Infrastruktura javnog ključa

Autor: Irma Masleša
Broj indeksa: IB180101
Fakultet: Fakultet informacijskih tehnologija
Univerzitet: Univerzitet Džemal Bijedić Mostar

Sažetak – Ovaj rad ima za cilj da predstavi osnovu rada infrastrukture javnog ključa i njenu primjenu. Svojim tokom rad će se dotaknuti osnova tema koje su potrebne za razumijevanje infrastrukture javnog ključa. Te teme su kriptografija, kao i vrste kriptografije, digitalni potpis i digitalni certifikat. U glavnom dijelu rada se fokus stavlja na samu infrastrukturu javnog ključa, njene komponente, način rada kao i njene primjene. Rad je koncipiran tako da čitaoca sa predznanjem iz oblasti informacijske sigurnosti upozna sa konceptom.

Ključne riječi – infrastruktura javnog ključa, kriptografija, plain text, cipher text, privatni ključ, javni ključ, simetrična kriptografija, asimetrična kriptografija, digitalni potpis, digitalni certifikat

I. UVOD

Hijeroglifi uklesani na stelama 3000 godina prije nove ere se smatraju najstarijim poznatim primjerom enkripcije. [1] Od tada, pa sve do danas, je enkripcija konstantno napredovala. Kriptografija predstavlja metodu zaštite informacija upotrebom šifri, tako da ih samo osobe kojima su informacije namijenjene mogu pročitati i shvatiti. U računarskoj nauci, kriptografija se odnosi na osiguravanje informacija i algoritme koji se koriste da se informacije pretvore u oblik koji nije svima čitljiv.

Ukoliko se nađete na web stranici koja ne enkriptuje sav sadržaj, našli ste jedan od rijetkih izuzetaka. U današnjem vremenu, vrlo je neobično da neka web stranica šalje bilo kakve podatke u izvornom formatu. Međutim, nije samo sadržaj na web stranicama enkriptovan, i email server koriste enkripciju.

II. KRIPTOGRAFIJA

Međutim, povjerljivost, koja je već spomenuta nije jedini cilj kriptografije. Povjerljivost osigurava tajnost sadržaja za sve osim primatelja i pošiljaoca. Drugi cilj svih kriptosistema je autentifikacija. Pored toga što je važno znati da je sadržan zaštićen, bitno je i znati da li je sadržaj došao od osobe od koje smo očekivali da dođe. Možda i najbitnije, trebamo znati da je poslana poruka ista kao i primljena, što predstavlja integritet. [2] Kriptografski algoritmi mogu izvršiti i ovu vrstu verifikacije, a o tome će biti više riječi u nastavku. Enkripcija predstavlja privatnost, ali bitno je shvatiti da ona nije rješenje za sve probleme. Ukoliko napadač dobije pristup sistemu sa tuđim kredencijalima, podaci se ne mogu smatrati zaštićenima.

Pri enkripciji, početni sadržaj koji je potrebno enkriptovati se naziva plain text. Plain text predstavlja tekst, ili bilo koji drugi tip podatka, koji je čitljiv svima bez da obavljaju bilo kakve operacije nad njim. Nakon što plain text prođe proces enkripcije, dobijamo ono što se naziva cipher text. Cipher text je na prvu nečitljiv i zahtjeva obavljanje određenih operacija kako bi se vratio u čitljivi oblik, odnosno plain text. Operacija potrebna za pretvaranje cipher texta u plain text se naziva dekripcija. [3]

III. SIMETRIČNA KRIPTOGRAFIJA

Simetrična kriptografija je vrsta kriptografija kod koje se koristi samo jedan ključ i za enkripciju i za dekripciju. Ovaj ključ se naziva privatni ključ i s obzirom da se koristi u oba smjera, i za enkripciju i za dekripciju, on je simetričan. U ovom slučaju, upravlja se samo jednim ključem i nije bitno u kojem se smjeru obavlja transmisija. Od obje strane u procesu komunikacije, odnosno oba entiteta ili korisnika, se očekuje da imaju isti ključ. Ukoliko ključ nije isti, podaci enkriptovani prvim ključem, ne mogu biti dekriptovani drugim ključem, a isto važi i obrnuto.

