1. UVOD

Zahvaljujući razvoju tehnike danas se može govoriti o informacionom društvu gdje upotreba znanja i informacija ima centralnu ulogu, što je dovelo po potpuno novog načina poslovanja. Dok su u prošlosti ugovori i poslovi sklapani uglavnom lično, sada se to radi i sa udaljenih lokacija uz pomoć informaciono-komunikacionih tehnologija. Kako su u pitanju vrlo osjetljive informacije, finansije i korporativne tajne, bitno je zadržati povjerljivost relevantnih podataka, a takođe i utvrditi identitet sagovornika koji nije lično prisutan. Širenje interneta na globalnom nivou je doprinijelo razvoju ovog vida elektronskog poslovanja. To je donijelo mnoge prednosti kao što su ubrzanje rada, automatizacija, veća efikasnost, ali i nove probleme po pitanju bezbjednosti. Implementacija bezbjedne komunikacije putem interneta nije jednostavna s obzirom na njegovu otvorenu strukturu, zbog čega je bilo neophodno kreiranje novog sistema zaštite. Za tu svrhu se danas najviše koristi PKI (*Public Key Infrastructure*) infrastruktura [1].

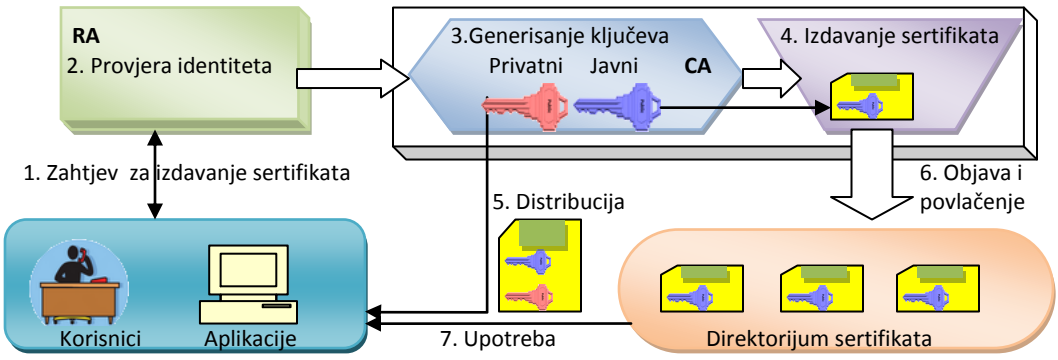
PKI infrastruktura podrazumijeva kompleksan sistem koji se sastoji iz niza različitih elemenata u koje spadaju hardver, softver, zaposleni u administraciji, korisnici, poslovna politika i procedure za digitalne sertifikate - njihovo kreiranje, distribucija, upravljanje i povlačenje. Na ovaj način omogućeno je da se svi podaci, poruke, službeni dokumenti prije slanja zaštite na način da se digitalno potpišu ili enkriptuju. Kada se koristi samo digitalni potpis on omogućava provjeru autentičnosti, neporecivosti i integriteta, odnosno kad se potpisana poruka pošalje eventualni presretač ima mogućnost da je pročita ali ne i da je mijenja bez detekcije. Uglavnom kad poruka stigne kod primaoca on može utvrditi identitet pošiljaoca, garanciju da je poruku zaista poslao pošiljalac, i verifikovati da nije modifikovana. Digitalni potpis ima praktičnu i pravnu validnost, u skladu sa zakonom, kao i svojeručni potpis. U slučaju da se želi omogućiti i tajnost informacija koje se šalju koristi se enkripcija, a zaštićena poruka se naziva envelopa [2].

Obe primjene se baziraju na šifrovanju pomoću enkripcionih algoritama sa kriptografskim ključevima. Ranije su algoritmi bili tajni, i na čemu se bazirala njihova 'snaga', dok su sada javni i standardizovani, a sigurnost im se bazira isključivo na tajnosti ključeva. Struktura PKI sistema zahtjeva zaštićenu distribuciju ključeva, što spada u najkomplikovanije elemenata PKI infrastrukture, a digitalni sertifikati su jedan od načina distribucije. Oni, uz ostale atribute, sadrže date ključeve i služe za njihov prenos, a za cjelokupno upravljanje sertifikatima zaduženo je sertifikaciono tijelo, tj. CA (*Certificate Authority*).

