta učesnika u komunikaciji
• neporecivost – sprečava mogućnost poricanja realizacije određenih aktivnosti učesnika u komunikaciji (kao što su slanje poruke, transakcija i dr.).

Simetrična kriptografija ili tzv. kriptografija tajnih ključeva je najstariji oblik kriptografije, stara gotovo koliko i ljudska komunikacija. Ona se razvijala i koristila kao alat u zaštiti informacija, naročito u vojnim, diplomatskim i državnim komunikacijama. Za proces kriptovanja u simetričnoj kriptografiji potrebno je znati algoritam kriptovanja i tajni ključ, a sigurnost zavisi od sigurnosti algoritma i dužine ključa. Najpoznatiji simetrični algoritmi su DES (eng. Data Encryption Standard), koji koji koristi ključeve dužine 56 bita i AES (eng. Advanced Encryption Standard), koji koristi ključeve dužine 128, 192 i 256 bita.

1. Dejan Đorđević, major veze Vojske Srbije, VP 5542 Beograd, Raška 2, 11000 Beograd, Srbija (+381-11-2064028; +381-64-1155076; e-mail: dejan.djordjevic@vj.yu).

Osnovni nedostatak simetričnih algoritama, odn. sistema zasnovanih na simetričnoj kriptografiji jeste upravljanje ključevima tj. njihova distribucija. Pre početka sigurne komunikacije subjekti komunikacije moraju razmeniti ključeve. Budući da se sigurnost svih zaštićenih (kriptovanih) informacija zasniva na sigurnosti ključa, razmena ključeva postaje vrlo ozbiljan problem, koji se usložava ako se komunikacija odvija na većoj udaljenosti i u njoj učestvuje više subjekata. Za n subjekata u komunikaciji potrebno je n(n - 1)/2 ključeva. Generisanje i upravljanje ovako velikim brojem ključeva najčešće je nepraktično, a njihova razmena je nesigurna.

Javni interes za kriptografiju drastično je porastao 1976. god. kada se prvi put javila ideja o infrastrukturi sa javnim ključevima (eng. Public Key Infrastructure, PKI). Naime Whitfield Diffie i Martin Hellman u svojoj publikaciji "New Directions in Cryptography" predstavili su ideju kriptografije bazirane na javnom i privatnom ključu. Tako je utemeljena asimetrična kriptografija ili tzv. kriptografija javnih ključeva čime se dobila mogućnost postizanja tajnosti informacija bez prethodne razmene tajnog ključa putem (ne)sigurnog komunikacionog kanala.
Osnova sigurnosti asimetričnih algoritama temelji se na nemogućnosti (ili vrlo teškoj mogućnosti) izračunavanja privatnog ključa iz javnog ključa.

1978. god. definisan je prvi praktični, asimetrični algoritam, koji se oznacava sa RSA (početna slova imena njegovih autora Rivesta, Shamira i Adlemana) i koji je iskorišćen za kreiranje digitalnog potpisa (eng. Digital Signature, DS).

1991. god. usvojen je prvi standard digitalnog potpisa, baziran na RSA asimetričnom algoritmu . 1994. god. američka Nacionalna Bezbednosna Agencija (eng. National Security Agency, NSA) razvila je i usvojila standard digitalnog potpisa (eng. Digital Signature Standard, DSS), kako bi omogućila generisanje digitalnog potpisa u svrhu autentifikacije elektronskih dokumenata.
Sve ovo, uz ubrzan razvoj savremene komunikacije preko različitih medija (najviše Interneta), dovelo je do realizacije infrastrukture sa javnim ključevima (PKI) koja omogućuje sigurnu komunikaciju preko nesigurnog kanala.

II. DIGITALNI POTPIS

„Digitalni potpis (eng. *Digital Signature*) predstavlja postupak kojim se određeni segment bloka podataka, ili standardizovane poruke, kriptografski obeležava potpisnikovim tajnim parametrom.“

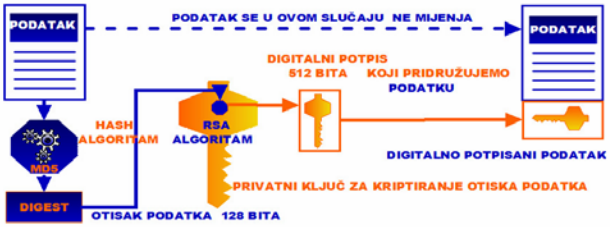
Digitalni potpis je 51-bitni broj koji se dobija primenom RSA algoritma na HASH vrednost generisanu iz bloka podataka koji se štiti. On se dodaje na kraj bloka podataka koji se šalje. Pod blokom podataka misli se na čitav DER (Datoteka za elektronsku razmenu podataka) osim njegovog poslednjeg dela.

