Sigurnosni aspekti infrastrukture javnog ključa na arhitekturi Microsoft Windows

Mlinar, Antun

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

SIGURNOSNI ASPEKTI INFRASTRUKTURE JAVNOG KLJUČA NA ARHITEKTURI MICROSOFT WINDOWS

SECURITY ASPECTS OF PUBLIC KEY INFRASTRUCTURE ON MICROSOFT WINDOWS ARCHITECTURE

Mentor: doc. dr. sc. Ivan Cvitić

Student: Antun Mlinar

JMBAG: 0135245503

Zagreb, Rujan 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 19. travnja 2024.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Sigurnost i zaštita informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 7669

Pristupnik: **Antun Mlinar (0135245503)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Sigurnosni aspekti infrastrukture javnog ključa na arhitekturi Microsoft Windows**

Opis zadatka:

U okviru diplomskog rada potrebno je analizirati aktualnu znanstveno-stručnu literaturu u području sigurnosti infrastrukture javnog ključa te pružiti pregled mogućnosti primjene takve infrastrukture. Potrebno je u testnom okruženje implementirati infrastrukturu javnog ključa te u takvom okruženju istražiti sigurnosne nedostatke i ranjivosti. Prikupljenje podatke potrebno je analizirati i izvući zaključke te pružiti pregled budućih trendova razvoja infrastrukture javnog ključa.

Mentor:

doc. dr. sc. Ivan Cvitić

Predsjednik povjerenstva za diplomski ispit:

SIGURNOSNI ASPEKTI INFRASTRUKTURE JAVNOG KLJUČA NA ARHITEKTURI MICROSOFT WINDOWS

SAŽETAK

Sigurnosni aspekti infrastrukture javnog ključa na arhitekturi *Microsoft Windows* predstavljaju ključni element u osiguravanju povjerljivosti, integriteta i autentičnosti digitalnih podataka u modernim informacijskim sustavima. Kroz rad analizirani su različiti aspekti PKI-a, počevši od temeljnih koncepata i pregleda dosadašnjih istraživanja, preko praktične primjene i tehničke implementacije, do istraživanja sigurnosnih izazova i budućih trendova razvoja PKI-a. Kroz detaljnu analizu sigurnosnih aspekata PKI-a, ovaj rad pokazao je da unatoč visokoj razini sigurnosti, postoje specifične ranjivosti koje zahtijevaju pažljivo upravljanje i stalno praćenje. Rad nudi sveobuhvatan pregled sigurnosnih aspekata PKI-a i pruža smjernice za uspješnu primjenu i zaštitu u *Microsoft Windows* okruženju.

KLJUČNE RIJEČI: Infrastruktura javnog ključa, certifikati, certificirajući predlošci, ADCS napadi

SECURITY ASPECTS OF PUBLIC KEY INFRASTRUCTURE ON MICROSOFT WINDOWS ARCHITECTURE

SUMMARY

The security aspects of the public key infrastructure on the *Microsoft Windows* architecture represent a key element in ensuring the confidentiality, integrity and authenticity of digital data in modern information systems. Through the paper, various aspects of PKI were analyzed, starting from the basic concepts and overview of previous research, through practical application and technical implementation, to the research of security challenges and future trends of PKI development. Through a detailed analysis of the security aspects of PKI, this paper has shown that despite the high level of security, there are specific vulnerabilities that require careful management and constant monitoring. The paper offers a comprehensive overview of the security aspects of PKI and provides guidance for successful implementation and protection in a *Microsoft Windows* environment.

KEYWORDS: Public Key Infrastructure, Certificates, Certificate Templates, ADCS attacks

Sadržaj

1. Uvod

U današnjem digitalnom dobu, sigurnost informacija postala je ključna komponenta u osiguravanju privatnosti i integriteta podataka. Jedan od temeljnih mehanizama za postizanje ove sigurnosti je infrastruktura javnog ključa (engl. *Public Key Infrastructure* - PKI). Ona omogućuje sigurno upravljanje digitalnim certifikatima i kriptografskim ključevima, pružajući osnovu za autentifikaciju, enkripciju i digitalne potpise. Posebno je važna u okruženju operacijskih sustava kao što je *Microsoft Windows*, koji se široko koristi u poslovnim i privatnim okruženjima diljem svijeta.

Arhitektura *Microsoft Windows* nudi integrirane alate i servise za implementaciju PKI-a, kao što su AD CS (engl. *Active Directory Certificate Services*), koji omogućuju korisnicima izdavanje i upravljanje digitalnim certifikatima unutar mreže organizacije. Međutim, implementacija PKI-a na ovoj platformi sa sobom nosi niz sigurnosnih izazova. Upravljanje ključevima, zaštita certifikata, autentifikacija korisnika, te sigurnosne politike su samo neki od aspekata koji zahtijevaju pažljivo planiranje i provedbu.

Ovaj rad istražuje sigurnosne aspekte infrastrukture javnog ključa na arhitekturi *Microsoft Windows*, s posebnim fokusom na najbolje prakse, izazove i rješenja koja omogućuju visoku razinu sigurnosti u poslovnim okruženjima. Analizirat će se različiti sigurnosni mehanizmi, pristupi i propusti u upravljanju certifikatima, te utjecaj sigurnosnih politika na cjelokupnu arhitekturu sustava. Cilj rada je pružiti sveobuhvatan pregled sigurnosnih aspekata infrastrukture javnog ključa na *Microsoft Windows* operativnom sustavu, te ponuditi smjernice za implementaciju sigurnih i pouzdanih PKI sustava.

Diplomski rad sastoji se od sedam poglavlja:

1. Uvod
2. Pregled dosadašnjih istraživanja
3. Primjena infrastrukture javnog ključa
4. Implementacija infrastrukture javnog ključa
5. Istraživanje sigurnosnih izazova
6. Budući trendovi razvoja infrastrukture javnog ključa
7. Zaključak

Unutar drugog poglavlja obuhvaćen je pregled relevantnih istraživanja i literature na području infrastrukture javnog ključa. Analiziraju se postojeća rješenja, metode i tehnike koje su korištene u dosadašnjim istraživanjima, te se identificiraju ključni problemi i izazovi u području sigurnosti PKI-a.

U trećem poglavlju detaljno se opisuje primjena PKI-a u različitim kontekstima i scenarijima. Prikazuju se praktični primjeri i studije slučaja koje ilustriraju kako PKI može unaprijediti sigurnost i efikasnost u poslovnim okruženjima. Također se razmatraju specifične industrijske potrebe i zahtjevi, te kako PKI može zadovoljiti te zahtjeve.

Četvrto poglavlje se fokusira na tehničke aspekte implementacije PKI-a na *Microsoft Windows* operativnom sustavu. Objašnjavaju se koraci i postupci potrebni za uspostavu PKI-a, uključujući konfiguraciju AD CS-a i upravljanje certifikatima. Osim toga, opisuju se mrežne karakteristike potrebne kako bi PKI uredno ispunjavao svoje mogućnosti unutar domene.

U petom poglavlju su provedena dva napada nad ranjivim predlošcima unutar PKI-a. Paralelno s probojima, poglavlje analizira sigurnosne izazove povezane s implementacijom i upravljanjem PKI-om.

U šestom poglavlju rada istražuju se budući trendovi i inovacije u području PKI-a. Analiziraju se najnovija tehnološka dostignuća i predviđanja o tome kako će se PKI razvijati u narednim godinama, uključujući utjecaj novih sigurnosnih standarda i tehnologija. Razmatra se potencijal umjetne inteligencije i strojnog učenja u unapređenju PKI-a, te kombinacija *blockchain* tehnologije i PKI-a kako bi se postigli uvjeti koji će zadovoljiti buduće zahtjeve infrastrukture javnog ključa.

2. Pregled dosadašnjih istraživanja

Sukladno brojnim ranjivostima i načinima probijanja napadača u infrastrukturu razvija se rješenje infrastrukture javnog ključa (engl. *Public Key Infrastructure* - PKI) koja je zaživjela široku primjenu u brojnim tvrtkama diljem svijeta. Prateći ubrzan razvoj tehnologije, PKI je svoju svrhu pronašao u sferi sigurnosti sustava. Istraživanja navedena ispod teksta ujedinjuju različite metode instalacije sustava i kreativne ideje kako bi se PKI sustav mogao unaprijediti, te smanjiti rizik neovlaštenih radnji vezanih za autentifikaciju i autorizaciju osoba i aplikacija putem Interneta. Također, radovi ispod sadrže detaljno razrađen postupak razvijanja takvog sustava na *Microsoft Windows* arhitekturi.

Prema radu [1] iz 2007. razmatraju se sigurni i učinkoviti načini šifriranja javnim ključem, te sheme potpisa koristeći infrastrukturu javnog ključa. Za razliku od tradicionalnih analiza koje istraživanja temelje na pretpostavci idealnog okruženja, u ovom radu je realniji pristup na način da su autori pretpostavili kako sustav ima propuste i ranjivosti. Analiza koju autori provode pojašnjava i potvrđuje nekoliko ključnih aspekata kao što su stupanj povjerenja u certificirajuća tijela, potreba i specifičnosti dokaza o posjedovanju tajnih ključeva, te sigurnost osnovnih značajki infrastrukture javnog ključa u ovom složenom okruženju. Također se definiraju konstrukcije za šifriranje i sheme potpisa koje zadovoljavaju snažne sigurnosne definicije efikasnije od tradicionalnih konstrukcija koje pretpostavljaju da se digitalni certifikat izdan od strane certificirajućeg tijela mora provjeravati svaki put kad se koristi javni ključ, [1].

Osim toga, knjiga se usredotočuje na dizajn i standardizaciju PKI-ja, posebno u kontekstu projekta standardizacije ANSI X9.109. Autori pružaju smjernice za poboljšanje dizajna PKI-ja i definiraju važne aspekte koji trebaju biti uzeti u obzir prilikom implementacije PKI-ja u stvarnom okruženju, [1].

Sveukupno, knjiga *A Closer Look at PKI: Security and Efficiency* je temeljita i sveobuhvatna knjiga koja pruža dublje razumijevanje sigurnosnih aspekata infrastruktura javnog ključa. Njezini rezultati istraživanja, analize i konstrukcije imaju važne implikacije za praksu dizajna, implementacije i standardizacije PKI-ja, te mogu pružiti smjernice za poboljšanje sigurnosti i učinkovitosti ovih kritičnih sustava, [1].