A. Tipovi simetričnih kriptografskih algoritama

Simetrični kriptografski algoritmi se mogu podijeliti u dvije grupe, a to su stream algoritmi i block algoritmi. Block algoritmi enkriptuju čitave blokove podataka. Podaci se dijele u blokove fiksne dužine. Ako dužina podataka nije djeljiva sa dužinom bloka, posljednji blok se dopunjava do potrebne dužine. Stream algoritmi enkriptuju podatke bajt po bajt. Podaci se enkriptuju slovo po slovo bez referenci na neki drugi dio poruke. Blok algoritmi uobičajeno koriste blokove dužine 64b, odnosno 8 karaktera koji zauzimaju po jedan bajt.

IV. ASIMETRIČNA KRIPTOGRAFIJA

Nasuprot simetrične kriptografije koja koristi isti ključ i za enkripciju i za dekripciju, tu je asimetrična kriptografija koja koristi dva ključa. Ključevi koje ova vrsta kriptografije koristi su privatni i javni ključ. Zbog ove činjenice, asimetrična kriptografija se naziva i kriptografija javnog ključa. Ova dva ključa su matematički povezana, na način da šta jedan ključ radi, drugi ključ poništava, odnosno šta jedan ključ enkriptuje drugi može dekriptovati.

S obzirom na dva ključa, pojavljuje se problem razmjene ključeva između dva entiteta. Od dva ključa, jedan mora biti zaštićen, a to je privatni ključ. Drugi ključ, odnosno javni ključ, ne treba nikakvu zaštitu i može se bezbjedno razmijeniti. Javni ključ je i namijenjen da bude javan i dostupan, tako da jedini način na koji asimetrična kriptografija može raditi je da ljudi posjeduju javni ključ.

Asimetrična enkripcija koristi javni ključ za enkriptovanje poruka koje samo privatni ključ može dekriptovati. Prilikom razmjene enkriptovanih poruka, potrebno je razmijeniti i javne ključeve, što je sasvim uredu jer ne postoji problem pri njihovom slanju.

V. POREĐENJE SIMETRIČNE I ASIMETRIČNE KRIPTOGRAFIJE

Iako je nemoguće direktno porediti simetričnu i asimetričnu kriptografiju, ključevi koji se koriste kod asimetrične kriptografije su znatno veći. Ukoliko se napad oslanja na brute force metodu, bilo bi potrebno znatno više vremena za probijanje 1024 bitnog ključa, nego za probijanje 128b ključa [4], jednostavno jer postoji više kombinacija. Zašto onda uvijek ne koristimo asimetričnu enkripciju?

Pa, ključevi koji se koriste za asimetričnu kriptografiju jesu teži za probiti, ali ova vrsta kriptografije zahtjeva više resursa i nije naročito brza upravo zbog veličine ključa. Iako ovaj problem nije istih razmjera kao što je nekad bio, danas se koriste sve veći i veći ključevi koji traže sve više i više resursa. Druga stvar, postoje i dodatni troškovi kada je u pitanju asimetrična kriptografija. Ukoliko je želimo koristiti svugdje, svako bi morao imati ključ, što je vrlo nepraktično, što će biti objašnjeno kasnije infrastrukturom javnog ključa.

Dodatna vrijednost asimetrične kriptografije je to što privatni i javni ključ pripadaju isključivo jednom korisniku, odnosno entitetu. Ovaj princip se naziva neosporivost i ona onemogućuje pošiljaocu da kaže da nije poslao poruku ukoliko je poruka poslana koristeći njegov privatni ključ. Uz ovaj princip se koriste digitalni potpisi o kojima će biti više riječi u nastavku.

Za zaštitu podataka na mreži se koristi asimetrična kriptografija, odnosno kriptografija javnog ključa.

VI. ASIMETRIČNA KRIPTOGRAFIJA I INFRASTRUKTURA JAVNOG KLJUČA

Kriptografija asimetričnim, odnosno javnim ključem, koristi par ključeva, jedan javni koji je poznat svima i jedan privatni koji je poznat samo primatelju. Podatak enkriptovan javnim ključem se može dekriptovati samo odgovarajućim privatnim ključem primatelja, što znači da pošiljalac slobodno može objaviti javni ključ. Ova vrsta kriptografije treba da ispuni već spomenute zahtjeve autentifikacije, integriteta, povjerljivosti i neosporivosti.