Digitalni potpis i digitalno potpisani dokumenat se mogu izraziti formulom:

Digitalni potpis = E [H(m), SA]
Digitalno potpisani dokument = m; E [H(m), SA] gde su:
m - digitalni dokument koji se potpisuje,
H(m) - otisak digitalnog dokumenta, a *H* funkcija sažetka,
SA – tajni (privatni) ključ potpisnika,
E - funkcija šifrovanja (asimetrično kriptovanje).

A.. Kreiranje digitalnog potpisa

Postupak kreiranja digitalnog potpisa se sastoji iz dve faze:
- u prvoj fazi se primenom odgovarajuće kriptografske kompresione funkcije (MD5 HASH) određuje otisak poruke *(message digest)*,
- u drugoj fazi potpisnik poruke šifruje dobijeni otisak svojim tajnim (privatnim) ključem, primenom odgovarajućeg asimetričnog algoritma (RSA). Šifrovani otisak poruke predstavlja njen digitalni potpis i pridružuje joj se.



Slika 1. Kreiranje digitalnog potpisa (primer za MD5 HASH alogoritam i RSA algoritam)

Da bi potpisao dokument, potpisnik mora jasno naznačiti granice dokumenta koji potpisuje. Za označenu poruku (podatak) koji treba sigurno preneti, HASH funkcija softvera potpisnika izračunava jedinstveni otisak *(message digest)*, pridružen jedino toj poruci.

Softver zatim transformiše otisak u digitalni potpis koristeći se potpisnikovim tajnim (privatnim) ključem. Tako nastali digitalni potpis je stoga jedinstven i za poruku i za privatni ključ koji ga je kreirao.

Uobičajeno je da se digitalni potpis pridodaje poruci, skladišti i šalje zajedno s njom. Medutim, on se može poslati i kao odvojeni podatak, dokle god zadržava pouzdanu vezu s originalnom porukom. Kako je svaki potpis jedinstveno vezan uz original, besmisleno ga je u potpunosti odvojiti od izvora na osnovu kojeg je nastao.

B. Verifikacija digitalnog potpisa

Postupak verifikacije digitalnog postupka sastoji se iz 3 faze:
- u prvoj fazi se iz dobijene poruke izdvaja digitalni potpis i dešifruje javnim ključem pošiljaoca
- u drugoj fazi primalac kreira otisak informacionog dela dobijene poruke identičnim postupkom kao na predajnoj strani
- u trećoj fazi vrši se poređenje, i ako je dobijeni otisak poruke identičan sa dešifrovanim otiskom, verifikacija je uspešna.

Slika 2. Verifikacija digitalnog potpisa

C. Funkcionalnost digitalnog potpisa

Na osnovu iznetog može se zaključiti da je za funkcionalnost digitalnog potpisa potrebno izvršiti dva procesa, od kojih jedan sprovodi potpisnik, a drugi primalac.

Uspešnom proverom digitalnog potpisa garantuje se:
- *Autentičnost*, pouzdanost identiteta pošiljaoca je posledica činjenice da je otisak poruke koji je šifrovan tajnim ključem, moguće uspešno dešifrovati samo primenom odgovarajućeg javnog ključa.
- *Integritet*, upoređivanjem izračunatog i dešifrovanog otiska poruke utvrđuje se da poruka nije modifikovana.
- *Neporecivost*, pošiljalac ne može da porekne slanje poruke pošto je potpisana njegovim tajnim ključem.

Važno je pomenuti da elektronski potpisi uopšte, pa tako ni digitalni potpis ne pružaju zaštitu *Tajnosti* podataka od neovlašćenog čitanja, jer se svi podaci šalju u svom originalnom (nepromenjenom) obliku.