Članak [2] napisan 2001. godine pruža uvide u infrastrukture javnih ključeva i njihovu povijest, izazove i implementacije. Svako se poglavlje usredotočuje na specifične aspekte PKI-ja, a zajedno čine sveobuhvatan pregled teme. Članak govori o ulozi PKI-ja kao usluge, a ne kao tehnologije, ističući njegovu važnost kao komponentne infrastrukture. Točno naglašava da sama kriptografska tehnologija nije najkritičniji aspekt PKI-ja, već prije hijerarhija povjerenja i sposobnost vezanja identiteta na javne ključeve. Članak daje jasno objašnjenje skalabilnosti PKI-ja i njegovog značaja u pružanju sigurnosnih rješenja za različite slojeve povezivanja. Također daje kratku povijest PKI-ja, ocrtavajući izazov povezivanja identiteta s javnim ključevima. Predstavlja koncept certifikacijskih tijela (engl. *Certificate Authority* - CA) i digitalnih certifikata, nudeći vrijedan kontekst za razvoj PKI-a. Također rad zadire u specifična problematična područja s

trenutnim infrastrukturama javnog ključa, posebno u vezi s *web* preglednicima i njihovom implementacijom sigurnosnih rješenja što će se dodatno spominjati kasnije u radu. U članku se pobliže objasnio povijesni kontekst koji naglašava razvoj tehnologije SSL (engl. *Secure Sockets Layer*). Tekst pojašnjava izazove s kojima se certifikacijska tijela suočavaju u podržavanju različitih ponašanja internet preglednika, [2].

Članak istražuje različite aspekte infrastrukture javnih ključeva, posebno se fokusirajući na sučelja za provjeru valjanosti i protokole koji se koriste za provjeru statusa certifikata. U tekstu se govori o izazovima povezanim s listama opozvanih certifikata (engl. *Certificate revocation list* - CRL) i predstavlja alternativna rješenja kao što su OCSP (engl. *Online Certificate Status Protocol*) i SCVP (engl. *Simple Certificate Validation Protocol)*. Također predlaže bolja rješenja za budućnost, kao što je centralizirano upravljanje politikama i uloga posrednika za provjeru valjanosti preko više certifikacijskih tijela, [2].

Članak [3] pruža sveobuhvatan pregled infrastrukture javnih ključeva i njezinog značaja u osiguravanju sigurnosti, autentifikacije, integriteta podataka i neporicanja za digitalne komunikacije i transakcije. Razmatra se korištenje digitalnih certifikata, uloge tijela za izdavanje certifikata i važnost poslovnog PKI-ja u zaštiti informacijske imovine. Tekst je kvalitetno strukturiran, predstavlja informacije logičnim redoslijedom s jasnim naslovima za svaki odjeljak. Osim toga, članak objašnjava tehnologiju digitalnog potpisa, njezino oslanjanje na kriptografiju s javnim ključem i njezine primjene za osiguranje integriteta podataka. Jasno je objašnjena razlika između javnih i privatnih ključeva, ističući važnost kontrole privatnih ključeva za sigurne transakcije, [3].

Sveukupno, ovaj članak nudi zaokruženo razumijevanje infrastrukture javnog ključa i njegovih praktičnih implikacija u osiguranju digitalnih komunikacija, osiguravanju autentičnosti podataka i pojednostavljenju procesa rada. Ističe prednosti sigurnih elektroničkih potpisa u zamjenu za tradicionalna odobrenja temeljenih na papiru, što dovodi do povećane učinkovitosti i smanjenih troškova. Članak također komentira izazove i razmatranja koja su uključena u implementaciju PKI-ja, pružajući vrijedne uvide organizacijama koje žele usvojiti ovu tehnologiju za poboljšanu sigurnost i pouzdanost, [3].

U radu [4] je opisan rizik od krivotvorenja certifikata zbog nedostatka sigurnosnih rješenja za održavanje infrastrukture javnog ključa. Svrha istraživanja je unaprjeđenje digitalnog potpisa i korištenje QR koda (engl. *Quick Response code*) čime bi se mogućnost preslikavanja certifikata minimizirala. Razvoj napadačkih tehnika uvodi nove prijetnje u servise izdavanja certifikata što bi se korištenjem aplikacije osmišljene u ovom radu značajno smanjilo. Rad je podijeljen u dvije osnovne kategorije, a to su kreacija e-certifikata i verifikacija istog putem QR koda, [4].

Članak istražuje problem validiranja stručnih certifikata, tj. zapisa o priznavanju koje su pojedinci stekli nakon položenih ispita u specifičnim područjima studija. Certifikati su vjerodajnice važne za stručnjake jer ukazuju na njihovo znanje, sposobnosti i stav u skladu s industrijskim standardima, čineći ih konkurentnijima na tržištu rada, kvalificiranima za bolje plaće

poboljšavajući njihove izglede za karijeru. Problematika validacije stručnih certifikata rezultirala je porastom lažnih operacija korištenjem lažnih certifikata. Kriminalci su uključeni u izradu i distribuciju lažnih certifikata, ugrožavajući legitimnost i autentičnost ispravnih certifikata, [4].

Cilj istraživanja je izraditi aplikaciju pod nazivom *creatcate* koja objavljuje sigurne e-certifikate, a istovremeno smanjuje krivotvorenje i umnožavanje. Integracija digitalnih potpisa i QR kodova poboljšava sigurnost i autentičnost certifikata, čineći postupak verifikacije lakšim za korisnike. Predloženo rješenje ima za cilj minimizirati izradu certifikata, eliminirati dupliciranje certifikata i poboljšati ukupnu sigurnost procesa certificiranja spajanjem digitalnih potpisa s QR kodovima. Ovo istraživanje posebno je istaknuto i uključeno zbog svoje značajne novine, a to je da se prvi put razmatra uvođenje QR koda kao inovativnog načina za provjeru autentičnosti certifikata. Ovaj pristup predstavlja potencijalno revolucionarnu metodu validacije koja bi mogla unaprijediti sigurnost infrastrukture javnog ključa i olakšati provjeru važnih dokumenata, [4].

3. Primjena infrastrukture javnog ključa

Infrastruktura javnog ključa je skup tehnologija kojim se omogućuje sigurna razmjena informacija putem mreže. PKI se temelji na korištenju javnog i privatnog ključa koji se prilikom izrade stvaraju u paru. Javni ključ kriptografskog para je dostupan svima i koristi se za šifriranje podataka ili verifikaciju digitalnog potpisa, dok je privatni ključ tajni ključ poznat samo vlasniku, te se koristi za dešifriranje podataka ili kreaciju digitalnog potpisa. PKI infrastruktura služi za generiranje, distribuciju, upravljanje i povlačenje javnih ključeva, kao i za verifikaciju identiteta korisnika, [5].

3.1. Digitalni potpis

Korištenje infrastrukture javnog ključa za digitalno potpisivanje je jedna od ključnih primjena PKI tehnologije. Digitalno potpisivanje omogućuje pouzdano i cjelovito korištenje elektronskih dokumenata, poruka ili transakcija. Prednosti korištenja infrastrukture javnog ključa za digitalno potpisivanje uključuje, [5]:

- Autentifikaciju - potpis na dokumentu potiče od ispravnog izvora,
- Pouzdanost - dokument je potpisan od strane certificirajućeg tijela koji je priznat kao službeno javno certificirajuće tijelo,
- Integritet - dokument nije mijenjan nakon potpisa,
- Neporecivost – digitalni potpis ne može biti promijenjen ili obrisan bez traga.

FINA je digitalni potpis definirala kao potvrdu u elektroničkom obliku koja predstavlja elektronički identitet u elektroničkim transakcijama koji omogućuje sigurnu i povjerljivu komunikaciju internetom te dokazuje autentičnost primljene informacije. Također, FINA je certifikate podijelila po namjeni, a to su idući, [6]:

- Kvalificirani certifikati za elektronički potpis,
- Certifikati za autentikaciju,
- Certifikati za elektronički pečat,
- Certifikati za aplikacije.

Zahtjevi koji se postavljaju pred digitalni potpis mogu se formulirati na temelju razmatranja svojstava potencijalnih aktualnih prijetnji i slabosti. Neki od zahtjeva digitalnog potpisa su, [7]:

- Digitalni potpis mora biti oblikovan kao niz bitova koji se temelji na poruci koja se potpisuje,
- Za potpisivanje se moraju koristiti podaci koji su poznati samo pošiljatelju, kako bi se spriječilo krivotvorenje i poricanje,
- Digitalni potpis mora biti relativno jednostavan za generiranje,
- Potpis mora biti lako prepoznatljiv i provjerljiv na jednostavan način,

- Stvaranje ili manipulacija digitalnim potpisom mora biti računalno neizvediva, bilo putem konstruiranja nove poruke koja odgovara postojećem potpisu ili stvaranja lažnog digitalnog potpisa za određenu poruku,
- Potpis mora omogućiti praktično pohranjivanje kopije digitalnog potpisa.

Digitalni potpisi su važan alat u osiguravanju autentičnosti i integriteta digitalnih podataka, ali kao i svaki sigurnosni mehanizam imaju svoje slabosti. Slabosti digitalnih potpisa uključuju ranjivosti u sigurnosti privatnih ključeva, mogućnost napada na samu kriptografsku shemu i potencijalne prijetnje od napadača koji koriste napredne tehnike kao što su kvantna računala. Idućom podjelom su definirane razine mogućeg utjecaja probijanja sigurnosti digitalnog potpisa od strane napadača, [7]:

- Potpuni prekid - Napadač otkriva korisnikov privatni ključ,
- Univerzalno krivotvorenje - Napadač otkriva učinkovit algoritam potpisivanja koji omogućuje izgradnju valjanih potpisa za proizvoljne poruke,
- Selektivno krivotvorenje - Napadač krivotvori potpis za određenu poruku koju je napadač odabrao,
- Egzistencijalno krivotvorenje - Napadač krivotvori potpis za barem jednu poruku, pri čemu napadač nema kontrolu nad odabranom porukom. Stoga, ta krivotvorina može samo djelomično narušiti integritet korisnika.