Digitalni sertifikat je elektronski potpisan dokument koji potvrđuje vezu javnog ključa sa entitetom kome pripada. Može se reći da je to jedna vrsta lične karte u virtuelnom svijetu informacija i predstavlja digitalni identitet vlasnika sertifikata. Sadrži bitne podatke kao što su ime osobe ili naziv organizacije kojoj je izdan, javni ključ korisnika, datum izdavanja, period validnosti, serijski broj, itd. Svi ovi podaci se digitalno potpisuju od strane sertifikacionog tijela koje ga je izdalo, pomoću privatnog ključa CA, čime se garantuje njihova ispravnost. Ovdje je uveden pojam javnog i privatnog ključa asimetričnih algoritama koji se koriste u te svrhe. Ti algoritmi će biti detaljnije objašnjeni u narednim glavama. Za sad je dovoljno reći da svaki korisnik ima par ključeva, od kojih se privatni ključ drži u tajnosti dok je javni dostupan svima, a oni se zavisno od potrebe koriste za šifrovanje i dešifrovanje. Jedna od najčešćih primjena sertifikata je za HTTPS (*HyperText Transfer Protocol Secure*) protokol koga čini spoj HTTP-a sa SSL-om (*Secure Sockets Layer*) ili TLS-om (*Transport Layer Security*) radi povećanja sigurnosti internet komunikacije. Omogućuje bezbjednu vezu klijenta sa serverom, a primjena na internetu se odnosi na obezbjeđivanje autentičnost web stranice i web servera [2].

Najkraće rečeno PKI je infrastruktura sistema sa javnim ključevima koji obezbjeđuju enkripciju za sigurnu komunikaciju preko javnih mreža. Sastoji se od nekoliko osnovnih komponenata prikazanih na slici 1.1, a u koje spadaju:

- CA - Sertifikaciono tijelo, generiše i povlači digitalne sertifikate.
- RA (*Registration Authority*) - Registraciono tijelo, prihvata i provjerava zahtjeve korisnika pa ih prosljeđuje CA za izdavanje sertifikata.
- Osnovni dokumenti rada sistema, definišu politiku sertifikacije i praktična pravila rada.
- Sistem za distribuciju i upravljanje sertifikatima.
- PKI aplikacije, u koje spadaju zaštita web transakcije, e-dokumenata, e-mail i dr.



Slika 1.1 *Model PKI sistema (centralizovan – serversko generisanje ključeva)*

CA odnosno sertifikaciono tijelo je jezgro PKI sistema čije povjerenje zavisi od digitalnog potpisa ovog tijela koji se zasniva na asimetričnom kriptografskom algoritmu i privatnom ključu. Za algoritam se najčešće koristi RSA (*Rivest, Shamir, Adleman*) koji je bezbjedan zbog matematičke neefikasnosti algoritma za faktorizaciju velikih prirodnih brojeva što praktično onemogućava *brute-force*[1] napad za dovoljno velik ključ. Takođe, bitno je znati da u slučaju ako korisnik izgubi svoj privatni ključ ili na bilo koji način dođe do njegove kompromitacije važno je da to prijavi CA koje tad njegov sertifikat povlači i stavlja na listu povučenih sertifikata, CRL (*Certificate Revocation List*), ili objavljuje putem OCSP (*Online Certificate Status Protocol*) protokola.

Danas postoji mnoštvo gotovih PKI sistema od kojih su neka besplatna i *open-source*[2] a druga pak komercijalna. Analiza će se baviti samo *open-source* rješenjima u koja ubrajamo OpenCA, EJBCA, DigiCA, Dogtag, XCA i druga. Suština ovog diplomskog rada je analiza upravo spomenutih rješenja, njihovo poređenje kao i načini implementacije od kojih ćemo jedan detaljno obraditi. Rad će u nastavku pokazati detaljan opis i strukturu cjelokupnog PKI sistema i sertifikacionih tijela kao i njihovih komponenata, a zatim analizirati različite implementacije postojećih *open-source* rješenja. Na kraju su prikazani načini upotrebe CA, CRL i OCSP i izveden je zaključak na osnovu urađene analize.