Postupci kreiranja i verifikacije digitalnog potpisa prolaze kroz postupke modifikacije vec čitavu deceniju, i mogu se automatizovati do te mere da je ljudska interakcija potrebna samo u izuzetnim slučajevima.

Verovatnoća otkaza ili problem sigurnosti u sistemima kriptografije koji su dizajnirani i implementirani prema razvijenim industrijskim standardima je beznačajan, i puno je manji od rizika neprimećenog falsifikata ili izmene dokumenta na papiru.

III. DIGITALNI SERTIFIKAT

A. Pojam digitalnog sertifikata

Kreiranje digitalnog potpisa i njegova verifikacija vrše se, kako je već pomenuto, asimetričnim kriptografskim sistemom, prilikom čega se koriste:
- tajni (privatni) ključ poznat jedino potpisniku
- javni ključ poznat širem krugu, a ne samo primaocu.

Međutim, kako možetmo biti sigurni da je to zaista javni ključ potpisnika? Rešenje ovog problema postiže se upotrebom *digitalnog sertifikata*. Digitalni certifikat je digitalno potpisani dokument koji povezuje javni kljuc s osobom kojoj pripada. Možemo ga nazvati i *digitalnom ličnom kartom*, jer on to zaista i jeste - digitalna lična karta u ”syber prostoru”, odn. sredstvo kojim dokazujemo identitet na Internetu.

”Digitalni sertifikat *(eng. Digital Certificate)* predstavlja element kojim se utvrđuje veza između identiteta subjekta i njegovog javnog ključa primenjenog asimetričnog algoritma”.

B. Struktura digitalnog sertifikata

Elementi koji čine strukturu digitalnog certifikata su:
- **verzija formata sertifikata** - sadrži oznaku strukture digitalnog sertifikata. Jedan od najzastupljenijih formata digitalnih sertifikata definisan je X.509 standardom.
- **serijski broj sertifikata -** sadrži vrednost koju dodeljuje sertifikacioni autoritet u trenutku kreiranja digitalnog sertifikata
- **identifikator algoritma -** sadrži podatke o algoritmu koji je pirmenjen za digitalno potpisivanje

- **naziv sertifikacionog tela -** identifikuje izdavača digitalnog sertfikata
- **rok važnosti sertifikata -** sadrži vremenski period u kome je izdati digitalni sertifikat validan.
- **vlasnik sertifikata** - predstavljen je složenom strukturom koja obuhvata nekoliko ličnih podataka:
  - dvoslovni niz koji označava državu
  - region u okviru države
  - elektronska adresa (e-mail)
  - naziv mesta u kome stanuje
  - naziv organizacije u kojoj je zaposlen
  - ime vlasnika,
  - naziv odeljenja (niže organizacione celine) u organizaciji
  - ime vlasnika sertifikata
- **polje dodatnih atributa** - sadrži vrednosti koje identifikuju vlasnika sertifikata a nisu sadržane u polju vlasnik sertifikata (broj telefona, broj faxa itd.)
- **informacija o javnom ključu vlasnika** - sadrži javni ključ i identifikator asimetričnog algoritma sa kojim se dati ključ primenjuje
- **digitalni potpis sertifikata** - od strane ustanove koja je izdala setifikat (CA).

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

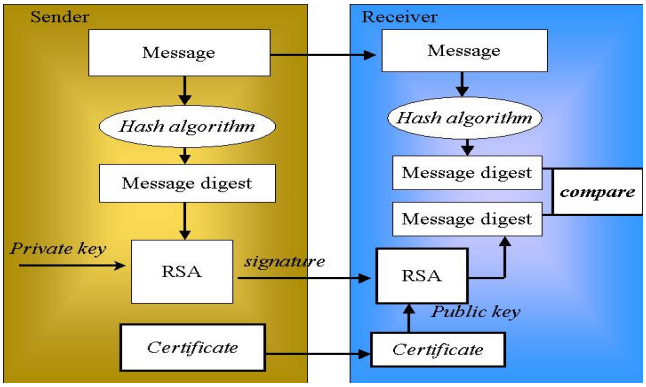
Slika 3. Struktura digitalnog sertifikata

Prema dosadašnjim iskustvima ovakva struktura sertifikata ispunjava zahteve savremenih kriptografkih sistema zaštite. Većina savremenih sistema zaštite, koji uključuju infrastrukturu sa javnim ključevima (PKI), bazira se na primeni X.509 digitalnih sertifikata.