Međutim, da bi se ovi zahtjevi mogli implementirati, infrastruktura koja njima upravlja mora biti dobro isplanirana. U klasičnoj, i najčešćoj, shemi enkripcije javni i privatni ključ, u najboljem slučaju, moraju biti kreirani, kontrolisani, podijeljeni, sačuvani i, na kraju, uništeni. Postoji više enkripcijskih framework-a koji mogu ispuniti navedene zahtjeve, a većina ih se bazira na infrastrukturi javnog ključa koja korisnicima omogućava da nesigurnim kanalima vrše sigurnu komunikaciju.

Infrastruktura javnog ključa tako predstavlja osnovu na kojoj su aplikacije i sistemi izgrađeni. Sistemi koji zahtijevaju korištenje sigurnosnih mehanizama zasnovanih na infrastrukturi javnog ključa uključuju email i internet bankarstvo. Bitno je razumjeti da infrastruktura javnog ključa sama po sebi ne predstavlja mehanizam za autentifikaciju, autorizaciju, privatnost i integritet, nego infrastrukturu koja pruža podršku ovim mehanizmima.

VII. ARHITEKTURA INFRASTRUKTURE JAVNOG KLJUČA

Fig. 1. Komponente sistema infrastrukture javnog ključa

Komponente infrastrukture javnog ključa su: korisnik, certifikator (CA), registrator (RA), baza opozvanih i valjanih certifikata i izdavač opozvanih certifikata. [5] Fig. 1. prikazuje komponente sistema infrastrukture javnog ključa i njihovu moguću komunikaciju, gdje su neobavezni putevi komunikacije prikazani svjetlijom

bojom. U nastavku će komponente infrastrukture javnog ključa biti detaljnije opisane.

A. Korisnik

Korisnik predstavlja subjekat certifikata i ne mora biti isključivo osoba. Korisnik, pored osobe, može biti uređaj, program ili proces, odnosno sve što se može identifikovati imenom na certifikatu.

B. Certifikator (Certification Authirity – CA)

Certifikator, odnosno CA, element predstavlja treće lice koje kada označi korisnika validnim, može mu se vjerovati, sa relativnom pouzdanošću. Njegova uloga je generisanje, izdavanje i opoziv digitalnih certifikata koji se koriste za verifikaciju identiteta. [6] Certifikator direktno, ili preko registratora (RA) registruje korisnike i verifikuje njihov identitet. Certifikator također vodi računa o svim certifikatima unutar sistema i brine se o listi opozvanih certifikata koja se koristi za evidenciju certifikata koji imaju problem ili su povučeni. Dodatno, certifikator može obavljati i sigurnu pohranu ključeva. Dakle, certifikator predstavlja izvor povjerenja, koje se smatra osnovom infrastrukture javnog ključa.

S obzirom da certifikator obezbjeđuje certifikat i javni ključ, korisnik može biti siguran da određeni javni ključ pripada primaocu kojem je poruka namijenjena. Certifikator također olakšava distribuciju ključeva jer korisnik može od njega tražiti ključ koji mu je potreban. S obzirom da digitalni potpis certifikatora validira čitav sistem, njegova zaštita je visokoprioritetna.

U mnogim sistemima infrastrukture privatnog ključa, postoji i vanjski entitet koji se zove validator, odnosno Validation Authority – VA, čija je uloga validacija certifikata. [7]

C. Registrator (Registration Authority – RA)

Registrator, odnosno RA, element je opcionalna komponenta sistema infrastrukture javnih ključeva. Rregistrator predstavlja svojevrstan interfejs između korisnika i CA. Njegova uloga je validacija identifikacije korisnika. [8] Registrator može provjeravati da li korisnikov privatni ključ odgovara javnom ključu koji će se nalaziti na certifikatu, ili sam može generisati ključeve. Također, može predstavljati posrednika između certifikatora i korisnika prilikom dohvatanja informacija o kompromitovanju privatnog ključa.

U sistemima koji nemaju registratora, koji se još naziva i sporedni certifikator, sve gore navedene funkcije obavlja certifikator. U sistemu također može da postoji i nekoliko registratora.

S obzirom da se registrator također smatra korisnikom sistema infrastrukture javnog ključa, on ima svoj javni ključ i certifikat. Funkcija koju registrator ne smije obavljati je izdavanje i opoziv izdatih certifikata.

D. Baza opozvanih i valjanih certifikata

Baza, odnosno spremište, certifikata predstavlja sistem ili skup distribuisanih sistema koji čuvaju certifikate, kao i listu opozvanih certifikata. Certifikati koji se čuvaju su dostupni korisnicima infrastrukture privatnog ključa koji za identifikaciju koriste certifikate.

