UDC: 004.738.5:339 INFO M: str. 9-14

UPRAVLJANJE ŽIVOTNIM CIKLUSOM DIGITALNIH SERTIFIKATA
DIGITAL CERTIFICATES LIFE CYCLE MANAGEMENT

Goran Miličić

REZIME: Ovaj rad daje pregled osnovnih pojmova vezanih za digitalni potpis, digitalne sertifikate i faze životnog ciklusa digitalnih sertifikata. Namera je da se čitaocu pomogne da razume sigurnosne probleme koji su povezani sa dobijanjem i upravljanjem digitalnim sertifikatima, kao i da asistira kako postojećim tako i novim korisnicima PKI, kod nekih ključnih koncepata i odgovornosti koji se mogu javiti pri radu sa sertifikatima.
KLJUČNE REČI: Kriptografija, PKI, digitalni sertifikati, digitalni potpis, sertifikacioni autoritet (CA), zahtev za izdavanje sertifikata (CSR), lista povučenih sertifikata (CRL).
ABSTRACT: This paper gives a general overview of basic principles related to digital signatures, digital certificates and phases of digital certificates life cycle. The purpose is to help readers understand the security issues related to obtaining and managing digital certificates, and to assist both current and new users of PKI on some of the key concepts and responsibilities they face when working with certificates.
KEY WORDS: Cryptography, PKI, digital certificates, digital signatures, Certification Authority (CA), Certificate Signing Request (CSR), Certificate Revocation Lists (CRL).

1. UVOD

Kriptologija je termin koji potiče od grčkih reči kriptos (skriven, tajan) i logos (nauka), i označava naučnu disciplinu koja se bavi sigurnim (tajnim) komunikacijama.

Simetrična kriptografija ili tzv. kriptografija tajnih ključeva, je najstariji oblik kriptografije, stara gotovo koliko i ljudska komunikacija. Ona se razvijala i koristila kao alat za zaštitu 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 i dužine ključa.

Javni interes za kriptografiju drastično je porastao 1976. godine 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.

1978. godine definisan je prvi praktični, asimetrični algoritam, koji se označava sa RSA (početna slova imena njegovih autora Rivesta, Shamira i Adlemana) i koji je iskorišćen za kreiranje digitalnog potpisa (eng. Digital Signature, DS). 1991. godine usvojen je prvi standard digitalnog potpisa, baziran na RSA asimetričnom algoritmu. 1994. godine 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 autentikacije elektronskih dokumenata. Sve ovo, uz ubrzan razvoj savremene komunikacije preko različitih medija (najviše Interneta), dovelo je do realizacije infrastrukture sa javnim ključevima (PKI) koja omogućava sigurnu komunikaciju preko nesigurnog kanala [1].

Prva praktična primena PKI počela je u SAD kada je tadašnji američki predsednik Bil Klintom, juna 2000. godine, po prvi put upotrebio PKI tehnologiju prilikom potpisa Zakona o elektronskom potpisu. Tom prilikom predsednik Klinton je dokument o usvajanju ovog Zakona simbolično potpisao naliv-perom i svojim digitalnim potpisom.

2. OPIS PROBLEMA KOJI SE REŠAVA

Digitalni sertifikati su ekvivalentni ličnoj karti, vozačkoj dozvoli, pasošu ili nekom drugom dokumentu pomoću kojeg je danas moguće dokazati identitet. Jedina razlika je što se digitalni setifikati primenjuju u konjukciji sa sistemom enkripcije javnim ključevima. Digitalni setifikati se koriste svuda gde je neophodno ostvariti sigurnu i bezbednu komunikaciju i dokazati identitet učesnika i integritet podataka u komunikaciji. Najčešća primena je pri digitalnom potpisivanju e-mail poruka i elektronskih dokumenata, prilikom pristupanja računarskim resursima umesto korisničkog imena i lozinke, kod organizacija kojima je potreban pouzdan dokaz identiteta, kod servera koji moraju da dokažu da se na njima nalazi sadržaj koji korisnik zahteva, za softver za koji mora da se dokaže poreklo, za 'online' bezbedne poslovne transakcije između kompanija, za sigurnost organizacija u privatnom, javnom i državnom sektoru.

Kvalifikovani digitalni sertifikat, po Zakonu o digitalnom potpisu i pripadajućim podzakonskim aktima, izdaju se od treće strane, tj. Strane od poverenja, poznate kao Sertifikacioni autoritet ili CA (Certification Authority) koji ispunjava određene zakonske uslove i ima dozvolu za rad. Kvalifikovani digitalni sertifikat sa odgovarajućim parom ključeva se može upotrebiti za kreiranje kvalifikovanog digitalnog potpisa, elektronskog dokumenta koji je po pravnoj snazi ekvivalentan papirnom dokumentu potpisanom na klasičan način – olovkom i pečatom.