3.2. Šifriranje komunikacije

Kao i u svakoj inačici korištenja infrastrukture javnog ključa, prvi korak je generiranje para ključeva. Javni ključ je javno dostupan i koristi se za šifriranje komunikacije, dok privatni ključ služi za dešifriranje komunikacije. Nakon generiranja para ključeva, digitalni certifikati izdaju se u svrhu potvrđivanja identiteta vlasnika ključa. Certifikat je digitalni dokument koji sadrži informacije o vlasniku ključa, poput imena, adrese e-pošte i javnog ključa. Kako bi se osiguralo povjerenje u autentičnost certifikata, on mora biti potpisan od strane pouzdane treće strane - certifikacijskog tijela. CA provjerava identitet vlasnika ključa, odrađuje postupak provjere autentičnosti i integriteta podataka, te potpisuje certifikat svojim privatnim ključem. Na taj način se osigurao integritet certifikata, te je potvrđeno da je izdan od strane pouzdane organizacije, [8].

Nakon što su certifikati potpisani i infrastruktura javnog ključa je postojana, slijedi distribucija certifikata. Certifikati se distribuiraju putem javno dostupnih repozitorija koristeći protokole poput HTTP-a (engl. *Hypertext Transfer Protocol*). Upotrebom javnih repozitorija osigurava se pristup korisniku do javnog ključa certificirajućeg tijela koji je potreban kako bi se izgradio lanac povjerenja certifikata kako bi korisnički certifikat bio validan. Spomenute lokacije ili repozitoriji se još nazivaju i točke distribucije certifikata (engl. *Certificate Distribution Point* - CDP). CDP lokacija je pohranjena u svakom certifikatu, te je nužna za potvrdu autentičnosti certifikata na dnu lanca. Osim CDP lokacije bitno je spomenuti listu opoziva certifikata (engl. *Certificate Revocation List* - CRL). Putanja CRL liste je također zapisana unutar svakog certifikata,

te služi tome da bi se moglo ustvrditi nalazi li se krajnji certifikat na toj listi. Svaki certifikat koji se nalazi na CRL listi je iz nekog razloga opozvan, te više nije pravovaljan. Primjeri opozivanja certifikata mogu biti scenariji poput kompromitacije privatnog ključa, lažnog predstavljanja s informacijama unutar samog certifikata i slično, [9].

Nakon što se provjeri CDP i CRL lokacija, te se ustanovi da je certifikat važeći i izdan od strane certificirajućeg tijela koje je javno legitimno, korisniku se omogućuje HTTPS (engl. *Hypertext transfer protocol secure*) komunikacija što znači da se komunikacija odvija preko protokola koji je šifriran. Šifrirana komunikacija se odnosi na postupak pretvaranja podataka u nečitljiv oblik koji se može čitati samo uz pomoć odgovarajućeg ključa ili šifre. Nekoliko ključnih prednosti šifrirane komunikacije su, [10]:

- Sigurnost podataka – Štiti podatke od neovlaštenog pristupa. Ukoliko komunikacija bude kompromitirana, podaci će i dalje biti nečitljivi bez ključa za dešifriranje,
- Vjerodostojnost – Šifrirana komunikacija pruža autentičnost podataka i identiteta strana koje komuniciraju,
- Povjerljivost – Samo osobe s odgovarajućim ključem mogu dešifrirati podatke. Povjerljivost je nužna u razmjenama financijskih podataka, osobnih podataka ili povjerljivih poslovnih informacija,
- Integracija u mrežnu sigurnost – Šifriranje je važan dio sigurnosnih protokola i zaštite infrastrukture. Svoju svrhu pronalazi u raznim mrežnim aplikacijama, protokolima, virtualnim privatnim mrežama, te osiguravanju slanja električne pošte,
- Usklađenost s propisima – Koristi se kao mjera usklađenosti sa zakonima i propisima koji su odgovorni za regulaciju zaštite privatnosti podataka, poput opće uredbe o zaštiti podataka (engl. *General Data Protection Regulation* – GDPR).

Iako šifriranje pruža visoku razinu sigurnosti, važno je napomenuti da nije potpuno neprobojno. Sigurnost šifriranih podataka ovisi o šiframa, ključevima i kvaliteti korištenih algoritama za šifriranje. Sigurnost šifrirane komunikacije može biti ugrožena na nekoliko načina, [10]:

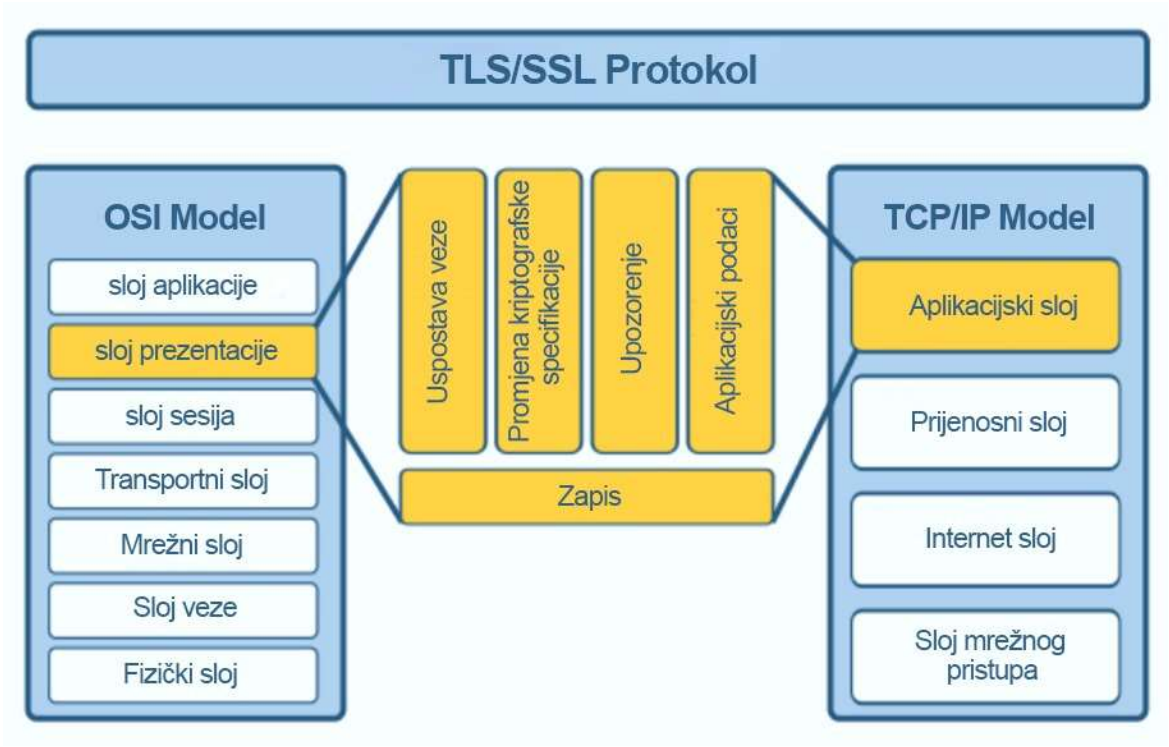
- Slab algoritam - Korištenje zastarjelog ili slabijeg algoritma olakšava probijanje šifrirane komunikacije,
- Slaba šifra ili ključ - Kratkotrajne, predvidljive ili slabo generirane šifre ili ključevi lakše budu probijeni,
- Napadi na ključeve - Uključuje metode poput *brute-force* napada ili napada na baze podataka ključeva,
- Napadi na implementaciju - Ranjivosti u softveru, hardveru ili mrežnoj infrastrukturi pružaju priliku za pristupanjem šifriranim podacima.

Kako bi se onemogućila kompromitacija infrastrukture javnog ključa i šifrirane komunikacije važno je redovito ažurirati kriptografske algoritme i pratiti najnovije preporuke i standarde. Također je važno da organizacije koriste sigurne prakse u generiranju, upravljanju i

zaštiti ključeva. Iako šifriranje nije neprobojno, s pravilno implementiranim algoritmima, jakim šiframa i ključevima te pažljivom sigurnosnom praksom može pružiti visoku razinu sigurnosti za šifrirane podatke, [10].

Šifrirana komunikacija se odvija preko sigurnosnih protokola koji se baziraju na kriptografiji kao takvoj, što znači da se prilikom komunikacije koriste ključevi. Sigurnosni protokoli su ključni elementi zaštite podataka i komunikacije u digitalnom svijetu. Uz sve veću prisutnost interneta i ovisnost o razmjeni podataka putem mreža, sigurnost postaje prioritetni cilj za organizacije i pojedince. Sigurnosni protokoli, koji se temelje na kriptografiji, pružaju mehanizme zaštite podataka od prisluškivanja, manipulacije, neovlaštenog pristupa ili krađe [11].

Jedan od najpoznatijih i najčešće korištenih sigurnosnih protokola je SSL/TLS (engl. *Secure Sockets Layer/Transport Layer Security*). Slikom 1 ispod prikazan je položaj SSL/TLS sigurnosnog protokola u mrežnim modelima OSI (engl. O*pen Systems Interconnection*) i TCP/IP (engl. *Transmission Control Protocol/Internet Protocol*), [11].



Slika 1. Položaj SSL/TLS protokola u mrežnim modelima OSI i TCP/IP, [12]

SSL/TLS se koristi za zaštitu *web* prometa (HTTPS) i aplikacija koje zahtijevaju sigurnu komunikaciju putem interneta. Ovaj protokol koristi kombinaciju simetrične i asimetrične kriptografije kako bi šifrirao podatke između klijenta i poslužitelja, osiguravajući da neovlaštene osobe ne mogu presresti ili pročitati podatke, [11].