Cilj istraživanja je bio da uzimajući u obzir neke od bezbjednosnih problema postojećih komunikacionih tehnologija objasni određene načine njihovog prevazilaženja i na kraju da se demonstrira upotreba konkretnog rješenja. Autor se odlučio za obradu ove teme radi rastuće potrebe osiguravanja bezbjednosti u današnjim digitalnim komunikacijama kao i zbog želje da nauči nove načine implementacije i korišćenja spomenute tehnologije.

[1] *Brute-force* napad – strategija u kriptografiji za probijanje zaštite šifrovanih podataka na način da se provjeravaju sve moguće kombincije ključeva dok se ne nađe pravi. Praktično je funkcionalna samo za male ključeve zbog dugog vremena potrebnog za provjeru svih kombinacija čiji broj eksponencijalno raste sa porastom veličine ključa.

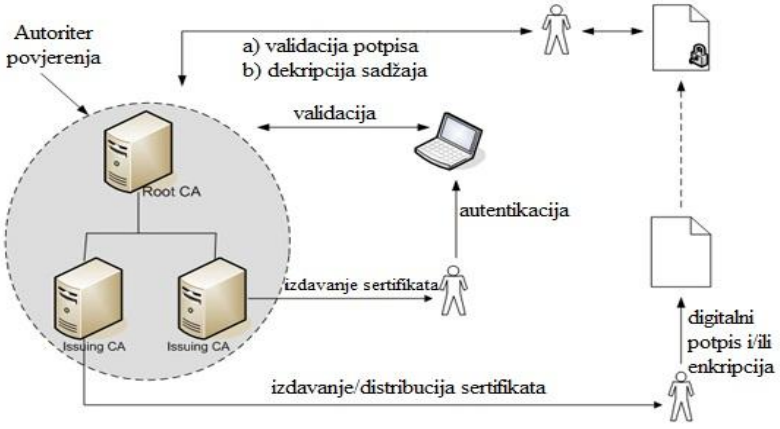
[2] *Open-source* – metodologija razvijanja softvera, može se čak nazvati i filozofija, u kojoj se promoviše besplatna distribucija, zatim pristup gotovoj aplikaciji kao i detaljna implementacije sa kompletnim kodom. Iako koncept dijeljena informacija postoji od ranije ovaj sistem se proširio tek u novije vrijeme zahvaljujući razvoju interneta [3].

2. OPIS PKI INFRASTRUKTURE

Kao što je već rečeno PKI predstavlja tehniku za bezbjednu komunikaciju putem nesigurnih javnih mreža gdje se provjera identiteta osigurava upotrebom digitalnog potpisa. Čini je arhitektura sa javnim ključevima, a zasniva se na upotrebi simetričnih i asimetričnih kriptografskih algoritama. Jedna od glavnih primjena PKI-a je za povećanje bezbjednost u elektronskom poslovanju. Sistem je prilično kompleksan sa mnoštvom različitih komponenata koji čine jednu funkcionalnu cjelinu. U njih spadaju: sertifikaciono tijelo, registraciono tijelo, digitalni sertifikati, sistem za distribuciju i upravljanje sertifikatima, centralni direktorijum sertifikata, sigurnosna politika sistema, zaposleni, korisnici, aplikacije, tokeni i dr. Neke od komponenata već su spomenute a detaljnije će biti analizirane u narednim glavama.

Iako je termin PKI već definisan, radi boljeg razumijevanja treba naglasiti da on može imati više značenja zavisno od konteksta upotrebe. S jedne strane se može reći da predstavlja upotrebu javnog i privatnog ključa odnosno asimetrične kriptografije na čemu je baziran, što je obrazloženo, a sa druge se može odnositi na tehnologije i metode sigurne infrastrukture. Funkcionalnosti koji sistem treba da ponudi korisnicima su:

- Garancija tajnosti informacija
- Pouzdana autentikacija učesnika
- Provjera integriteta podataka
- Uvjerenje da su svi elektronski ugovori pravno validni na sudu kao i štampani ekvivalenti
- Neporecivost transakcije
- Vremensku oznaku poruke



Slika 2.1 *Dijagram funkcionisanja PKI sistema* [4]