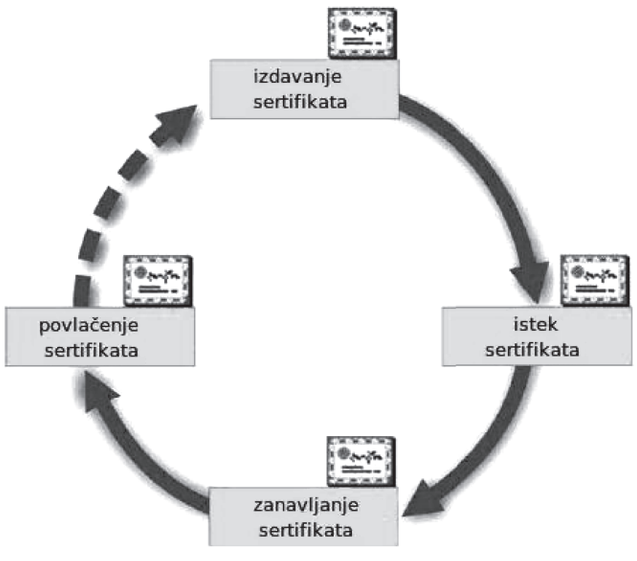
Čak i prema pomenutom zakonu, postoji nekoliko izuzetaka, gde se digitalni sertifiakati ne priznaju. To su, prenos prava svojine na nepokretnosti, sklapanje braka ili uređenje imovinskih odnosa između bračnih drugova, ugovori o poklonu ili doživotnom izdržavanju, sporazumi u vezi sa nasleđem.

Elektronsko bankarastvo, virtualna trgovina i drugi elektronski servisi koje obezbeđuju sigurno plaćanje putem nesigurnih mreža, kao što je Internet, svoju sigurnost zasnivaju na digitalnim sertifikatima. Mnogi sistemi elektronske pošte kao Privacy Enhanced Mail (PEM) ili Secure/Multipurpose Internet Mail Extensions (S/MIME) za ostvarivanje sigurne elektronske pošte koriste digitalne sertifikate za potpisivanje ili kriptovanje/dekriptovanje pošte. Digitalni sertifikati se u sistemima sa digitalnim potpisivanjem dokumenata mogu koristiti kao zamena za ručne potpise, pri čemu digitalno potpisan dokument ima istu snagu i značaj kao i onaj koji je potpisan rukom.

Digitalni sertifikati imaju dve osnovne funkcije. Prva je, da svedoči da su ljudi, web stranice, mrežni resursi kao što su serveri ili ruteri, upravo oni za koje se izdaju da jesu, odnosno, da potvrdi njihov identitet. Druga funkcija je, da obezbedi zaštitu podataka, njihovu izmenu ili krađu, prilikom interakcije između korisnika i raznih servisa. Ova druga funkcionalnost digitalnih sertifikata je bitna upravo u elektronskom poslovanju, gde je tajnost, zaštita i autentičnost podataka od suštinskog značaja.

3. ŽIVOTNI CIKLUS DIGITALNIH SERTIFIKATA

Svaki digitalni sertifikat tokom svoje primene, od izdavanja pa sve do povlačenja ili isteka važenja, prolazi nekoliko faza. Te faze predstavljaju životni ciklus digitalnih sertifikata. Tokom životnog ciklusa digitalnog sertifikata sertifikacioni autoritet izvršava sledeće poslove: izdavanje, obnavljanje, suspendovanje i opozivanje digitalnih sertifikata, objavljivanje liste povučenih sertifikata – CRL, uzajamna sertifikacija sa drugim sertifikacionim telima i sl.



Slika 1. – *Faze životnog ciklusa digitalnih sertifikata*

Životni ciklus digitalnih sertifikata može se podeliti u pet ključnih faza, pri čemu te faze mogu da imaju svoje podfaze [2]:

– izdavanje sertifikata,
– podnošenje zahteva,
  – generisanje zahteva (CSR),
  – provera informacija,
– istek sertifikata,
– zanavljanje sertifikata,
– povlačenje sertifikata.

3.1. *Izdavanje sertifikata*

Infrastruktura javnih ključeva satoji se od dva elementa – samog ključa i infrastrukture. Dok javni ključ može skoro svako da obezbedi, upravljanje ključevima tj. infrastrukturom je komplikovano i ključno za ostvarivanje uspešnog funkcionisanja PKI. Budući da individualci i organizacije uglavnom nemaju ni resurse ni znanje za ostvarivanje odgovarajuće infrastrukture, to je razlog zašto se oni obraćaju sertifikacionim autoritetima (CA). CA obično zahteva da se podnosilac zahteva za sertifikat obaveže na određene obaveze prilikom korišćenja sertifikata. Neke od tih obaveza su:

– Podnosilac zahteva mora odmah da obavesti CA u slučaju promene u upotrebi sertifikata.
– Podnosilac se obavezuje da će par ključeva koristiti na propisan način.
– Mora se obavezati da će tajni ključ čuvati na adekvatan način i da će ga štititi od falsikovanja ili gubitka.
– Podnosilac ili korisnik ključa mora garantovati da ni jedan iz para ključeva neće nikada dati nikom drugom i da će ih isključivo koristiti samo vlasnik.
– Obavezuje sa na to da neće koristiti ključ nakon njegovog isteka ili nakon što je bio povučen.
– Da će odmah obavestiti CA u slučaju gubitka ili diskreditacije ključa na bilo koji način.
– I konačno, podnosilac se obavezuje da će u potpunosti poštovati ugovor potpisan sa CA.