E. Izdavač opozvanih certifikata

Izdavač opozvanih certifikata predstavlja komponentu sistema koja izdaje listu opozvanih certifikata. Iako se certifikati izdaju sa određenim periodom važenja, postoje mnogobrojni razlozi zašto certifikat može postati nevažeći i prije isteka. Jedan od primjera je kompromitacija privatnog ključa. Svaki opozvani certifikat se identifikuje serijskim brojem. Lista sa opozvanim certifikatima je svima javno dostupna.

VIII. NAČIN RADA INFRASTRUKTURE JAVNOG KLJUČA

Infrastruktura javnog ključa u suštini predstavlja strukturu dizajniranu da verifikuje i autentifikuje identitet korisnika, bili oni osobe, kompanije ili bilo koja druga vrsta korisnika. Nisu svi sistemi infrastrukture javnog ključa isti, ali na Fig. 2. je prikazan pojednostavljeni način rada sistema, a u nastavku će on biti opisan.

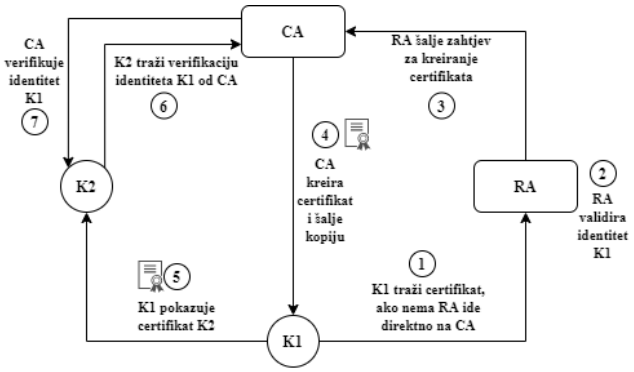

Fig. 2. Način rada infrastrukture javnog ključa

Koraci rada sistema infrastrukture javnog ključa:

1. U prvom koraku, novi korisnik, predstavljen oznakom K1, od registratora, predstavljenog znakom RA, traži certifikat. Ukoliko u sistemu ne postoji registrator, korisnik direktno od certifikatora, koji je predstavljen oznakom CA, traži certifikat.

2. Ukoliko u sistemu postoji registrator, on u drugom koraku validira identitet korisnika koji je tražio certifikat. Ukoliko registrator ne postoji, ovaj korak će izvršiti sam certifikator.

3. Nakon validacije identiteta, registrator šalje zahtjev za kreiranje certifikata certifikatoru. Ukoliko registrator ne postoji u sistemu, ni ovaj korak naravno ne postoji.

4. U četvrtom koraku, certifikator generiše i izdaje certifikat korisniku koji ga je tražio.

5. Nakon što je dobio traženi certifikat, korisnik može komunicirati sa drugim korisnicima u sistemu. Prvi korak pri komunikaciji je predstavljanje, kao i pokazivanje certifikata.

6. Po razmjeni certifikata, drugi korisnik, odnosno korisnik primatelj, na slici predstavljen sa K2, može od certifikatora tražiti provjeru identiteta korisnika pošiljaoca, odnosno prvog korisnika.

7. Nakon što certifikator izvrši traženu validaciju identiteta, on drugom korisniku šalje izvještaj, odnosno saopštava da li je identitet prvog korisnika validan. Poslije ovoga, korisnici mogu nastaviti komunicirati.

IX. MODEL POVJERENJA

Dodatni termin povezan sa infrastrukturom javnog ključa je i model povjerenja. Model povjerenja opisuje kako entiteti unutar organizacije koriste ključeve, digitalne potpise i digitalne certifikate. [9] Postoje tri osnovna modela, a to su mreža povjerenja, sistem jedinstvenog autoriteta i hijerarhijski sistem povjerenja.

U prvom modelu nekoliko entiteta potpisuje certifikate međusobno. Pojednostavljeno, korisnici iz sistema vjeruju jedni drugima na osnovu certifikata koje primaju od drugih korisnika istog sistema.

Druga dva modela imaju razvijeniju strukturu. Sistem jedinstvenog autoriteta ima nadređenog certifikatora koji kreira i uručuje certifikate, a korisnici vjeruju jedni drugima na osnovu njega. Posljednji sistem također ima certifikatora na vrhu, koji jepoznat kao korijenski certifikator, ali ima više registratora na hijerarhijski nižem nivou koji uručuju certifikate i upravljaju njima. Ovaj sistem se predstavlja kao najsigurniji.