2.1 Način funkcionisanja PKI sistema (slika 2.1)

Kriptografski gledano PKI obezbjeđuje povezivanje korisnika i njegovog realnog identiteta sa javnim ključem preko digitalnog sertifikata. Ako se krene od aspekta primjene ove arhitekture vidi se potreba korisnika za sigurnom komunikacijom što se ostvaruje simetričnom ili asimetričnom enkripcijom pomoću odgovarajućih algoritama. Opet za ovaj vid enkripcije neophodna je sigurna razmjena kriptografskih ključeva što predstavlja novu problematiku. Direktna razmjena ključeva jeste moguća ali ona ne daje dokaz o identitetu sagovornika što je sigurnosni problem povjerenja koji PKI rješava upotrebom digitalnih sertifikata. Tako učesnici, prije bilo kakve međusobne komunikacije, moraju prvo imati digitalne sertifikate i razmijeniti ih. Da bi dobili sertifikate korisnici podnose zahtjev registracionom tijelu, koje provjerava validnost tog zahtjeva i njihov identitet, pa u slučaju ispravne potvrde sertifikaciono tijelo vrši izdavanje samog sertifikata sa javnim ključem korisnika i potpisuje ga svojim privatnim ključem. Po izvršenju procedure generisanja ključeva i sertifikata, koja je objašnjena u narednom poglavlju, učesnici mogu realizovati potrebnu bezbjednost i zaštitu u međusobnoj razmjeni informacija.

U ovu svrhu mogu se koristiti usluge specijalizovanih kompanija koje prodaju sertifikate kao što su *'VeriSign'* [5] i '*Comodo'* [6], poznate po obezbjeđivanju sigurnosti u međunarodnim poslovnim transakcijama. Alternativa je napraviti sopstveno sertifikaciono tijelo koje se obično koristi za internu bezbjednost u firmi. Bilo koje rješenje da se koristi ono za krajnjeg korisnika ima ulogu TTP-a (*Trusted Third Party*), odnosno treće strane od povjerenja svim učesnicima [7].

Metode sertifikacije

Generalno postoje tri metode za sertifikovanje od kojih je CA samo jedna, ali najviše korišćena, i kojom se rad isključivo bavi. Ova metoda je već donekle objašnjena a u nastavku je detaljna analiza. Ipak treba spomenuti i druge mogućnosti, gdje je jedna alternativa WoT (*Web of Trust*), a druga SPKI (*Simple public key infrastructure*). WoT šema koristi samopotpisane sertifikate koje potvrđuje treća pouzdana strana i nema centralizovan CA, već se zasniva se na logici distribucije novih sertifikata za koje nam garantuje već provjerena osoba. Primjeri su PGP (*Pretty Good Privacy*) i GnuPGP (*OpenPGP*) koji podržavaju digitalni potpis e-mail-a. SPKI je jednostavniji sistem koji ne povezuje korisnike sa osobama, a ključ je taj kome se vjeruje prije nego osobama. Nema koncept povjerenja jer je izdavač sertifikata istovremeno i verifikator [8].

2.2 Funkcionalni zahtjevi PKI infrastrukture

U opšte zahtjeve koje kvalitetna PKI infrastruktura treba da ispunjava spadaju:

- Nezavisna struktura sa podrškom za različite bezbjednosne politike

Pravilno projektovana arhitektura omogućava vrlo jednostavno prilagođavanje u slučaju promjene bezbjednosne politike sistema ili zakonske regulative koja se odnosi na ovu oblast, što je posebno bitno za kvalitet i pouzdanost sistema.

- Visok nivo sigurnosti sistema

Pošto je CA središnji dio cijelog sistema i predstavlja centralnu tačku povjerenja svih učesnika, najbitnija je bezbjednost upravo ovog tijela i tu se osigurava najveći nivo zaštite. U slučaju kompromitacije CA ili njegovog privatnog ključa narušava se sigurnost kompletnog sistema.

- Skalabilnost

Sistemi su dizajnirani da podržavaju širok dijapazon od malih infrastruktura koje rade na jednom računaru, do kompleksnih infrastruktura za velike korporacije, kao i promjene tokom rasta bez gašenja sistema. U složenim arhitekturama obično postoji više CA sa hijerarhijskom strukturom od kojih je jedan glavni ili korjeni (*Root*) i nalazi se na vrhu, a svaki je potpisan privatnim ključem onih iznad. U takvim situacijama Root CA treba da ima najveći nivo sigurnosti.