U zavisnosti od vremena, novca i toga da li se sertifikat izdaje za pojedinca ili uređaj, zahtev za dobijanje digitalnog sertifikata moguće je podneti na sledeće načine:

– Skuplji i sporiji način je da se lično obrati CA i podnese zahtev. Pre nego što dođe u prostorije CA, podnosilac zahteva na svom računaru generiše par ključeva. Sada, kada ima javni i tajni ključ podnosilac zahteva odlazi do kancelarije CA. Dužnost CA je da utvrdi identitet podnosioca zahteva.

– Drugi, jefiniji i brži način je da se zahtev podnese preko web-a. Podnosilac zahteva na svom računaru generiše par ključeva. Nakon generisanja ključeva podnosilac zahteva odlazi na web sajt CA gde unosi svoje ime, adresu, telefonski broj, e-mail i druge podatke ako je potrebno. Na osnovu toga kompjuter generiše zahtev za sertifikat, koji uključuje informacije koje je podnosilac uneo i njegov javni ključ. Zatim se zahtev za sertifikat potpisuje tajnim ključem podnosioca. Ovo je veoma bitno jer podnosilac mora da dokaže da poseduje tajni ključ koji odgovara javnom ključu koji se nal-

azi u zahtevu. CA može proveriti zahtev koristeći javni ključ podnosioca. Tako dobijenu formu CSR (Certificate Signing Request), podnosilac zajedno sa brojem svoje platne kartice prosleđuje na CA web sajt.

– Ukoliko se podnosi zahtev za sertifikat koji treba da se nalazi na smart kartici, podnosilac zahteva prvo mora da kupi odgovarajuću smart karticu i odgovarajući čitač kartica. Smart kartica mora imati sledeće karakteristike: na njoj se može generisati tajni i javni ključ, sa kartice svako može da pročita javni ključ ali ne i tajni ključ, mogućnost potpisivanja i kriptovanja podataka pomoću čitača povezanog na računar, brisanje memorije kartice da bi se uništili podaci na njoj. Nakon toga podnosilac odlazi do CA kancelarije da podnese zahtev za dobijanje sertifikata.

– Ukoliko se podnosi zahtev za neki hardverski uređaj, na primer: web server, računar koji je sposoban da sam sebi generiše par ključeva (tajni i javni) ili neki drugi uređaj koji nije u stanju da sam generiše ključeve, na primer Wireless Access Point ili WAP sa kojim se komunicira korišćenjem digitalnih sertifikata. Pošto uređaji ne mogu sami sebe da registruju, za to im je potrebna osoba koja će to obaviti. Zahtev za uređaje podnosi osoba koja je odgovorna za njihovo funkcionisanje. Prilikom podnošenja zahteva koristiće se identitet odgovorne osobe. Odgovorna osoba pored dokazivanja svog identiteta mora dokazati i da su uređaji, za koje se podnosi zahtev, pod njenom kontrolom.

Pre nego što se neki sertifikat izda, Sertifikacioni autoritet mora verifikovati identitet podnosioca zahteva. Ta verifikacija može uključivati čitavu seriju provera. Pošto provera identiteta podnosioca predstavlja prvu fazu u životnom ciklusu digitalnih sertifikata, organizacije koje predstavljaju sertifikacione autoritete moraju da budu potpuno sigurne u to da je osoba ili organizacija koja zahteva sertifikat upravo ona za koju se predstavlja, u protivnom čitav PKI bi bio kompromitovan. Ako ne verujete CA-u, ne možete koristiti ni usluge tog CA. Upravo zato CA uvodi više različtih provera identiteta podnosioca zahteva, kao što su:

– Identifikacija podnosioca – ime, adresa, telefon, e-mail.
– Identifikacija organizacije – ime, adresa, telefon i tip poslovanja kojim se bavi organizacija.
– Identifikacija namere korišćenja sertifikata – sertifikat se može izdati za različtite namene, a može se izdavati kako fizičkim licima tako i hardverskim uređajima.