C. Funkcionalnost digitalnog sertifikata

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" (eng. *Trusted Tthird Party,* TTP). Ukoliko prijemna strana uspešno verifikuje dobijeni sertifikat, onda je ona sigurna u autentičnost pošiljaoca poruke – vlasnika odgovarajućeg tajnog ključa.

Kako je par ključeva matematicki povezan, ako je asimetrični sistem dobro oblikovan i implementiran, nemoguće je iz javnog ključa izdvojiti tajni (privatni) ključ. Stoga, bez obzira na to što je javni ključ poznat mnogima, u svrhu potvrde identiteta potpisnika, nemoguće je otkriti njegov tajni ključ i iskoristiti ga za lažiranje digitalnog potpisa. Ova činjenica se naziva načelo ireverzibilnosti.



Slika 4. Postupak kreiranja i provere digitalnog potpisa

Digitalni sertifikati mogu biti:

- samopotpisani
- kvalifikovani.

Samopotpisane digitalne sertifikate može da izda „bilo ko", pa čak i sam korisnik. Uglavnom se koriste interno, a „pravna snaga" dobija se potpisivanjem posebnog ugovora sa korisnikom (npr. e-banking sistemi).

Kvalifikovane digitalne sertifikate može da izda samo sertifikaciono telo koje ispunjava određene zakonske uslove i ima dozvolu za rad, što je definisano Zakonom o digitalnom potpisu i pripadajućim podzakonskim aktima. Kvalifikovani digitalni sertifikat sa odgovarajućim parom ključeva može se upotrebiti za kreiranje „kvalifikovanog digitalnog potpisa" elektronskog dokumenta, koji je po pravnoj snazi ekvivalentan papirnom dokumentu potpisanom i overenom na klasičan način – olovkom i pečatom.

IV. INFRASTRUKTURA SA JAVNIM KLJUČEVIMA

A. Pojam infrastrukture sa javnim ključevima (PKI)

Infrastruktura sa javnim ključevima (eng. *Public Key Infrastrukture,* PKI) predstavlja kombinaciju hardverskih i softverskih elemenata, ljudi, politika i procedura neophodnih za generisanje, skladištenje, upravljanje, distribuciju i opoziv digitalnih sertifikata. Njena osnovna uloga je uspostavljanje ***digitalnog identiteta*** (eng. *digital IDs*) subjekata u okviru mreže baziraniog na digitalnim sertifikatima, čime se stvara pogodno okruženje za realizaciju drugih bezbednosnih servisa, prvenstveno onih kod kojih je od značaja autentičnost subjekata koji komuniciraju.

Infrastruktura sa javnim ključevima (PKI) se bazira na politici zaštite informacionog sistema u kome se primenjuje. Politika zaštite uspostavlja i definiše osnovne pravce i strategiju razvoja bezbednosti informacionog sistema organizacije, propisuje procedure i principe korišćenja kriptografskih mehanizama u sistemu (način upravljanja ključevima), propisuje neophodne nivoe kontrole koji odgovaraju nivoima rizika itd.

Drugačije rečeno, uspostavljanje infrastrukture sa javnim ključevima (PKI) je osnovni preduslov za realizaciju sistema zaštite. Servisi infrastrukture sa javnim ključevima

(PKI) koriste se na svim nivoima zaštite računarskih resursa i mreža.

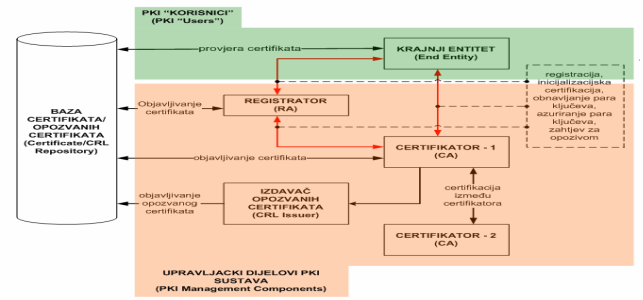
Primeri aplikacija zasnovanih na infrastrukturi sa javnim ključevima (PKI) su:

- formiranje virtualne privatne mreže (eng. *Virtual Private Network,* VPN)
- formiranje pouzdanog sistema zaštite na transportnom nivou u računarskoj mreži
- zaštita E-mail servisa
- zaštita WEB transakcija
- bezbedna razmena dokumenata
- kontrola radnog vremena i pristupa određenim prostorijama.