- Fleksibilnost - lakoća adaptacije pri ispunjavanju različitih zahtjeva kao što su:

- više načina dostave sertifikata: e-mail, web, VPN (*Virtual Private Network*), lično...
- omogućavanje rada sa raznim HSM (*Hardware Security Module*) modulima i *smart* karticama
- podrška različitim kriptografskim algoritmima
- različiti sistemi objavljivanja i povlačenja sertifikata
- mnogostruke provjere validnosti sertifikata
- podrška hijerarhijskoj strukturi
- višestruki ključevi za jednog korisnika
- prilagodljiv proces autorizacije

- Jednostavnost upotrebe

Struktura treba biti takva da omogući što lakše korišćenje sistema radi smanjivanja potrebne obuke korisnika sistema gdje spadaju: PKI i CA administrator, RA operator, krajnji korisnici.

- Otvorenost sistema - nužna primjena otvorenih standarda radi ispunjavanja potrebe za interoperabilnošću. Važnu ulogu ima X.509 standard koji definiše format digitalnog sertifikata.

3. ANALIZA I PRIMJENA DIGITALNIH SERTIFIKATA

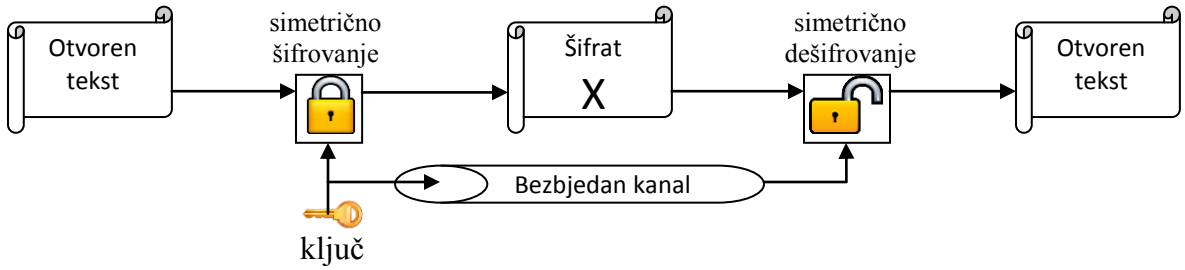
Pojednostavljeno, digitalni sertifikat u računarskom svijetu čini jedan fajl koji sadrži informacije za dokazivanje identiteta vlasnika javnog ključa asimetričnog kriptografskog algoritma. Treba napomenuti da oni nisu isključivo neophodni za funkcionisanje PKI sistema, dovoljna je određena šema koja povezuje ključ sa vlasnikom, a digitalni sertifikati su najčešća implementacija te šeme. Do sad se moglo primijetiti da se sve funkcionalnosti zaštite svode na kriptografske ključeve i algoritme enkripcije tako da će oni prvi biti detaljnije pojašnjeni radi lakšeg razumijevanja cjelokupnog PKI sistema i samih sertifikata.

3.1 Kriptografski algoritmi

Kriptografski algoritmi su procedure za modifikaciju informacije radi obezbjeđenja sigurnosti i tajnosti. Oni otvoren tekst pretvaraju u šifrat pomoću matematičkih funkcija, a u praksi se izvršavaju na računaru. U opštem smislu dijele se na simetrične i asimetrične algoritme.

Simetrični kriptografski algoritmi

Suština im je da za šifrovanje i dešifrovanje imaju iste ključeve koji se čuvaju od javnosti čime obezbjeđuju privatnost i tajnost komunikacije, a što se vidi na slici 3.1. Postoje dvije vrste ovih algoritama: blok šifarski koji procesiraju blokove otvorenog teksta i šifrata, i sekvencijalni (*Stream chiper*) koji procesiraju nizove bita ili bajta. U prve spadaju DES (*Data Encyption Standard*), 3-DES, IDEA, AES (*Advance Encyption Standard* - brži i sigurniji od prethodnih), a često se koriste u modulima uz razne načine upotrebe algoritma sa povratnim petljama i prostim operacijama. Sekvencijalni su pogodniji za hardversku implementaciju, a najpoznatiji je RC4.