Poslednja aktivnost koja se obavlja prilikom izrade sertifikata je izdavanje samog sertifikata. Registracioni Autoritet (RA) u ime CA generiše referencijalni broj za nalog, a nakon toga i autorizacioni kod. Oba koda se daju podnosiocu zahteva. Podnosilac zahteva sada koristi računar da kreira formu zahteva za sertifikat. Ta forma uključuje sledeće:

– informacije, koje je ranije dostavio CA (ime, adresa, e-mail ...)
– autorizacioni kod koji je CA napravio
– javni ključ podnosioca zahteva

Podnosilac tada koristeći svoj tajni ključ potpisuje formu zahteva za sertifikat. Ovo je veoma bitno pošto CA neće izdati sertifikat ako ne uspe da, na osnovu javnog ključa koji se nalazi u zahtevu, uspešno verifikuje digitalni potpis na zahtevu za dobijanje sertifikata. Nakon toga podnosilac odlazi na web sajt CA i koristeći svoj referencijalni broj prosleđuje mu CSR. Nakon što je primio CSR, CA vrši dodatne provere. Prvo, proverava da li su refencijalni broj i autorizacioni kod odgovarajući. Zatim koristeći javni ključ iz zahteva proverava digitalni potpis kojim je potpisan zahtev. Ukoliko su sve provere prošle bez problema, CA izdaje sertifikat i šalje ga nazad ka podnosiocu. CA istovremeno objavljuje taj sertifikat u javnom repozitorijumu, tako da svako može proveriti njegov identitet.

Kada se uspešno uradi provera podataka koje je dostavio podnosilac zahteva (bilo preko web-a ili ličnim dolaskom u kancelarije CA) i kada se takav zahtev (CSR) potpiše digitalnim sertifikatom od strane CA, dobija se digitalni sertifikat za korisnika koji je podneo zahtev. Izdavanjem tog sertifikata završava se prva faza životnog ciklusa digitalnog sertifikata. Nakon toga očuvanje tajnosti i integriteta tajnog ključa je ključno za uspešno funkcionisanje PKI.

3.2. *Istek sertifikata*

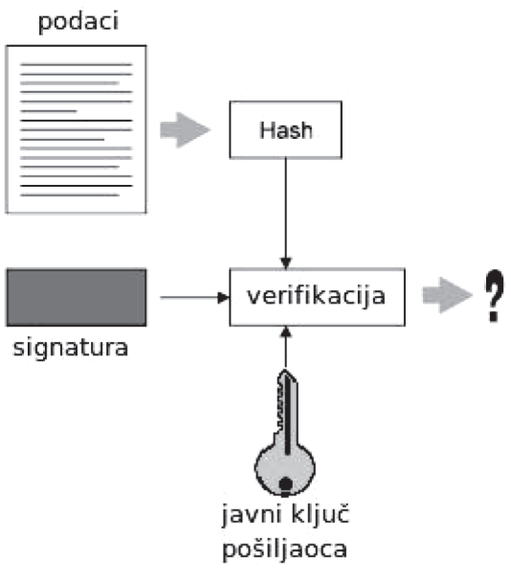
Da bi se dodatno smanjila mogućnost da neko na osnovu javnog ključa reprodukuje tajni ključ ili da se na neki drugi način domogne tajnog ključa, Sertifikacioni autoritet izdaje sertifikate sa vremenskim ograničenjem, tako da oni periodično moraju biti zanovljani. Svaki potpis tokom perioda u kojem je sertifikat bio validan ostaje važeći neograničeno dugo, dok su potpisi nakon isteka validnosti signature nevažeći. Budući da svaki sertifikat ima definisano vreme pre kojeg taj sertifikat ne važi, kao i vreme nakon kojeg ne važi, odgovornst je na učesnicima u komunikaciji i softveru koji koriste da redovno proveravaju da li je neki sertifikat validan ili ne.

Jedna od ključnih tehnika za uspešno funkcionisanje PKI je i verifikacija digitalnih sertifikata pošiljaoca. Bez obzira na sve provere koje preduzimaju RA i CA prilikom izdavanaja sertifikata, prevare, krađe i gubici ključeva ili sertifikata uvek su mogući. Da bi se izbegle štetne posledice ovih malicioznih aktivnosti potrebno je vršiti pravilnu verifikaciju sertifikata pošiljaoca.

Ako korisnik primi poruku od drugog korisnika koja je digitalno potpisana, zajedno sa porukom primalac poruke primiće i digitalni sertifikat koji nosi ime pošiljaoca poruke, a izdat je od strane CA. Primalac lako može proveriti digitalni potpis kojim je poruka potpisana, pošto sertifikat uključuje i javni ključ pošiljaoca.

Ali, kako primalac poruke može biti sigura da je ta poruka zaista stigla od pošiljaoca koji se predstavlja u poruci? Kako može znati da li je CA koji je naveden u sertifikatu zaista i izdao taj sertifikat? Kako može biti siguran da li da veruje sertifikatu u poruci?

Prilikom provere sertifikata koji dolazi uz primljenu poruku, primalac poruke može imati dve situacije: da je poruka potpisana digitalnim sertifikatom koji je izdao poznat (veliki, svetski ili nacionalni) CA ili da je poruka potpisana sertifikatom koji je izdao nepoznat (mali, lokalni ili interni) CA [3].