3.3. Virtualne privatne mreže (VPN)

Sigurnost na internetu postaje sve važnija kako se digitalna era nastavlja razvijati. U svijetu u kojem se velika količina informacija prenosi putem mreže, zaštita privatnosti i povjerljivosti postaju imperativ. Jedan od ključnih alata koji pruža sigurnost i privatnost na internetu je virtualna privatna mreža (engl. *Virtual Private Network* - VPN). VPN pruža sigurnu vezu između korisnikovog uređaja i infrastrukture tako da se podaci kriptiraju i prolaze kroz poseban tunel. Time se osigurava da korisnikova privatnost ostane netaknuta i da se osjetljivi podaci ne mogu lako presresti ili dešifrirati. Certifikati igraju važnu ulogu u zaštiti virtualne privatne konekcije pružavši joj sloj sigurnosti kroz autentifikaciju, enkripciju, integritet podataka i povjerljivost. Certifikati su digitalni identifikatori koji potvrđuju autentičnost i identitet sudionika u VPN-u. Oni osiguravaju da korisnik komunicira s pravim VPN poslužiteljem, a ne sa zlonamjernim napadačem koji pokušava pristupiti podacima. Certifikati također pružaju mehanizme za enkripciju podataka i provjeru integriteta tijekom komunikacije. Bez certifikata, VPN bi bio ranjiv na različite vrste napada, uključujući prisluškivanje, lažiranje identiteta i krađu podataka, [13].

VPN poslužitelj ima svoj certifikat koji potvrđuje njegovu autentičnost, dok korisnik ima svoj certifikat koji potvrđuje njegov identitet. Kada se korisnik povezuje s VPN poslužiteljem, oba certifikata se razmjenjuju kako bi se provjerile identifikacije i osiguralo povjerenje između njih. Kada se uspostavi veza, koristi se javni ključ sadržan u certifikatu kako bi se sigurno razmijenio simetrični ključ koji se koristi za enkripciju podataka tijekom komunikacije. Certifikati osiguravaju da samo autorizirani sudionici mogu dekriptirati podatke. Tijekom trajanja konekcije koriste se digitalni potpisi koji se generiraju pomoću privatnog ključa sadržanog u certifikatu. Digitalni potpisi se u ovom slučaju koriste za provjeru da su podaci tijekom prijenosa ostali netaknuti i nepromijenjeni, [13].

Slikom 2 prikazano je sučelje kreiranja nove VPN konekcije u alatu *FortiClient VPN*. Prilikom postavljanja VPN pristupnih podataka nalazi se mogućnost dodavanja certifikata kako bi se osigurala sigurna povezanost.

Slika 2. Certifikati za VPN u FortiClient VPN alatu

Certifikati mogu biti pohranjeni na tri različite lokacije, a to su, [13]:

- certifikati - lokalno računalo,
- certifikati - trenutni korisnik,
- Pametna kartica za pohranu certifikata.

3.4. Mobilne aplikacije

Mobilni uređaji su revolucionirali poslovne operacije, omogućujući tvrtkama i zaposlenicima da ostanu u kontaktu i van ureda. Iako povećana povezanost donosi prednosti za poslovanje, ona također uvodi značajne sigurnosne prijetnje, probleme s privatnošću i ranjivosti u poslovne sustave. Iz perspektive poslodavca, upravljanje povjerenjem u mobilnim okruženjima slično je upravljanju povjerenjem u korporativnim računalima. IT odjeli koriste alate za centralizirano upravljanje softverom i aplikacijama te aktivni direktorij za postavljanje korisničkih uloga i pravila. Većina organizacija ne dozvoljava zaposlenicima preuzimanje softvera ili aplikacija na korporativna računala, niti im dopušta korištenje osobnih prijenosnih računala za pristup svim korporativnim mrežama i podacima. Dakle, kao što je slučaj s korporativnim računalima, samo autoriziranim i provjerenim mobilnim uređajima treba biti omogućen pristup korporativnim resursima, [14].

Certifikati za mobilne aplikacije su digitalni potpisi koji se koriste za verifikaciju integriteta i autentičnosti mobilnih aplikacija, siguran pristup elektroničkoj pošti, enkripciju elektroničke pošte, osiguran *Wi-Fi (*engl*. Wireless Fidelity)*, VPN pristup i slično, [14].

Na primjeru instalacije aplikacija, postupak korištenja certifikata za mobilne aplikacije može se opisati u nekoliko koraka. Prvo, izdavačka kuća ili razvojni tim koji stoji iza mobilne aplikacije generira digitalni certifikat. Ovaj certifikat se može izdati od strane certifikacijskog tijela ili se može samostalno potpisati ukoliko je riječ o internom izdanju aplikacije. Drugo, nakon što je mobilna aplikacija razvijena, izdavač koristi privatni ključ certifikata kako bi digitalno potpisao aplikaciju. Taj potpis je jedinstven za svaku aplikaciju i koristi se kao dokaz o autentičnosti. Zatim se certifikat zajedno s potpisanim aplikacijskim paketom distribuira na relevantne trgovine aplikacija poput *Apple App Store*-a ili *Google Play Store*-a. Također, certifikat se može distribuirati i putem drugih kanala, kao što su interni sustavi ili alternativne trgovine aplikacija. Korisnici koji preuzmu mobilnu aplikaciju s trgovine aplikacija ili drugog izvora mobilnih aplikacija koriste certifikate kako bi provjerili autentičnost aplikacije prije nego je instaliraju. U pozadini, uređaji koriste javni ključ certifikata za provjeru digitalnog potpisa aplikacije. Da bi se vjerovalo certifikatu, uređaji koriste korijenske certifikate za povjerenje. Korijenski certifikati (engl. *Root Certificates*) su certifikati izdavačkih kuća koje su već prepoznate kao pouzdane. Ako je certifikat mobilne aplikacije izdan od strane vjerodostojne izdavačke kuće i potpisan njenim privatnim ključem koji se može povezati s valjanim korijenskim certifikatom, uređaj će vjerovati certifikatu aplikacije. Ovaj proces povjerenja i provjere certifikata osigurava korisnicima da je aplikacija autentična, da nije izmijenjena nakon potpisivanja te da je izdavačka kuća prepoznata i provjerena. Time se sprječava distribucija zlonamjernih aplikacija ili aplikacija koje su izdane od neovlaštenih izdavača, [14].

Prednosti korištenja digitalnih certifikata u sferi mobilnih uređaja su, [15]:

- Poboljšano korisničko iskustvo – manji zahtjevi za upis lozinke,
- Povećana sigurnost – baze podataka koje pohranjuju lozinke često budu mete napada, dok je rjeđi oblik napada na digitalne certifikate,
- Međusobna povezanost u povjerenju korijenskih certifikata između različitih operativnih sustava mobilnih uređaja,
- Ekonomičan način uvođenja sigurnosnog sloja – za razliku od MDM-a (engl. *Mobile Device Management*) i EMM-a (engl. *Enterprise Mobility Management*), primjena PKI digitalnih certifikata je već prisutna u većini mobilnih uređaja. Samim time, osiguravanje uređaja pomoću certifikata ne zahtjeva velika ulaganja, te podešavanje i održavanje nije kompliciranо.

3.5. Internet stvari

Eksplozivan rast senzorskih i pokretačkih uređaja povezanih s Internetom donosi brojne sigurnosne izazove u svijetu tehnologije. Bez obzira na to koliko je svaki pojedini uređaj jednostavan, Internet stvari predstavlja značajnu sigurnosnu prijetnju zbog svojih ogromnih razmjera, [16].

IoT (engl. *Internet of Things*) uređaji konstantno prikupljaju i razmjenjuju osjetljive podatke, najčešće je naglasak na osobnim podacima. Nedostatak sigurnih veza izlaže podatke napadima i krađi. Kako bi se ovi podaci zaštitili od neovlaštenog pristupa, PKI koristi asimetrične kriptografske algoritme kako bi omogućio sigurnu razmjenu ključeva između uređaja. Time se osigurava da samo ovlašteni uređaji mogu dekriptirati i pristupiti podacima, [16].

PKI olakšava sigurnu razmjenu simetričnih ključeva između IoT uređaja. Iako je simetrična kriptografija brža od asimetrične, ona zahtijeva prethodno dijeljenje ključeva, što je teže učiniti u dinamičnim IoT okruženjima. PKI omogućuje IoT uređajima da koriste asimetričnu kriptografiju za sigurnu razmjenu simetričnih ključeva, nakon čega se daljnja komunikacija obavlja bržim simetričnim kriptografskim algoritmima, [16].

IoT uređaji su često jednostavni senzori s resursima brojivim u desecima kilobajta. Kako bi ti uređaji bili dio infrastrukture javnog ključa, moraju imati razvijene postupke za dobivanje prvog certifikata i para ključeva, te obnovu i provjeru certifikata. Navedene operacije nisu kompleksnih struktura, no trenutni standardi infrastrukture javnog ključa nisu dizajnirani za uređaje na baterije s desecima kilobajta radne memorije, [17]. Nekoliko web protokola definirano je posljednjih godina kako bi se omogućilo IPv6 umrežavanje na uređajima s ograničenim resursima. Ovi protokoli obuhvaćaju različite slojeve OSI modela i pružaju različite funkcionalnosti, ovisno o specifičnim potrebama i zahtjevima IoT aplikacija. Neki od najpoznatijih protokola osmišljenih za IoT su, [17]:

- MQTT (engl. *Message Queuing Telemetry Transport*) je lagani protokol za komunikaciju koji je dizajniran za pouzdanu razmjenu poruka između IoT uređaja i poslužitelja. Omogućuje slanje poruka u obliku *publisher-subscriber* modela, što znači da uređaji mogu biti i izvori i primatelji podataka. Često se koristi u aplikacijama koje zahtijevaju minimalnu potrošnju energije i brz prijenos informacija, kao što su industrijska automatizacija, pametni kućanski uređaji i senzorske mreže,
- CoAP (engl. *Constrained Application Protocol*) je protokol namijenjen komunikaciji između uređaja s ograničenim resursima, kao što su senzori i mikrokontroleri. Ovaj protokol koristi REST arhitekturu (engl. *Representational State Transfer*) i ima sličnosti s HTTP-om, ali je optimiziran za rad u mrežama s niskom propusnošću i visokim kašnjenjem,
- BLE (engl. *Bluetooth Low Energy*) je bežični komunikacijski protokol koji je posebno osmišljen za uređaje s niskom potrošnjom energije. Često se koristi za povezivanje

pametnih telefona s raznim IoT uređajima, poput pametnih satova, pametnih zvučnika, zdravstvenih senzora i sl.;

- LoRaWAN (engl. *Long Range Wide Area Networking*) je protokol za bežičnu komunikaciju koji koristi tehnologiju niskog raspona za prijenos podataka na velike udaljenosti. Ovaj protokol omogućuje dugi doseg i nisku potrošnju energije, što ga čini prikladnim za aplikacije poput pametnih gradova, praćenja stoke i poljoprivrede.