X. DIGITALNI POTPIS

Korištenje digitalnog potpisa je omogućeno prilikom upotrebe asimetrične kriptografije, te je na taj način omogućeno i rješavanje problema integriteta. Ovaj potpis, analogno pravom potpisu, može kreirati samo jedna osoba, ali ga mnogo drugih može pročitati. Digitalni potpis koristi koncept para ključeva. S obzirom da se ključevi kreiraju tako da jedan poništava šta je drugi uradio, digitalni potpis koristi činjenicu da je podatke moguće enkriptovati privatnim, a dekriptovati javnim ključem.

Mora postojati privatni ključ, poznat samo pošiljaocu, tako da su potpisani podaci eksplicitno vezani za pošiljaoca. Također, mora postojati i javni ključ, dostupan široj grupi osoba, tako da potpis može biti provjeren i povezan sa pošiljaocem. Na ovaj način digitalni potpis omogućava autentifikaciju i neosporivost. Umjesto da se enkriptuje sama poruka, enkriptuje se njen hash. Dakle, poruka koja se šalje ima proizvoljnu dužinu, a za njeno hashiranje se koristi kriptografska one-way hash funkcija.

One-way hash funkcija mapira ulaz proizvoljne dužine u izlaz određene dužine, a skoro je nemoguće da dva ulaza proizvedu isti izlaz. Zatim se hash enkriptuje privatnim ključem pošiljaoca i tako pretvara u digitalni potpis koji se zajedno sa originalnom porukom šalje primaocu. Kada primalac dobije poruku on je dekriptuje javnim ključem i tako dobija hash vrijednost. Također, s obzirom da je hash funkcija javna, primalac originalnu poruku hashira i provjerava jednakost dva dobivena hasha. Ukoliko su oni jednaki, to predstavlja integritet, odnosno postoji dokaz da poruka nije mijenjana. [10]

Autentifikacija, odnosno utvrđivanje identiteta pošiljaoca, zahtjeva provjeru da li javni ključ stvarno pripada osobi za koju pošiljatelj tvrdi da jeste, što se može utvrditi na osnovu digitalnog certifikata.

XI. DIGITALNI CERTIFIKAT

Za rješavanje problema autentifikacije se koristi digitalni certifikat. On predstavlja dokument za identifikaciju korisnika i njegovo povezivanje sa javnim ključem. [11]

Certifikati prate X.509 standard koji se koristi globalno. Ovaj standard, koji je dio velike porodice standarda definiše šta treba i ne treba biti u digitalnom certifikatu. Zbog njega, svaki sistem koji je saglasan sa ovim standardom može razmjenjivati i koristiti certifikate za autentifikaciju.

Metode koje se koriste za dokazivanje identiteta variraju. Ovlaštena služba, odnosno Cartification Authority – CA ili certifikator, koristi svoju objavljenu proceduru za verifikaciju za određeni tip certifikata. Izdati certifikat povezuje javni ključ sa imenom korisnika. Samo javni ključ potvrđen certifikatom radi sa tajnim ključem koji posjeduje osoba identifikovana certifikatom.

Certifikat, pored imena i javnog ključa, sadrži period važenja, verziju, serijski broj, ID algoritma koji je korišten za kreiranje digitalnog potpisa, ime službe koja ga je izdala, namjenu i dodatna opcionalna polja. Ono što je najvažnije, certifikat uvijek sadrži digitalni potpis službe koja ga je izdala i na taj način dozvoljava certifikatu da radi kao potvrda korisnicima koji vjeruju službi, ali ne znaju osoba koja se certifikatom predstavlja.

Na slikama koje slijede u nastavku je prikazan jedan primjer digitalnog certifikata. Na Fig. 3. se mogu vidjeti opće informacije o certifikatu, kao što su namjena, period važenja, ime službe koja ga je izdala i kome je izdat. Fig. 4. prikazuje detaljne informacije o certifikatu sa svim gore navedenim poljima. I na posljednjoj, Fig. 5. vidimo certifikacijsku putanju za posmatrani certifikat.