B. Sastav infrastrukture sa javnim ključevima (PKI)

Infrastruktura sa javnim ključevima (PKI) sastoji se iz sledećih komponenti:

- sertifikacionog autoriteta (eng. *Certification Authority,* CA), koje izdaje digitalne certifikate i reguliše način njihove upotrebe tokom perioda važnosti
- osnovnog dokumenta rada Politike sertifikacije (eng. *Certificate Policy*, CP), koja utvrđuje osnovne principe rada CA i ostalih komponenti Infrastrukture sa javnim ključevima (PKI)
- praktičnih pravila rada (eng. *Certificate Practice Statement*, CPS), predstavljenih dokumentom koji praktično opisuje rad CA i neophodan je u slučaju komercijalnog rada. CPS je detaljan dokument koji sadrži operacione procedure za realizaciju principa koji su navedeni u politici sertifikacije i predstavlja praktičnu podršku sistemu. On uključuje definicije kako je CA formiran, kako radi, kako se generišu digitalni sertifikati, kako se povlače, kako će ključevi biti generisani, registrovani i sertifikovani, gde će se čuvati i kako će biti raspoloživi korisnicima
- registracionih autoriteta (eng. *Registration Authority,* RA), koji predstavljaju interfejs odn. mesta za podnošenje zahteva za izdavanje sertifikata
- komunikacionih sistema za razmenu podataka između registracionog i sertifikacionog autoriteta, distribuciju zahteva za izdavanje sertifikata i slanje digitalnih sertifikata.
- kriptografskih aplikacija za realizaciju funkcija infrastrukture sa javnim ključevima (PKI) subjekata koji komuniciraju u mrežnom okruženju, na bazi izdatih digitalnih sertifikata
- krajnih korisnika odn. subjekata koji komuniciraju.



Slika 5. Sastav infrastrukture sa javnim ključevima (zasnovanog na ITU/T X.509)

V. UMESTO ZAKLJUČKA

Sve brži razvoj informacionih sistema i promet elektronskih dokumenata u državnoj administraciji, bankarstvu, pravosuđu i ostalim sferama društva, kao i komuniciranje u otvorenim mrežama bez direktnog ličnog kontakta, zahteva nove oblike utvrđivanja identiteta i zaštite sadržaja koji se razmjenjuje.

Dok se funkcije zaštite tajnosti i integriteta podataka mogu realizovati i primenom tradicionalnih simetričnih tehnika, funkcije autentičnosti i neporecivosti transakcija zahtevaju primenu asimetričnih kriptografskih sistema. Najbolje karakteristike pokazuju sistemi u kojima su realizovane sve pomenute četiri funkcije. Infrastruktura sa javnim ključevima (PKI) obezbeđuje pouzdan metod za realizaciju sva četiri osnovna bezbednosna zahteva (servisa), koji je baziran na precizno utvrđenoj politici rada. Ona će brzo postati ključna karika svih sistema elektronske trgovine i korporacijske bezbednosti i sigurno će dominirati u bezbednosnim sistemima budućnosti.

LITERATURA

[1] „Osnovi bezbednosti i zaštite informacionih sistema“, Milan Milosavljević, Gojko Grubor

[2] „Da li ste sigurni da ste bezbedni“, Boško Rodić, Goran Đorđević

[3] „Tehnike zaštite podataka i kriptografski protokoli u savremenim računarskim mrežama“, Milan Marković

[4] „Handbook of Applied Cryptography“, Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone

[5] „Cryptography and Network Security“ , Stallings W

[6] „Java Cryptography“, Jonathan Knudsen.

ABSTRACT

Digital certificates are digital files that certify the identityof an individual or institution seeking access to com-puter-based information. In enabling such access, theyserve the same purpose as a driver’s license or librarycard. The digital certificate links the identifier of anindividual or institution to a digital public key.

The combination of standards, protocols, and softwarethat support digital certificates is called a public key infrastructure, or PKI.

DIGITAL SIGNATURE AND DIGITAL CERTIFICATE

Dejan Djordjevic