PKI također omogućuje digitalno potpisivanje podataka koje šalje IoT uređaj. Kada IoT uređaj digitalno potpiše podatke, drugi uređaji mogu provjeriti vjerodostojnost tih podataka i osigurati da nisu izmijenjeni tijekom prijenosa.

3.6. Usluge u oblaku

Infrastruktura javnog ključa utemeljena na oblaku, također poznata kao PKIAAS (engl. PKI-as-a-Service), predstavlja suvremenu alternativu tradicionalnim lokalnim PKI implementacijama. Ovaj pristup obuhvaća model u kojem je PKI smješten i održavan unutar *cloud* okruženja te se korisnicima pruža kao usluga na zahtjev. Time korisnici ostvaruju sve prednosti potpune PKI infrastrukture bez potrebe za upravljanjem troškovima vezanim uz hosting, održavanje i fizičku infrastrukturu. Infrastrukturu u pozadini, uključujući održavanje, sigurnosne aspekte i izradu sigurnosnih kopija, preuzima na sebe pružatelj *cloud* PKI usluge, [18].

Glavne prednosti infrastrukture javnog ključa temeljene na oblaku su, [18]:

- Jednostavnost implementacije - omogućava brzu i jednostavnu uspostavu cjelokupne hijerarhije certifikacijskih tijela za izdavanje različitih vrsta certifikata krajnjih entiteta, uz minimalan napor i u kraćem vremenskom roku. Ovaj pristup značajno smanjuje složenost postavljanja i održavanja tradicionalno složene PKI infrastrukture, istovremeno povećavajući operativnu učinkovitost,
- Robustan, siguran i usklađen PKI - Pružatelji cloud PKI usluga upravljaju postupkom stvaranja korijenskog certifikacijskog tijela uz osiguravanje najviših sigurnosnih standarda. U određenim slučajevima, poduzećima je omogućeno daljinsko postavljanje korijenskog certifikata, uključujući sigurnu izvedbu ključnih procesa poput stvaranja ključeva. Ključevi se generiraju i pohranjuju u napredne sigurnosne uređaje, kao što su hardverski sigurnosni moduli (engl. *Hardware Security Module* - HSM) koji zadovoljavaju FIPS (engl. *Federal Information Processing Standards*) standarde. Osim toga, automatizacija u PKI rješenjima temeljenim u oblaku omogućuje dosljednu primjenu PKI politika za izdavanje i upravljanje certifikatima i ključevima, što unapređuje sigurnost i osigurava usklađenost s relevantnim regulativama,
- Visoko dostupna i skalabilna infrastruktura - S obzirom na sve veći broj digitalnih certifikata potrebnih u suvremenim poslovnim okruženjima, kao i na skraćeni životni vijek tih certifikata, PKI temeljen na oblaku nudi prilagodljivu infrastrukturu koja se može brzo skalirati prema potrebama, bez brige o prekidima u radu. Ova infrastruktura

pruža neograničen kapacitet, omogućujući poduzećima da prilagode svoje resurse u skladu s poslovnim zahtjevima, dok pružatelj PKI usluge preuzima odgovornost za nadogradnju i održavanje infrastrukture. PKI temeljen na oblaku nudi se s neograničenim kapacitetom i može se povećati ili smanjiti ovisno o poslovnim potrebama. Budući da nadogradnjom infrastrukture u potpunosti upravlja pružatelj PKI usluga, poduzeća ne moraju planirati redizajn infrastrukture kako bi postigla skalabilnost,

- Smanjeni ukupni trošak vlasništva - PKI temeljen na oblaku eliminira potrebu za velikim kapitalnim ulaganjima u hardver i softver potreban za tradicionalni *on-premise* PKI. Poduzeća mogu koristiti ove usluge putem modela pretplate ili plaćanja po korištenju, čime se značajno smanjuju troškovi. Osim toga, potreba za specijaliziranim PKI osobljem i ekspertizom također je smanjena, čime se dodatno snižava ukupni trošak vlasništva u usporedbi s tradicionalnim rješenjima.

Neke od negativnih karakteristika korištenja PKIAAS usluge u *cloud* okruženju su, [18]:

- Ograničene značajke - Neki pružatelji usluga u oblaku mogu ponuditi samo ograničene verzije s manje značajki od onoga što tražite,
- Podrška - Ovisno o pružatelju usluga, podrška može predstavljati problem. Neki davatelji usluga nude ograničenu pomoć ili online podršku s kojom se može biti teško nositi,
- Prilagodba - može biti ograničena ovisno o odabranom pružatelju usluga. Sama kombinacija *on-premise* PKI komponente sa PKIAAS usluge može biti zahtjevno, te ukolikoo su mogućnosti ograničene, i neizvedivo.

U primjeru Microsoftovog *Cloud* PKI rješenja opisat će se funkcionalnost SCEP (engl. *Simple Certificate Enrollment Protocol*) servisa i Intune aplikacije, koji u kombinaciji sa *Cloud* PKI modelom potpisuju, monitoriraju i obnavljaju krajnje certifikate, [19].

S obzirom na sve veću podršku organizacija za hibridne i udaljene radne okoline, pojavljuju se izazovi vezani uz upravljanje raznovrsnim uređajima koji pristupaju organizacijskim resursima. Zaposlenici i studenti trebaju mogućnost sigurne suradnje, rada s različitih lokacija, te pristupa i povezivanja s ključnim resursima organizacije. Administratori su suočeni sa zadatkom zaštite organizacijskih podataka, upravljanja pristupom krajnjih korisnika, te pružanja podrške korisnicima bez obzira na njihovu fizičku lokaciju, [19].

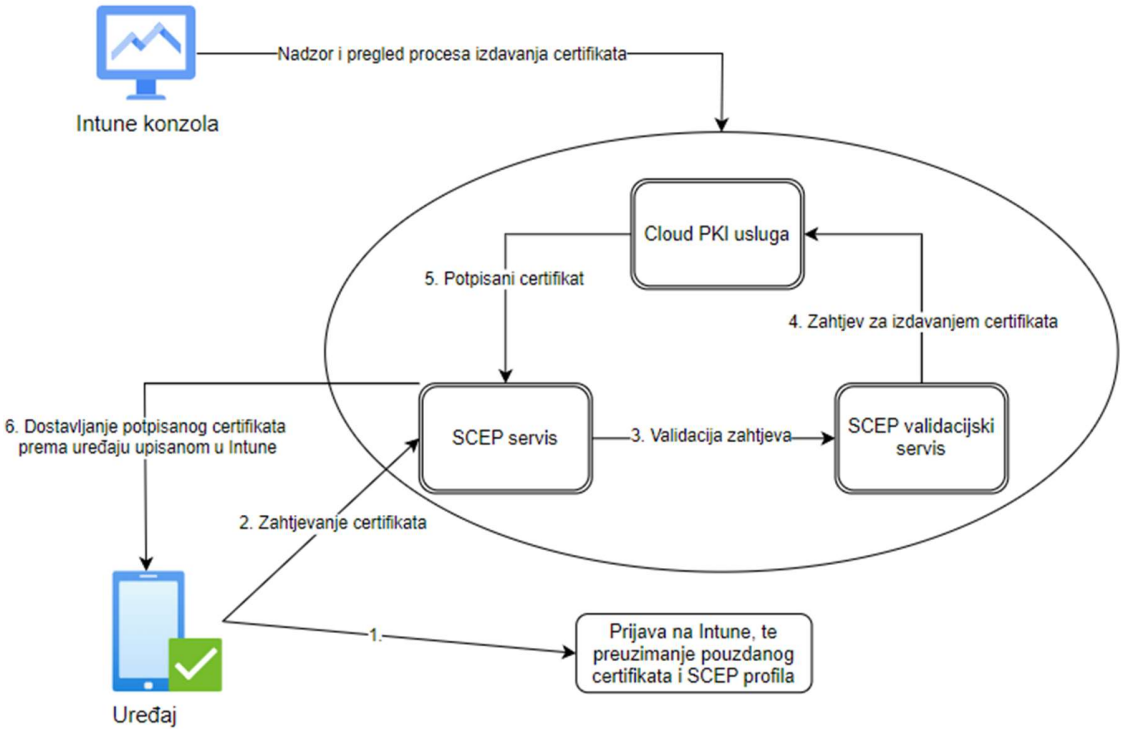
Microsoft Intune, kao rješenje za upravljanje krajnjim točkama utemeljeno na oblaku, nudi sveobuhvatne mogućnosti za upravljanje pristupom organizacijskim resursima. Ovaj sustav omogućuje centralizirano upravljanje aplikacijama i uređajima, uključujući mobilne uređaje, stolna računala i virtualne krajnje točke, čime se značajno pojednostavljuje administracija i povećava sigurnost u hibridnim radnim okruženjima, [19].

Kao rješenje temeljeno na oblaku, Microsoft Cloud PKI automatizira i pojednostavljuje upravljanje životnim ciklusom certifikata za uređaje pod upravom Intune-a. Ova usluga pruža namjensku infrastrukturu javnih ključeva za organizaciju, eliminirajući potrebu za lokalnim poslužiteljima, konektorima ili hardverom. Microsoft Cloud PKI preuzima odgovornost za

izdavanje, obnavljanje i opoziv certifikata na svim platformama koje su podržane unutar Intune okruženja, osiguravajući cjelovitost i sigurnost upravljanja certifikatima u organizaciji, [19].

Cloud PKI pruža SCEP protokol koji djeluje kao usluga za registraciju certifikata. Ova usluga u ime uređaja kojima upravlja Intune traži certifikate od certifikacijskog tijela koristeći SCEP profil. Na taj način, SCEP usluga automatizira proces izdavanja certifikata, omogućujući sigurno upravljanje certifikatima za uređaje unutar organizacije, [19].