Slika 2. – *Verifikacija ključa pošiljaoca*

Kada primalac dobije poruku koja je potpisana sertifikatom pošiljaoca poruke, izdatim od svetski poznatog CA, tada primalac poruke, ukoliko koristi softver sa ugrađenom listom najpoznatijih sertifikacionih autoriteta i njihovih javnih ključeva (a to je najčešće i slučaj), može lako da proveri verodostojnost takvog sertifikata. Ti poznati sertifikacioni autoriteti nazivaju se 'Trust Anchors' i svakom digitalnom sertifikatu koji je izdat i digitalno potpisan od strane 'Trust Anchors' CA može se automatski verovati. Budući da su ti sertifikati potpisani tajnim ključem tog CA, a da aplikacija koju koristi primalac poruke već ima ugrađen javni ključ koji pripada tom CA, aplikacija jednostavnom verifikacijom pomoću javnog ključa CA može da proveri verodostojnost sertifikata pošiljaoca poruke. Ukoliko je verifikacija uspešna znači da je sertifikat potpisao CA koji je naveden u sertifikatu, pa primalac poruke može da bude siguran da je poruka zaista stigla od onog koji se predstavlja u toj poruci.

Ukoliko primalac dobije poruku od pošiljaoca koja sadrži sertifikat koji je potpisao mali, lokalni CA, koji se prema tome ne nalazi na listi 'Trust Anchor'. Kako u takvoj situaciji primalac može da veruje da je poruka zaista stigla od autentičnog korisnika, ako ne veruje njegovom CA?

Da bi zadobio poverenje za svoje sertifikate 'mali' CA ima svoj sertifikat za potpisivanje, potpisan od strane nekog većeg CA. Taj drugi, veći CA može a ne mora da bude poznat, tj. da bude na listi 'Trust Anchor', ako nije, i taj veći CA ima svoj sertifikat za potpisivanje potpisan od strane još većeg CA. Ovaj lanac poverenja među CA može se nastaviti sve dok se sertifikat ne potpiše od strane nekog poznatog CA koji se nalazi na listi 'Trust Anchor' i uključen je u većinu softvera. Ovaj proces provere lanca poverenje za sertifikat pošiljaoca naziva se put validacije.

3.3. *Zanavljanje isteklog sertifikata*

Proces zanavljanja digitalnih sertifikata razlikuje se u zavisnosti od sertifikacionog autoriteta koji je izdao sertifikat. Uglavnom se zanavljanje sertifikata obavlja bez drugih promena.

Ukoliko korisnik sertifikata treba da zanovi svoj istekli sertifikat, on jednostavno treba da CA-u pošalje zahtev za zanavljanje sertifikata digitalno potpisanog svojim starim sertifikatom i tajnim ključem. Kada primi zahtev, CA pomoću javnog ključa korisnika verifikuje signaturu na zahtevu i kada se uveri u korisnikov identitet, izdaje novi sertifikat sa novim vremenom validnosti, i korisnik može da nastavi da ga koristi.

Korisnikov stari sertifikat ne mora da bude stavljen na CA listu povučenih sertifikata (Certificate Revocation Lists) CRL, zato što će on svakako isteći. Korisnik može da koristi sertifikat odmah po početku važenja njegovog perioda validnosti, međutim, najčešće važnost novog sertifikata počinje prestankom važnosti starog. Ukoliko korisnik želi da počne da koristi novi sertifikat pre nego što je stari istekao, CA će njegov stari sertifikat staviti na CRL dok ne prođe njegov period validnosti, nakon čega ga sklanja sa CRL.

Ukoliko korisnik sertifikata izgubi ili iz nekog drugog razloga želi da promeni svoj tajni ili javni ključ ili posumnja da su ključevi kompromitovani, lako može da generiše novi par ključeva, ali korisnik mora generisati i novi sertifikat da bi reflektovao zamenu ključeva. Da bi generisao novi sertifikat korisnik mora da podnese zahtev za novi sertifikat koji potpiše svojim tajnim ključem i prosledi taj zahtev do CA. CA kreira novi sertifikat i potpiše ga svojim tajnim ključem i vrati ga korisniku. Prema tome, postupak zamene starog sertifikata novim, potpuno je analogan izdavanju prvog sertifikata.

3.4. *Povlačenje sertifikata*

Kada se sertifikat izda za očekivati je da se on koristi tokom celog perioda njegove validnosti. Međutim, razne okolnosti mogu dovesti do toga da sertifikat postane nevažeći pre isteka njegovog perioda validnosti. Te okolnosti mogu biti različite. Svaki CA, po svom nahođenju, može da povuče neki sertifikat, ukoliko korisnik sertifikata ne poštuje neku od odredbi ugovora potpisanog između korisnika sertifikata i CA, ili ako korisnik nije upotrebio tajni ključ duže vreme (koje je precizno određeno). Pre nego što povuče neki serfikat, CA o tome obaveštava korisnika sertifikata. Nakon što povuče sertifikat, CA ga stavlja na listu povučenih sertifikata, CRL (Certificate Revocation Lists), koja je svima dostupna.