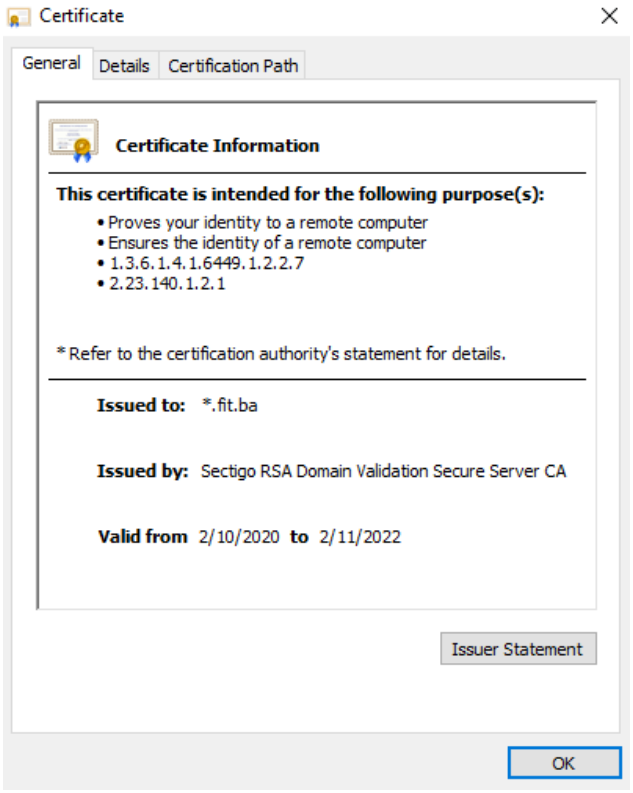

Fig. 3. Opće informacije o digitalnom certifikatu

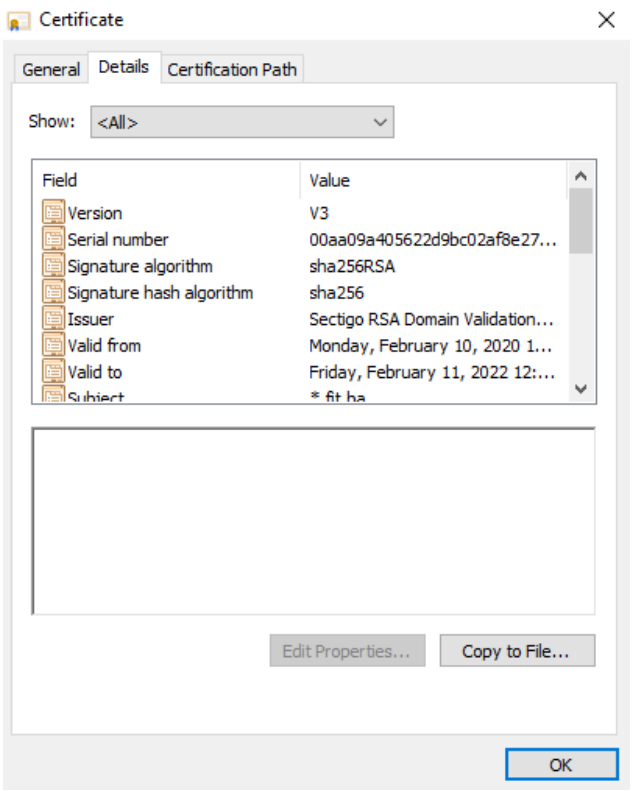

Fig. 4. Detaljne informacije o digitalnom certifikatu sa prikazom polja

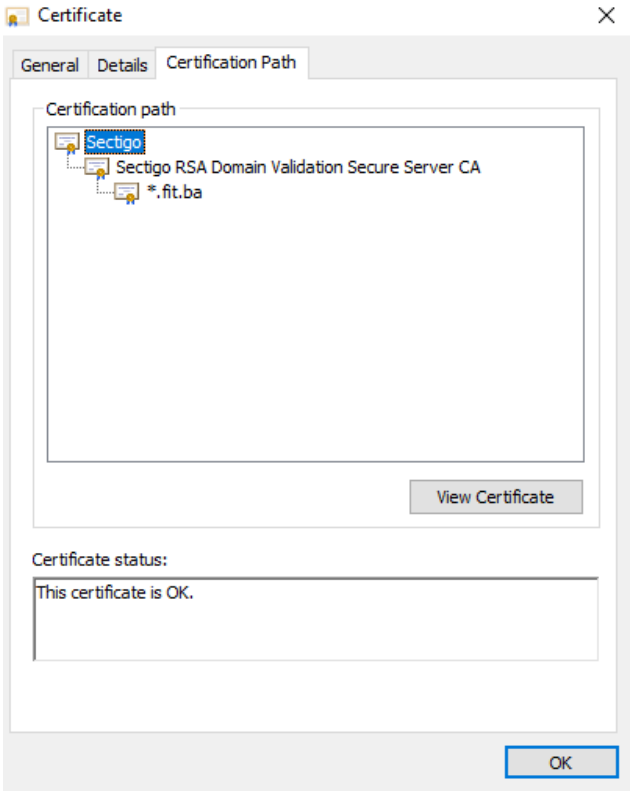

Fig. 5. Certifikacijska putanja digitalnog certifikata

XII. UPOTREBA INFRASTRUKTURE JAVNOG KLJUČA

Infrastruktura javnog ključa ima širok raspon upotrebe, ali njen dizajn uveliko zavisi od potreba. Infrastruktura javnog ključa se najčešće koristi pri Wi-Fi autentifikaciji, autentifikaciji na web aplikacijama, email sigurnosti i VPN autentifikaciji. Ispod će biti prikazano na koji način je svaka navedena stavka povezana sa infrastrukturom javnog ključa.

A. Wi-Fi autentifikacija

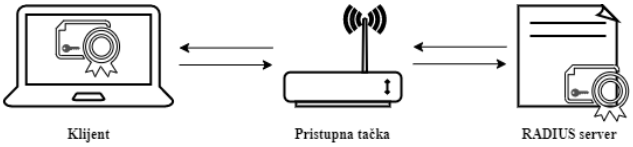

Fig. 6. WiFi autentifikacija koristeći infrastrukturu javnog ključa

Korisnici koji imaju certifikat potpisan od strane povjerljivog certifikatora se mogu povezati na bezbjedan SSID i biti autentifikovani od strane RADIUS-a koristeći EAP-TLS. EAP-TLS autentifikacija vrši autentifikaciju baziranu na certifikatu i uzajamnu autentifikaciju za klijenta i mrežu. [12] Dalje se certifikat se šalje i RADIUS potvrđuje identitet, uspostavljajući tako povjerenje koje garantuje siguran pristup mreži. RADIUS (eng. Remote Authenitcation Dial in User Service) predstavlja mrežni protokol koji omogućava centralizovano upravljanje autentifikacijom, autorizacijom i administracijom korisnika prilikom spajanja na mrežu i korištenja njenih usluga. [13]

B. Autentifikacija na web aplikacijama

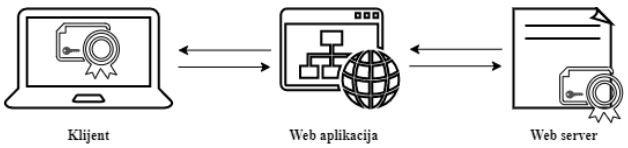