Slikom 3 je prikazan proces upisivanja uređaja na aplikaciju Intune, te uloge pojedinih komponenti.



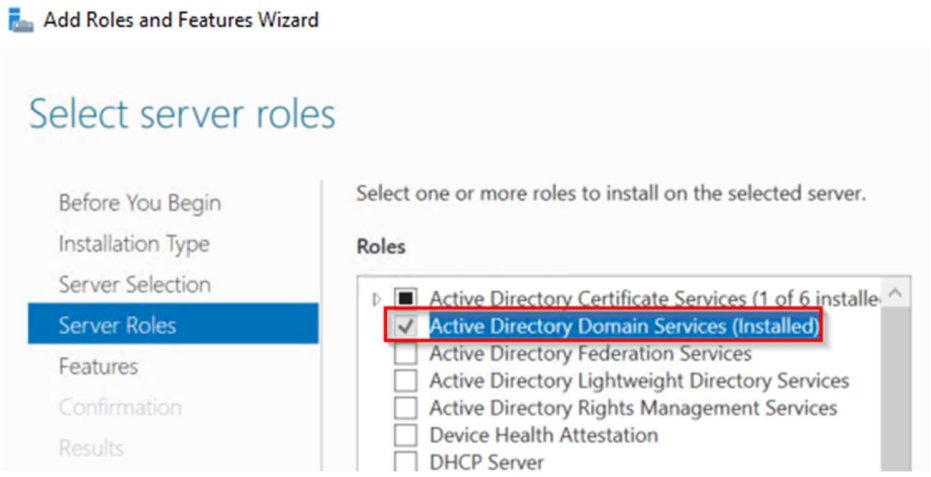
Slika 3. Proces upisivanja uređaja na aplikaciju *Intune*

4. Implementacija infrastrukture javnog ključa

U svrhu testiranja funkcionalnosti infrastrukture javnog ključa podići će se sustav u testnoj okolini. Sustav će sadržavati dva servera u obliku dvoslojne hijerarhije infrastrukture javnog ključa. Korijenski server (engl. *Root Server*) koji izdaje glavni certifikat, takozvani korijenski certifikat se smatra najvećim autoritativnim tijelom, te se ne nalazi u domeni i većinu je vremena ugašen. Zatim će se podići još jedan server koji ima ulogu potpisivanja certifikata krajnjim uređajima i korisnicima, takozvani izdavajući server (engl. *Issuing server*). Izdavajući server je dio domene, te se informacije o infrastrukturi javnog ključa preslikavaju u aktivni direktorij upravo preko tog servera. Izdavajući server će također imati instalirane dvije dodatne uloge, a to su uloga domenskog kontrolora kako bi domena bila postojana, te uloga Web servera, kako bi se mogla objaviti lokacija CRL repozitorija gdje krajnji uređaji mogu testirati valjanost certifikata.

4.1. Instalacija PKI komponente

Sama instalacija PKI komponente se odrađuje kroz izbornik *Server Manager*. Prilikom instalacije PKI komponente serveru bira se ADCS (engl. *Active Directory Certificate Services)* komponenta što je prikazano slikom 3.



Slika 4. Instalacija AD CS komponente

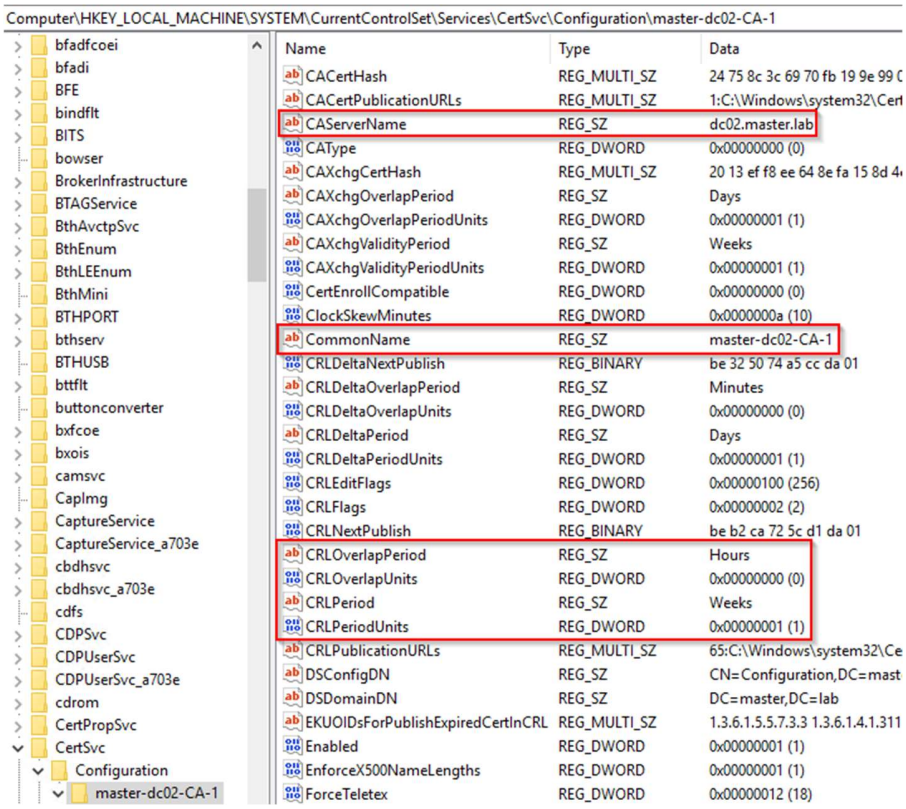
Nakon što je komponenta instalirana potrebno je konfigurirati postavke certificirajućeg tijela kako bi odgovarale potrebama organizaciji za koju se instalira. U ovom radu koristit će se osnovne postavke koje ne zahtijevaju specifičnu konfiguraciju. Postojeću konfiguraciju je moguće mijenjati alatom *Command Prompt,* te sve promjene su vidljive u uredniku registra na putanji koja je kreirana za certificirajuće karakteristike prilikom instalacije komponente AD CS. Budući da je certificirajućem tijelu dano ime *master-dc02-CA-1,* lokacija u registru na kojoj su zabilježene postavke ADCS komponente je

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\master-dc02-CA-1

Postavke koje su uređivane nakon instalacije ADCS komponente su iduće, [20]:

- DSConfigDN - daje informacije o tome gdje se nalazi konfiguracijska particija u slučaju da su CRL-ovi ili CA certifikati objavljeni u aktivnom direktoriju,
- CRLPeriodUnits – definira jedinicu kojom se utvrđuje vrijednost CRL dokumenta (npr. sati),
- CRLPeriod - definira trajanje CRL dokumenta (npr. 10),
- CRLOverlapPeriodUnits - definira jedinicu kojom se utvrđuje mogućnost postojanja dvaju CRL dokumenata istovremeno (npr. sati),
- CRLOverlapPeriod – definira vrijeme u kojem dva CRL dokumenta mogu postojati istovremeno (npr. 5),
- ValidityPeriodUnits – definira jedinicu maksimalne vrijednosti trajanja certifikata (npr. godina),
- ValidityPeriod – definira maksimalno trajanje certifikata (npr. 20 godina),
- AuditFilter – definira koji su ADCS relevantni događaji zabilježeni u sigurnosnim logovima,
- CRLPublicationURLs – definira putanju CRL repozitorija ukoliko je CRL objavljen na *Web serveru*.

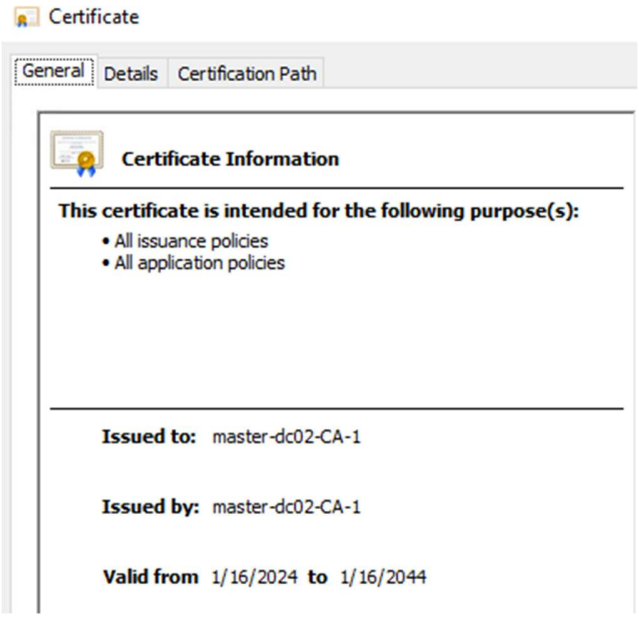
Slikom 4 su prikazane postavke certificirajućeg tijela nakon odrađenih promjena nad AD CS komponentom.



Slika 5. *Registry* postavke certificirajućeg tijela

Instalacija AD CS komponente je identična za vršni i izdavajući server. Jedina razlika na koju je potrebno obratiti pozornost je te da je izdavajući server dio domene, te je na njemu potrebno definirati lokacije AD kontenjera s kojih će krajnji uređaji povlačiti i provjeravati certifikate, [20].

Kako bi aktivni direktorij znao koji je server vršni, a koji izdavajući, potrebno je prilikom instalacije AD CS komponente definirati zasebno uloge servera. Nakon što je navedeno odrađeno, jedina radnja koju je potrebno napraviti na vršnom serveru je izdati certifikat s predloška *Subordinate Certification Authority,* te s kreiranim certifikatom potpisati izdavajući server kako bi izdavajući server naknadno mogao potpisivati krajnje certifikate u ime vršnog servera. Certifikat koji je izdan u svrhu potpisivanja izdavajućeg servera je prikazan slikom 5, [20].