Slika 3.1 *Dijagram rada simetrične kriptografije*

Asimetrični kriptografski algoritmi

Nastali su tokom rješavanja problema sigurne distribucije ključeva simetričnih algoritama. Spadaju u najveća otkrića prošlog vijeka u ovoj oblasti, pa i šire, zbog raznih mogućnosti primjene. Koriste različite ključeve za šifrovanje i dešifrovanje, tj. svi učesnici imaju par ključeva, javni i privatni(tajni) koji se po potrebi koriste za jednu od ovih procedura. Treba znati da su oni prilično zahtjevni sa aspekta računarske obrade pa nisu pogodni kod velikog protoka informacija, što i nije poseban problem jer se koriste uglavnom samo za prenos simetričnih ključeva, a dalja komunikacija se osigurava simetričnom enkripcijom koja je veoma brza. Suština snage tih algoritama se ogleda u činjenici da oni omogućavaju uspostavljanje zajedničke tajne informacije kod različitih učesnika bez potrebe za direktnim kontaktom. Ta funkcionalnost se zasniva na matematičkim procedurama od kojih je najpoznatiji RSA algoritam, a pored njega postoje još DSA (*Digital Signature Algoritham*) i ECDSA (*Eliptic Curve DSA*).

RSA se koristi za generisanje para privatnog i javnog ključa, dok mu osnova leži u rješavanju linearne kongruencije, kineskoj teoremi o ostacima i Ojlerovoj teoremi. Procedura je:

- Izbor p i q (prosti, pozitivni) i računanje proizvoda $n = p*q$
- Bira se e iz N, $1<e<\varphi(n)$, $\varphi(n) = (p-1)(q-1)$ da je NZD[3](e, $(\varphi(n))$ = 1
- Računa se d da je $d \equiv e^{-1} mod(\varphi(n))$, drugačije napisano $(d*e) mod\ \varphi(n) = 1$

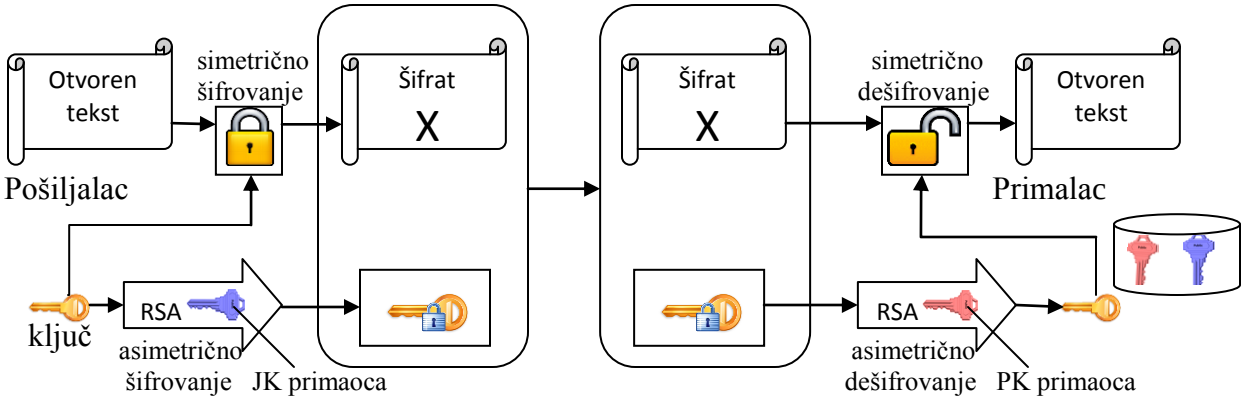
Javni ključ predstavlja par (e,n), a tajni ključ par (d,n) gdje imamo kriptografske transformacije:

- $C_i = M_i{}^e mod(n)$ – šifrovanje
- $M_i = C_i{}^d mod(n)$ – dešifrovanje

Algoritam je bezbjedan zbog neefikasnosti faktorizacije velikih brojeva a sigurnost zavisi od veličine n. Dalje kao što se vidi za kreiranje ključeva je bitan generator prostih brojeva koji koristi algoritme provjere da li je broj prost, a oni nisu baš jednostavni, pa postoje testovi za apsolutno dokazivanje da li je prost, ili sa određenom vjerovatnoćom kao *Miler-Rabinov*. Osnovne funkcionalnosti koje ovaj algoritam omogućava jesu provjere integriteta, autentičnosti i neporicanja, a način upotreba je definisan u standardu PKCS#1 (*Public-Key Cryptography Standards*) [9], gdje su obrazložene metode konstrukcije digitalnog koverta i potpisa.