Fig. 7. Autentifikacija na web aplikacijama koristeći infrastrukturu javnog ključa

Slično kao i kod wi-fi autentifikacije, identitet korisnika koji se spaja na web aplikaciju će biti potvrđen od strane web servera na osnovu certifikata. S obzirom da je certifikat potpisan od strane certifikatora kojem se vjeruje, korisnik dobija pravo pristupa web aplikaciji.

C. Email sigurnost

Enkripcija emailova sa certifikatima primjenjuje S/MIME protokol. I pošiljalac i primatelj su obavezni da imaju certifikate, koji su potpisani od strane certifikatora kojem se vjeruje, da bi se ostvarila sigurna konekcija između korisnika. S/MIME protokol je baziran na asimetričnoj kriptografiji i predstavlja protokol koji ima za zadatak da zaštiti emailove od neželjenog pristupa. Drugi zadatak ovog protokola je identifikacija pošiljaoca poruke na osnovu njegovog digitalnog potpisa, a treći je autentifikacija primateljevog certifikata kako bi se poruka dešifrovala. Drugi zadatak ovaj protokol čini vrlo efikasnom zaštitom od phishing napada. [14]

D. VPN autentifikacija

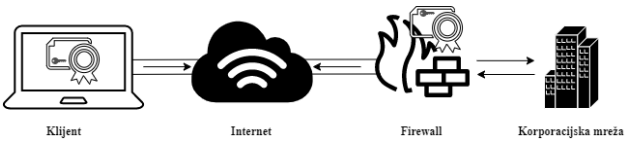

Fig. 8. VPN autentifikacija koristeći infrastrukturu javnog ključa

Certifikati se mogu koristiti i za autentifikaciju korisnika kako bi dobili VPN pristup. S obzirom da VPN može omogućiti pristup osjetljivim informacijama, metodi autentifikacije certifikatima se daje prednost ispred autentifikacija šifrom. Inače se na VPN-u čuva korijenski certifkator. Nakon završetka autentifikacije korisnika, između mreže i korisnika se kreira tunel koji obezbjeđuje sigurnost.