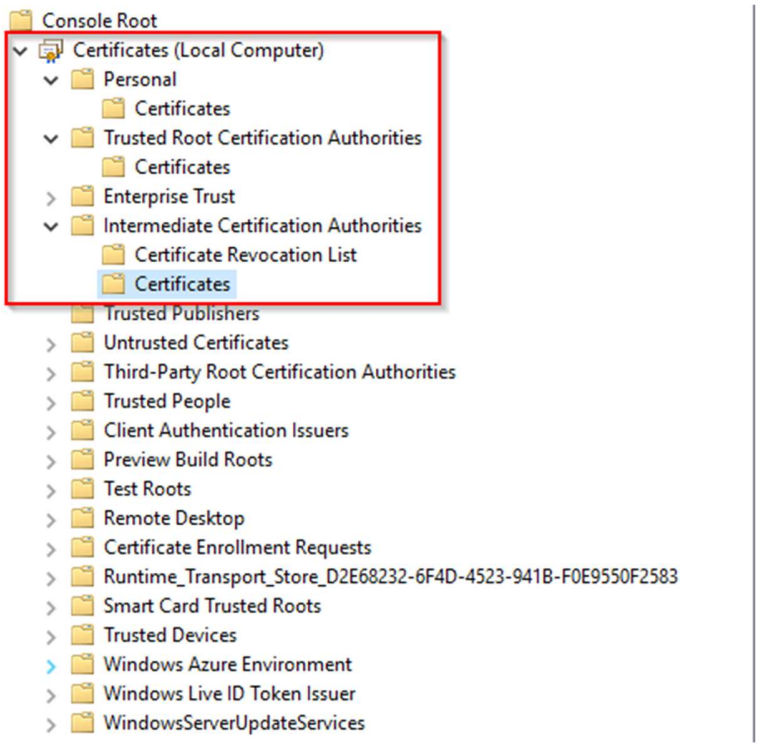
Slika 6. Korijenski certifikat

Nakon što je navedeno odrađeno, korijenski server je po najboljoj praksi potrebno ugasiti, te ga paliti jednom mjesečno prilikom instalacije sigurnosnih zakrpi, jednom u 6 mjeseci prilikom obnove CRL liste, te jednom u 20 godina prilikom obnove korijenskog certifikata (ovisno o definiranim trajanjima CRL liste i certifikata), [20].

Sve funkcionalnosti naknadno definirane u radu biti će prikazane i odrađene na izdavajućem serveru budući da je većina konfiguracije podesiva upravo na tom serveru.

4.2. Certifikati

Dok je u trećem poglavlju objašnjeno na koji se način certifikati mogu koristiti, ovaj odlomak će se više fokusirati na konfiguraciju certifikata, na koji način se sve certifikat može izdati te koje je sve funkcionalnosti moguće dodati certifikatu. Prvenstveno, certifikati se izdaju na temelju predloška koji se konfigurira na izdavajućem serveru. Prilikom otvaranja *mmc snap-in* alata (engl. *Microsoft management center*) moguće je pregledati koje sve certifikate računalo ili trenutno autenticirani korisnik posjeduju. Dodatno, uz same krajnje certifikate iz konzole je moguće vidjeti kojim izdavajućim i korijenskim certifikatima računalo vjeruje, tj. ima instalirane unutar svog računala i smatra pouzdanima. Konzola je prikazana slikom 6 gdje su vidljivi predefinirani folderi koji pohranjuju certifikate različitih funkcionalnosti i povjerenja, [21].



Slika 7. Konzola za pristup certifikatima iz perspektive korisnika

Tri su glavna foldera za lokalnu pohranu certifikata, a to su, [21]:

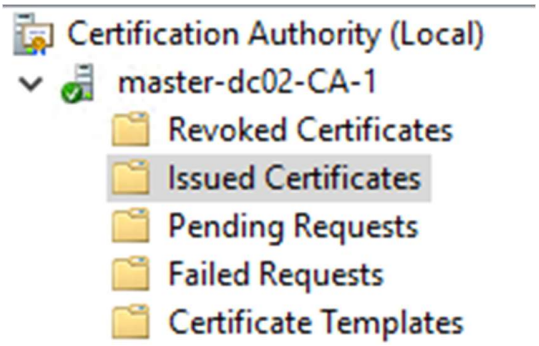
- Osobni (engl. *Personal*) – služi za pohranu krajnjih certifikata od korisnika,
- Korijenski certifikati (engl. *Trusted Root Certification Authorities*) – služi za pohranu korijenskih certifikata kojima računalo vjeruje,
- Izdavajući certifikati (engl. *Intermediate Certification Authorities*) – sadrži certifikate koji se nalaze u sredini certificirajućeg lanca; potpisani su od strane korijenskih certifikata, a izdali su krajnji certifikat.

Iz perspektive administratora PKI komponente konzola koja služi za pregled stanja izdanih certifikata naziva se tijelo za izdavanje certifikata (engl. *Certification Authority* - CA). Konzola sadrži informacije o stanju zahtjeva certifikata i informacije o izdanim certifikatima, [20]. Podjela je iduća, [22]:

- Povučeni certifikati – certifikati koji su iz određenih razloga povučeni iz uporabe te se nalaze na CRL listi,
- Izdani certifikati – svi certifikati koji su izdani od certificirajućeg tijela,
- Zahtjevi na čekanju – Najčešće se radi o zahtjevima koji traži izdavanje certifikata, no certifikat nije izdan prije dodatnog pregleda i odobrenja administratora PKI komponente,

- Neuspješni zahtjevi – Zahtjevi koji su iz određenih razloga (npr. korisnik nema pravo zatražiti certifikat s određenog predloška) nepravilno izvedeni,
- Predlošci certifikata – Lokacija koja pokazuje s kojih sve predložaka je moguće zatražiti certifikat, te osnovne informacije o samim predlošcima.

Slikom 7 je prikazana konzola za pristup certifikatima iz perspektive administratora PKI komponente. Samo određeni računi u domeni imaju pravo pristupiti navedenoj konzoli. Najčešće su prava definirana članstvom u grupi u aktivnom direktoriju, no prava također mogu biti direktno dodijeljena računu, [22].



Slika 8. Konzola za pristup certifikatima iz perspektive administratora

Lokacija gdje se definiraju postavke certifikata je zapravo mjesto gdje se konfiguriraju predlošci certifikata, budući da se certifikati izdaju na temelju predloška. Konzolu za pregled predložaka je također moguće pokrenuti kroz *mmc snap-in* te je prikazana slikom 8, [22].

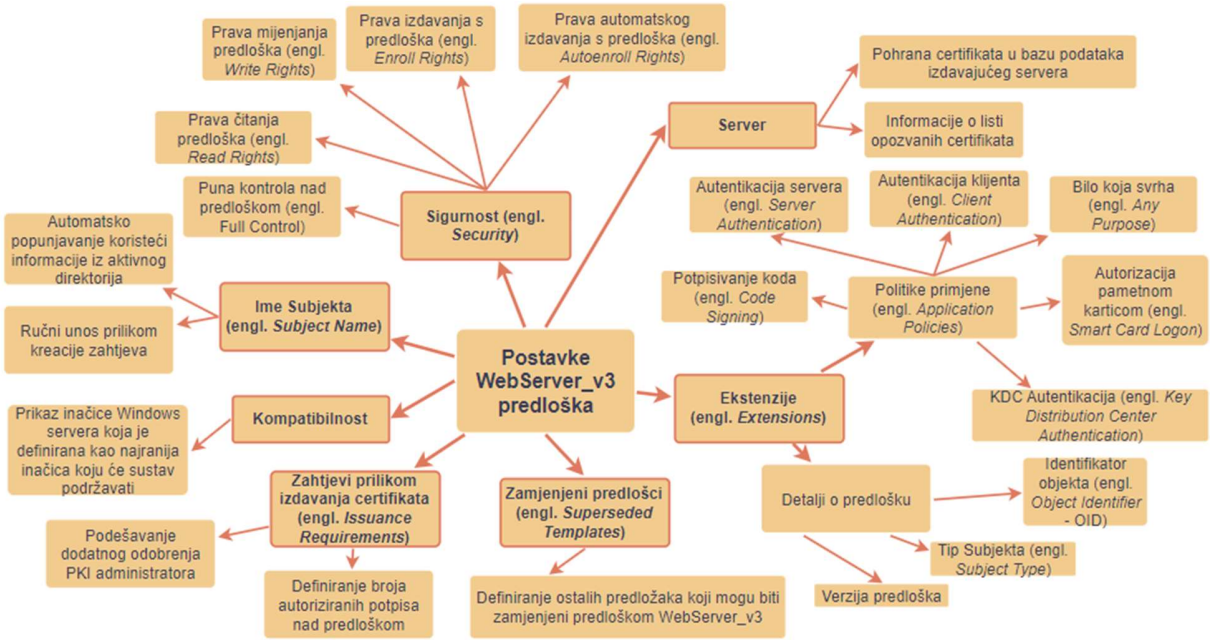
Iz slike ispod je moguće vidjeti predloške certifikata koji su definirani na certificirajućem tijelu. Osim imena i funkcionalnosti predložaka moguće je iščitati verziju sheme predloška. Verzija prikazuje radi li se o predlošku koji je modificiran (*Schema Version 2/3*) ili je predefiniran, tj. inicijalno kreiran prilikom kreacije PKI komponente (*Schema Version 1*). Predlošci koji su na slici modificirani će se u naknadnom poglavlju koristiti za kreaciju certifikata nad kojima je moguće ostvariti administratorska prava jer su konfigurirani da budu ranjivi na određene napade nad PKI komponentom, [22].