Kod digitalnog koverta ili **envelope** sadržaj se prvo šifruje simetričnim algoritmom a njegov ključ se zatim šifruje asimetričnim algoritmom uz pomoć javnog ključa primaoca. Na slici 3.2 vidi se postupak kreiranja i slanja envelope, koja se koristi za tajnost poruke [10].

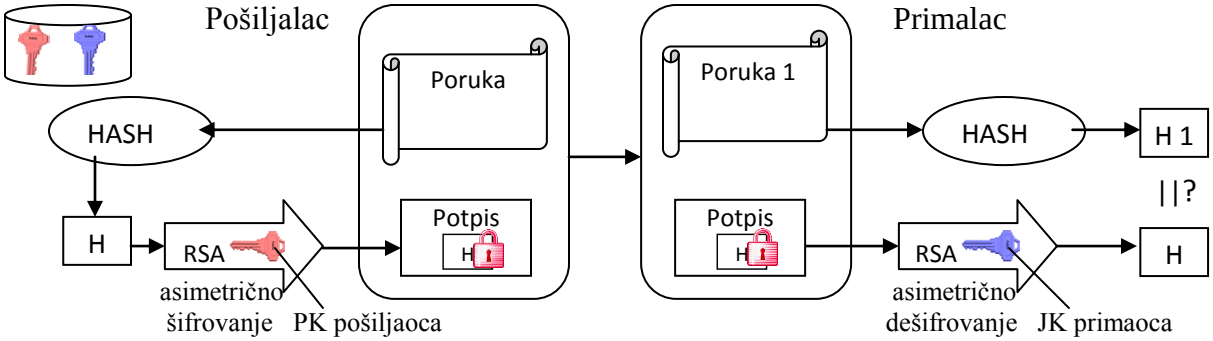
[3] NZD – Najmanji Zajednički Djelilac



Slika 3.2 *Model digitalnog koverta asimetrične kriptografije*

Za **digitalni potpis** (slika 3.3) situacija je malo drugačija pošto se kod njega ne zahtjeva tajnost informacija pa se sam sadržaj poruke šalje u izvornom obliku uz koga se prilaže informacija o potpisu koju čini enkriptovani redukovani otisak poruke tj. MD (*Message digest).* Otisak se dobija pomoću MD algoritama koji predstavljaju jednosmjerne *hash*[4] funkcije, nakon čega se dobijena *hash* vrijednost šifruje privatnim ključem pošiljaoca. Primalac vrši validaciju tako što dešifruje pomenutu *hash* vrijednost javnim ključem pošiljaoca i tako dobijen otisak poredi sa otiskom koji on izračunava iz dobijene poruke. Ako se oni podudaraju to je garancija da poruka nije mijenjana, tj. provjeren je integritet poruke. Na ovaj način, istovremeno su potvrđeni autentičnost pošiljaoca, kao i garancija neporecivosti jer je za potpis korišćen privatni ključ pošiljaoca koji niko drugi nema.

Očigledno da je za ove operacije potreban pristup javnim ključevima sagovornika kao i provjera identiteta što se obezbjeđuje raznim šemama a najčešće upravo digitalnim sertifikatima.



Slika 3.3 *Model digitalnog potpisa asimetrične kriptografije*

[4] *Hash* – procedura koja mapira veliku količinu podataka različite dužine u manju grupu podataka fiksne dužine, od kojih su najkorišćeniji algoritmi MD5, SHA-1 i SHA-2 [10]. Spada u kriptografske algoritme bez ključa.

3.2 Struktura digitalnog sertifikata

S obzirom da je rečeno kako sertifikate izdaje odgovarajuće CA tijelo, korisnik prvo mora kreirati zahtjev za sertifikat (PKCS#10 ili RFC 2511 standard) i poslati ga tom tijelu. Prije kreiranja sertifikata neophodno je imati kriptografski par ključeva koji se prethodno moraju generisati. U zavisnosti od mjesta generisanja tih ključeva, sistem možemo podijeliti na:

1. Centralizovani – kreiranje ključeva se vrši na serveru zajedno sa sertifikatom koji se zatim na određen način dostavljaju korisniku. Ova metoda je jednostavnija, ali manje bezbjedna jer server ima privatne ključeve svih korisnika.
2. Decentralizovani – par ključeva pravi sam klijent na lokalnom računaru, a zatim sistemu šalje svoj javni ključ zajedno sa zahtjevom za sertifikat koji samopotpisuje svojim privatnim ključem. Time server ima garanciju da je to zaista ključ onog ko se predstavlja kao vlasnik, a korisnik je siguran da niko osim drugi nema njegov privatni ključ.