Da bi CA povukao neki sertifikat, mora da postoji zahtev za njegovo povlačenje ili da se steknu određene okolnosti. CA će povući neki sertifikat i staviti ga na CRL ako se pojavi neki od sledećih uslova [6]:

– ukoliko se u sertifikatu promeni neka informacija,
– ukoliko se sumnja ili zna da je došlo do kompromitovanja tajnog ključa ili medijuma na kojem se nalazi tajni ključ,
– u slučaju smrti korisnika sertifikata ili njegovog napuštanja kompanije,
– ukoliko je korisnik sertifikata premešten na novo radno mesto, koje ne zahteva taj sertifikat,

– u slučaju da korisnik sertifikata podnese uredan formular za povlačenje sertifikata.

Kao što je rečeno, sertifikat može povući CA ili korisnik koji je podneo prijavu za izdavanje sertifikata, ali da bi se povukao sertifikat mora da se donese odluka o povlačenju sertifika. Tu odluku može da donese:

– korisnik koji je podneo zahtev za sertifikat ili imenovani korisnik sertifikata (ukoliko se sertifikat koristi na uređaju),
– odgovorna osoba u kompaniji koja koristi taj sertifikat,
– autorizovano osoblje u CA,
– automatski proces koji se izvršava u ime CA,
– RA, na zahtev korisnika koji je podneo zahtev za izdavanje sertifikata ili imenovanog korisnika sertifikata ili odgovorne osobe u kompaniji.

U slučaju da je potrebno povući sertifikat koji je CA izdao drugom CA, takozvani 'cross-certificate', zahtev za njegovo povlačenje može se pokrenuti samo od strane:

– CA kojem je izdat cross-certificate,
– autorizovanog osoblja CA koji je izdao sertifikat.

Pored povlačenja sertifikata, CA može da uradi i suspenziju sertifikata, dodavanjem koda 'on hold'. Sertifikati koji su suspendovani ne zahtevaju od korisnika sertifikata nikakve akcije po pitanju privatnog ključa sertifikata. CA neki sertifikat može da suspenduje ukoliko posumnja u kompromitovanje tajnog ključa za taj sertifikat ili medijuma na kojem se čuva tajni ključ. Takođe, sertifikat se suspenduje i ukoliko korisnici sertifikata ne poštuju sve odredbe ugovora, u slučaju određenog broja neuspešnih logovanja primenom sertifikata i kada CA sa razlogom sumnja u neke nepravilnosti prilikom korišćenja sertifikata.

3.5. *Lista povučenih sertifikata, CRL (Certificate Revocation Lists)*

CRL je lista koja identifikuje povučene sertifikate, koja je potpisana od strane CA ili nekog drugog izdavaoca CRL liste, i dostupna u javnom repozitorijumu. Najčešći izdavač CRL-a je CA. CA objavljuje CRL kako bi ponudio informacije o nevažećim sertifikatima koje je izdao. Međutim, odgovornost oko izdavanja CRL-a, CA može da delegira nekom drugom verujućem autoritetu. CRL koje održava CA koji nije izdao sertifikate naziva se indirektni CRL.

Sertifikati su u CRL-u identifikovani svojim serijskim brojem. Svaki CRL ima određeni delokrug (scope). CRL delokrug je skup sertifikata, koji se mogu pojaviti na toj CRL. CRL za svaki delokrug sadrži listu svih neisteklih sertifikata, koji su povučeni iz istog razloga za ceo delokrug. Na primer, delokrug može biti 'svi CA sertifikati izdati od CA X', 'svi sertifikati izdati od strane CA X koji su povučeni zbog kompromitovanja ključa ili kompromitovanja CA' ili neki set sertifikata na osnovu proizvoljnih informacija, na primer 'svi sertifikatai izdati za zaposlene firme Y locirane u mestu Z'.

CA koji izdaje CRL može da objavi 'delta CRL'. Delta CRL sadrži samo one sertifikate unutar delokruga, koji su povučeni nakon objavljivanja referentne kompletne CRL. Referentna kopletna CRL predstavlja osnovnu CRL.

Aplikacije koje se koriste za proveru kompletne CRL, moraju obavezno da imaju mogućnost procesiranja i verzije 1 i verzije 2 CRL, koje pružaju informacije o povlačenju svih sertifikata izdatih od strane nekog CA. Za razliku od toga da moraju da imaju mogućnost provere kompletne CRL, aplikacije ne moraju da imaju podršku za delta CRL ili indirektne CRL.