XIII. ZAKLJUČAK

Dakle, infrastruktura javnog ključa predstavlja sistem za omogućavanje sigurne komunikacije nesigurnim putevima, pri tome koristeći asimetričnu kriptografiju. Osnovnim alatima infrastrukture javnog ključa se mogu smatrati digitalni potpis i digitalni certifikat. Digitalni potpis služi kako bi komunikacija imala osobinu neosporivosti, odnosno da pošiljalac ne može tvrditi da on nije autor poruke. Dodatna mogućnost digitalnog potpisa je osiguravanje integriteta, gdje postoji mogućnost provjere da li je poruka primaocu stigla u izvornom obliku, odnosno tačno onako kako je poslana. Digitalni certifikat se koristi da bi se postigla osobina autorizacije, odnosno za provjeru identiteta korisnika, jer povezuje korisnika sa njegovim ključem. Kada su u pitanju oblasti koji trebaju sigurnu autentifikaciju, infrastruktura javnog ključa definitivno dolazi kao odlično rješenje. Iz tog razloga, struktura javnog ključa ima širok opseg upotrebe u današnjem svijetu, od finansijskog sektora pa sve do zdravstvenog.

[1] Book.itep.ru. 2013. History Of Cryptography. [online] Available at: <http://book.itep.ru/depository/crypto/Cryptography_history.pdf> [Accessed 26 December 2020].

[2] Kothari, J., 2020. Cryptography And Its Types. [online] GeeksforGeeks. Available at: <https://www.geeksforgeeks.org/cryptography-and-its-types/> [Accessed 26 December 2020].

[3] OpenLearn. n.d. Plaintext And Ciphertext. [online] Available at: <https://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=48322&section=1.1> [Accessed 27 December 2020].
[4] Stubbs, R., 2018. Classification Of Cryptographic Keys. [online] Cryptomathic.com. Available at: <https://www.cryptomathic.com/news-events/blog/classification-of-cryptographic-keys-functions-and-properties> [Accessed 26 December 2020].
[5] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R. and Polk, W., 2008. RFC 5280 - Internet X.509 Public Key Infrastructure Certificate And Certificate Revocation List (CRL) Profile. [online] Tools.ietf.org. Available at: <https://tools.ietf.org/html/rfc5280> [Accessed 26 December 2020].
[6] Support.dnsimple.com. n.d. What Is A Certificate Authority?. [online] Available at: <https://support.dnsimple.com/articles/what-is-certificate-authority/> [Accessed 26 December 2020].
[7] PrimeKey. n.d. What Is A Validation Authority?. [online] Available at: <https://www.primekey.com/wiki/what-is-a-validation-authority/> [Accessed 26 December 2020].
[8] Network Encyclopedia. n.d. Registration Authority. [online] Available at: <https://networkencyclopedia.com/registration-authority-ra/> [Accessed 26 December 2020].
[9] Jøsang, A., 2013. Theory And Practice Of Cryptography Solutions For Secure Information Systems. Hershey, Pa.: IGI Global
[10] Adams, C. and Lloyd, S., 1999. Understanding Public-Key Infrastructure. Indianapolis, IN: New Riders.
[11] Spvp.zesoi.fer.hr. 2002. Infrastruktura Javnog Kljuca. [online] Available at: <http://spvp.zesoi.fer.hr/seminari/2002/pki/PublicKeyInfrastructure.htm> [Accessed 24 December 2020].
[12] Cis.hr. n.d. Sigurnosni Elementi RADIUS Protokola. [online] Available at: <https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-07-306.pdf> [Accessed 26 December 2020].
[13] Intel. 2020. 802.1X Overview And EAP Types. [online] Available at: <https://www.intel.com/content/www/us/en/support/articles/000006999/network-and-i-o/wireless.html> [Accessed 26 December 2020].
[14] Publico, R., 2017. What Is S/MIME And How Does It Work?. [online] GlobalSign GMO Internet, Inc. Available at: <https://www.globalsign.com/en/blog/what-is-s-mime> [Accessed 26 December 2020].