Digitalni sertifikati imaju strukturu u skladu sa standardom X.509 koju čine sljedeća polja [11]:

- Broj verzije formata (validno 1 ili 3, v3 je proširen ekstenzijama, a v2 se ne preporučuje[5])
- Serijski broj sertifikata (jedinstven redni broj koji CA dodjeljuje pri kreiranju sertifikata)
- Identifikator algoritma kojim se vrši potpisivanje (oznaka asimetričnog algoritma i heš-a)
- Naziv sertifikacionog tijela koje ga je izdalo, čine ga komponente:
    - Ime vlasnika
    - Odjeljenje u organizaciji
    - Organizacija
    - Mjesto
    - E-mail
    - Regija
    - Država
- Rok važnosti sertifikata (period validnosti, sadrži početak i kraj važnosti)
- Naziv vlasnika sertifikata (*Distinguished Name - Dname*), komponente kao i naziv CA
- Digitalni potpis sertifikata privatnim ključem sertifikacionog tijela
- Javni ključ vlasnika (numerička reprezentacija)
- Specifični podaci o uslovima korišćenja
- Heš vrijednost javnog ključa
- Polje dodatnih atributa

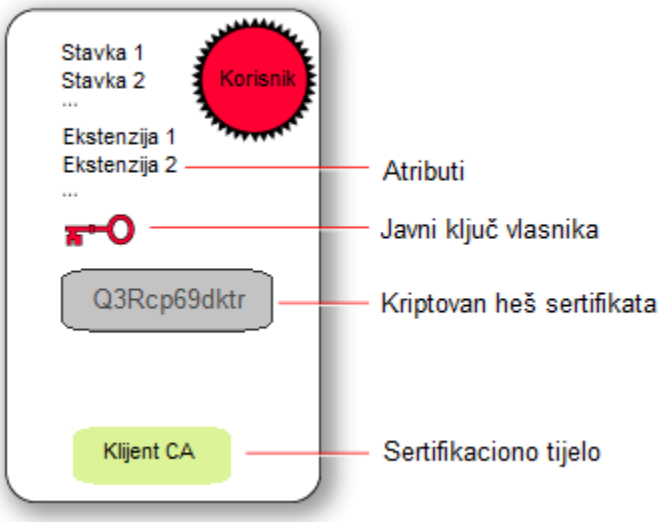
[5] X.509 v2 – kad se jedan CA ugasi dozvoljava ponovnu upotrebu njegovog imena za novi CA, ali se više ne koristi

3.3 Primjena digitalnih sertifikata

Očigledno je da su mogućnosti primjene digitalnih sertifikata veoma, a možda je najveća upotreba u poslovnim aplikacijama kao i finansijama. Primjeri upotrebe su [12]:

- Implementacija elektronskog potpisa – čini ga skup podataka pridruženih odgovarajućem dokumentu i služi za identifikaciju potpisnika a formira se pomoću kriptografskog ključa
- Digitalno potpisivanje pošte(e-mail), e-dokumenata i softvera
- Verifikacija potpisa
- Razmjena dijeljenog ključa za simetrični algoritam kod envelope
- Šifrovanje i dešifrovanje podataka
- Identifikacija, npr. u ličnim dokumentima
- Prijava na različite vrste sistema, kao i fizička kontrola pristupa
- Zaštita sadržaja (*DRM - Digital Rights Management*)
- Za elektronske sisteme plaćanja koji koriste digitalne sertifikate
- Ispunjavanje zahtjeva za sigurnošću transakcija u mobilnom poslovanju
- U VPN-u za zaštićenu vezu između udaljenih korisnika i korporativne mreže, a neka od VNP rješenja su: *OpenVPN, Cisco VPN, LogMeIn, Shrew Soft, Windows Built-In* [13].

Iako je digitalni sertifikat samo podatak na disku, praktično niz brojeva, na osnovu informacija i atributa koje sadrži, može se grafički prikazati njegov izgled kao na slici 3.4.



Slika 3.4 *Vizuelni prikaz modela digitalnog sertifikata*