4. ANALIZA – PREDNOSTI/NEDOSTACI

Primenom digitalnih sertifikata ostvaruju se četiri osnovna bezbednosna servisa koja se koriste prilikom korišćenja elektronske razmene podataka [5]:

– Poverljivost – obezbeđuje da informacioni sadržaj poruke bude dostupan samo onim korisnicima koji su ovlašćeni za to.
– Integritet – obezbeđuje otkrivanje neovlašćenih izmena sadržaja poruke. To uključuje umetanje, brisanje ili prepravljanje podataka.
– Autentičnost – omogućava proveru identiteta učesnika u komunikaciji.
– Neporecivost – sprečava mogućnost poricanja određenih aktivnosti tokom komunikacije (kao što su: slanje poruke, izvršenje transakcije, prepravke i dr.). Cilj je da primalac bude siguran u verodostojnost onoga što mu je pošiljalac poslao.

Za razliku od ručnog potpisa, digitalni potpis verifikuje integritet podataka na koje se odnosi. Ako su nakon primene digitalnog potpisa podaci bili izmenjeni, prilikom sledeće provere biće generisan različit 'message hash', a to znači i drugačiji potpis. Prema tome, ako je integritet podataka nekog dokumenta narušen, validacija potpisa biće neispravna.

U određenim uslovima digitalni potpis se može koristiti i za dokazivanje neporecivosti. Ako primalac poruke može da dokaže da pošiljalac poseduje tajni ključ koji je korišćen za generisanje digitalnog potpisa, tada pošiljalac ne može da poriče da je on generisao taj potpis. U principu, za puno ostvarivanje bezbednosnog servisa neporecivosti, trebalo bi da postoji neko treće telo koje će primaocu poruke garantovati da je pošiljalac poruke ujedno i vlasnik tajnog ključa koji je korišćen za potpisivanje poruke.

Neki asimetrični algoritmi (npr. DSA) mogu se koristiti za kriptovanje i dekriptovanje podataka. U praksi ovi algoritmi se retko koriste za kriptovanje velikih količina podataka, pošto su značajno sporiji od simetričnih ključeva. Međutim, oni su savršeno pogodni za kriptovanje malih količina podataka – kao što je simetrični ključ i HMAC. Ova operacija transporta simetričnih ključeva pomoću asimetričnih algoritama naziva se razmena ključeva, i veoma često se koristi [4].

U praksi, pošiljalac generiše simetrični ključ i sa njim kriptuje poruku, zatim kriptuje simetrični ključ koristeći javni ključ primaoca poruke, pa zatim i kriptovanu poruku i kriptovani ključ pošalje do primaoca. Primalac poruke koristi svoj tajni ključ da dekriptuje simetrični ključ koji mu je poslao pošiljalac, tako dobijen simetrični ključ koristi da dekriptuje poruku u 'plaintext' oblik. Prema tome, pošiljalac koristi asimetričnu kriptografiju kako bi obezbedio poveljivost (tajnost) prilikom razmene ključa. Na ovaj način ne obezbeđuju se

dodatni bezbednosni servisi – autentičnost, integritet i neporecivost, budući da pošiljalac koristi javni ključ primaoca poruke, koji može koristiti bilo ko da bi generisao poruku.

Iako ovaj način enkripcije značajno unapređuje sigurnost komunikacija u poređenju sa simetričnom enkripcijom, ni on nije bez nedostataka. Uobičajeni način 'razbijanja' ključa jeste upotreba metoda grube sile. Naime, ukoliko napadač poseduje dovoljnu procesorsku snagu, teoretski je moguć pokušaj razbijanja ključa. Kako su uobičajene dužine ključeva 1024, 2048 i 4096 bita, a algoritam prilično složen, resurse za ovakve napade imaju samo vlade pojedinih zemalja i njihove bezbednosne službe.

Međutim, enkripcija javnim ključem, mnogo je ranjivija na jednu drugu vrstu napada, koji se u literaturi popularno naziva - 'napad-čoveka-u-sredini' (man-in-the-middle-attack). Ovaj napad, podrazumeva postojanje treće osobe (zlonamerne) u lancu komunikacije između dva učesnika. Ukoliko zlonamerna osoba uspe da se domogne javnog ključa pošiljaoca poruke, a zatim svoj javni ključ 'poturi' primaocu poruke, kao javni ključ pošiljaoca, onda on može da menja sadržaj poruka koje se razmenjuju između te dve osobe i samim tim kompromituje njihovu komunikaciju.

Budući da je prilikom izdavanja sertifikata popunjavanjem web obrasca moguće izvršiti samo skromnu i nepouzdanu proveru identiteta, potencijalni napadač to može lako zloupotrebiti.

Ukoliko napadač želi da prisluškuje komunikaciju između pošiljaoca i primaoca, može da poseti web sajt CA i podnese zahtev za dobijanje digitalnog sertifikata predstavljajući se kao neka druga osoba, a koristeći svoj ključ. CA kao meru provere identiteta može telefonom nazvati osobu za koju se izdaje sertifikat, međutim napadač se uvek može predstavi kao ta druga osoba. Nakon toga CA napadaču izdaje sertifikat u ime druge osobe. Taj sertifikat napadač sada može da koristi da pošalje svoju poruku do nekog primaoca, predstavljajući se kao druga osoba. Primalac poruke proverava digitalni potpis i vidi da je sve u redu pošto se kod CA vodi na osobu koja se i predstavlja kao pošiljalac poruke.

Da bi se izbegle ovakve situacije, ukoliko postoje mogućnosti, uvek se preporučuje da se sertifikat pribavi podnošenjem zahteva direktno u kancelariji CA.

Prema tome, redovna i kvalitetna provera i verifikacija sertifikata koji dolaze uz poruku je siguran način za sprečavanje bilo kakvih zlouptreba ili malicioznih radnji. Međutim, osnovni uslov infrastrukture sa javnim ključevima i dalje mora biti strogo ispoštovan, a to je da sve strane koje učestvuju u komunikaciji moraju adekvatno čuvati svoj tajni ključ [4].

5. ZAKLJUČAK

Iako su najvažniji zakonski preduslovi ostvareni (postojanje Zakona o elektronskom potpisu i podzakonskih akata), korišćenje kvalifikovanog digitalnog potpisa u Republici Srbiji još uvijek nije primenjeno. Razlozi za to zasigurno nisu samo pravni (iako je za potpuno zaokruženje pravnog sistema elektronskog poslovanja potrebno sačekati donošenje Zakona o elektronskom dokumentu). Deo razloga zašto kvalifikovani digitalni potpis još nije zaživeo u praksi svakako je nedostatak odgovarajuće tehničke infrastrukture. Međutim, neki od razloga sigurno spadaju u sferu sociologije i psihologije, kao što su tradicija korišćenja papira, nepoznavanje tehnoloških mogućnosti, nekorišćenje Interneta kao nečeg uobičajenog, te stav da je i postojeći način rada dobar.

Sve to usporava širenje elektronskog poslovanja izvan segmenta Internet trgovina, te sličnih sistema namenjenih relativno jednostavnoj kupoprodaji, a koja se odvija i bez upotrebe kvalifikovanog digitalnog potpisa. Veliki deo problema zašto se kvalifikovani digitalni potpis ne koristi dovoljno leži i u činjenici da su njegove mogućnosti još uvek relativno nepoznate izvan uskog kruga stručnjaka za informacionu sigurnost. Stoga je izuzetno bitan uslov edukovanje stručne, pravne i šire javnosti u ovom pogledu, kako bi se u Republici Srbiji u praksi počele koristiti prednosti koje donosi poslovanje uz korišćenje kvalifikovanog digitalnog potpisa.

SAD i Europska Unija stvorili su snažnu pravnu osnovu za izgradnju sigurnog okruženja za unapređenje elektronske trgovine. Naš je zakon izrađen po uzoru na Direktivu Evropske Unije o elektronskim potpisima, pa su na taj način osigurani minimalni preduslovi za priključenje savremenim međunarodnim tokovima. Za pretpostaviti je da će kvalifikovani digitalni potpisi svoju prvu primenu naći u državnoj upravi (e-government) i sudstvu, uprkos njihovoj trenutno nedovoljnoj infrastrukturnoj opremljenosti. Najvažnija će svakako biti primena Zakona o elektronskom potpisu u privredi za koju je digitalni potpis jedna od pretpostavki priključivanja savremenim svetskim poslovnim tokovima.

6. LITERATURA

[1] *Basics of Cryptography & Digital Certificates*; Trusted Internet Services from VeriSign and SafeScrypt; http://safeexim.safescrypt.com/Basics_Of_Cryptography.pdf; 2008.

[2] Dave Coombs; *Certificate Life Cycle*; Carillon information security; 2006.

[3] *Digital Certificates Authentication and Trust on the Internet;* KPMG International; http://www.us.kpmg.com/RutUS_prod/Documents/12/DC80502.pdf; 2008.

[4] D. Richard Kuhn, Vincent C. Hu, W. Timothy Polk, Shu-Jen Chang; *Introduction to Public Key Technology and the Federal PKI Infrastructure;* National Institute of Standards and Technology; 2001.

[5] Miloš Piščević, Dejan Simić: *Reducing E-commerce Risks Using Digital Certificates; Proceedings of the 8th Balkan Conference on Operational Research – BALCOR-2007, Zlatibor, Serbia, 14-17. september 2007.*

[6] Danielle Ruest, Nelson Ruest; *Managing the Certificate Lifecycle;* Thawte; 2005.

Goran Miličić, NIS a.d., NIS-Petrol, OD Rafinerija nafte Novi Sad
Oblast interesovanja: Kriptografija, digitalni potpis, digitalni sertifikati