Certificate Templates

Template Display Name	Schema Version	Version	Intended Purposes
Workstation Authentication	2	101.0	Client Authentication
Web Server_v4	2	100.9	Any Purpose, Client Authentication, KDC A...
Web Server_v3	2	100.5	Server Authentication, Client Authentication
Web Server_v2	2	100.3	Server Authentication
Web Server_v	2	100.7	Server Authentication, KDC Authentication...
Web Server	1	4.1	
User Signature Only	1	4.1	
User	1	3.1	
Trust List Signing	1	3.1	
Subordinate Certification Authority	1	5.1	
Smartcard User	1	11.1	
Smartcard Logon	1	6.1	
Router (Offline request)	1	4.1	
Root Certification Authority	1	5.1	
RAS and IAS Server	2	101.0	Client Authentication, Server Authentication
OCSP Response Signing	3	101.0	OCSP Signing
Key Recovery Agent	2	105.0	Key Recovery Agent
Kerberos Authentication	2	110.0	Client Authentication, Server Authenticatio...
IPSec (Offline request)	1	7.1	

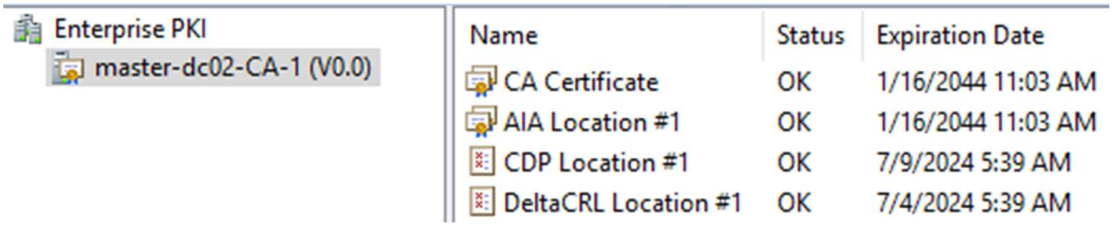
Slika 9. Konzola za konfiguraciju predložaka certifikata

U svrhu prikazivanja mogućnosti definiranja sigurnosnih mjera i prava nad predlošcima kao primjer uzet će se predložak WebServer_v3. Slikom 9 su prikazane postavke uređivanja predloška nad kojima je moguće konfigurirati iduće značajke:



Slika 10. Postavke WebServer_v3 predloška

Sučelje koje je dodatno važno napomenuti, osim sučelja za pregled izdanih certifikata i uređivanja predloška, je sučelje za pregled zdravlja PKI komponente. U navedenom sučelju je vidljivo stanje i vrijeme isteka glavnih certifikata (korijenskog i izdavajućeg certifikata), stanje i vrijeme isteka liste opozvanih certifikata te stanje Web lokacije nad kojim se certifikat može validirati, tj provjeriti je li i dalje valjan. Slikom 10 prikazano je navedeno sučelje, [22].

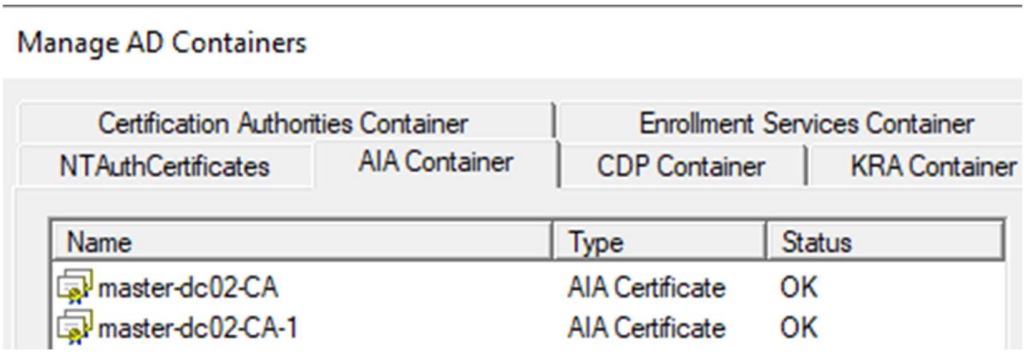


Slika 11. Sučelje za pregled zdravlja PKI komponente

Osim pregleda zdravlja ključnih PKI komponenti, u sučelju je također moguće vidjeti informacije koje su objavljene u aktivnom direktoriju, te ih dodatno dodavati ili brisati. Informacije pohranjene u aktivnom direktoriju se nalaze u takozvanim kontejnerima, te su podijeljene u iduće kontejnere), [23]:

- Kontejner certificirajućeg autoriteta (engl. *Certification Authorities Container*),
- Kontejner servisa za izdavanje certifikata (engl. *Enrollment Services Container*),
- Kontejner NTAuth Certificates,
- AIA kontejner (engl. *Authority Information Access Cointainer*),
- CDP kontejner (engl. C*ertificate Revocation List Distribution Point Cointainer*),
- KRA kontejner (engl. *Key Recovery Agent Cointainer*).

Slikom 11 je prikazano sučelje u kojem je moguće uređivati sadržaj pojedinih kontejnera.



Slika 12. Sučelje za uređivanje PKI kontejnera u aktivnom direktoriju

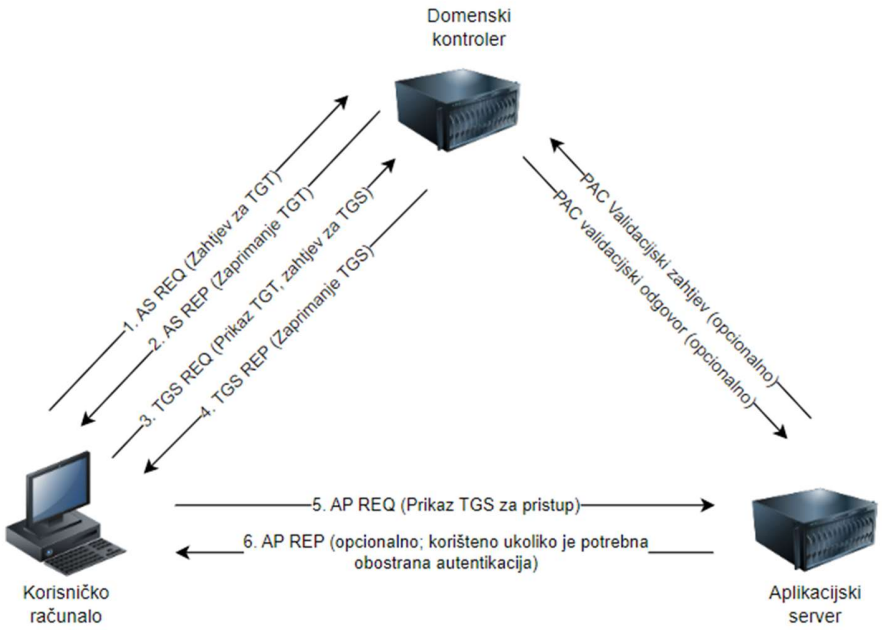
4.3. Mrežne karakteristike PKI komponente

Kao što je već spomenuto u radu, korijenski server je po najboljoj praksi izoliran od pristupa Internetu, izvan domene, te većinu vremena ugašen osim u situacijama u kojoj je potrebno instalirati mjesečne zakrpe, obnoviti CRL listu ili obnoviti korijenski certifikat. Izdavajući server je u drugu ruku definiran pravilima koje se moraju poštivati kako bi PKI komponenta mogla u potpunosti ispuniti funkcionalnost. Neki od glavnih karakteristika izdavajućeg certifikata su iduće, [24]:

- Nalazi se u domeni,
- Statička IP adresa,
- Otvoren port 135 prema svim uređajima u domeni u oba smjera (bidirekcionalno),
    - Port 135 podržava RPC protokol (engl. *Remote Procedure Call*) koji omogućuje jednom programu da traži uslugu od drugog programa na drugom računalu u mreži, bez potrebe za poznavanjem pojedinosti o mreži. Olakšava pokretanje koda na različitim sustavima, u ovom slučaju omogućuje zahtijevanje i prijenos certifikata,
    - Omogućuje transparentnost i neovisnost prilikom izdavanja certifikata krajnjem uređaju.
- Podešena lokacija na Web Serveru koja objavljuje CRL listu opozvanih certifikata,
    - Nužno je da je CRL lokacija dostupna svima, tj pristupa joj se putem HTTP procesa preko porta 80,
    - Nije nužno da CRL lokacija bude podešena na izdavajućem serveru, no u ovom radu je konfigurirano tako.
- Otvoren port 445 prema domenskim kontrolorima,
    - Nužno je zbog razmjene certifikata izdanog s predloška *Kerberos Authentication Template*, o kojem će se detaljnije pisati u tekstu ispod.

Kerberos dolazi od grčke riječi *Cerberus* koja predstavlja troglavog psa koji je čuvao ulaz u Had. Kerberos osigurava mrežu na principu trostruke provjere ili vjerovanja, te je osnovni

autentikacijski i autorizacijski protokol arhitekture *Microsoft Windows* još od *Windows Server 2000* verzije. Protokol daje pristup mrežnim aplikacijama i servisima na temelju KRBTGT ulaznice. U samom nazivu KRBTGT, *KRB* predstavlja *Kerberos*, dok *TGT* označava pojam *Ticket-Granting Ticket* kojem je funkcionalnost traženje ulaznice od domenskog kontrolora u svrhu pristupa mrežnim aplikacijama i servisima. Slikom 12 je prikazan tijek komunikacijskog procesa prilikom zahtijevanja i izdavanja TGT ulaznice, [25].



Slika 13. Tijek komunikacijskog procesa Kerberos servisa, [25]

Na domenskom kontroloru se nalazi treća strana kojoj se vjeruje nazvana Centar za distribuciju ključeva - KDC. Lozinka se pretvara u NTLM (engl. *New Technology LAN Manager*) *hash*, vremenska oznaka šifrirana je *hash*-om i poslana KDC-u kao autentifikator u zahtjevu za autentifikacijsku kartu (TGT) (AS-REQ). Zatim KDC provjerava korisničke podatke (ograničenja prijave, članstvo u grupi, itd.) i stvara TGT koji vraća korisniku (AS REP). Korisnik šalje TGT (TGS REQ) prema domenskom kontroloru koji sadrži KDC stranu, te ujedno šalje i zahtjev za onim čemu korisnik želi pristupiti. KDC server dekriptira TGT tajnim ključem, te se šifrirani token (engl. *Ticket-Granting Service* - TGS) šalje nazad korisniku (TGS REP). Aplikacijski poslužitelj zaprima TGS od korisnika (AP REQ) i provjerava token s KRBTGT lozinkom koja je dijeljena kao *hash* vrijednost, te ukoliko je token validan odobrava se pristup resursima korisniku (AP REP) na određeno vrijeme poznato pod nazivom TTL (engl. *Time to Leave*), [25].

Nakon što korisnik pošalje AP REQ aplikacijskom serveru, u rijetkim slučajevima aplikacijski server proslijeđuje AP REQ prema domenskom kontroloru i zatražuje verifikaciju PAC (engl. *Privileged Attribute Certificate*) potpisa. Domenski kontroler provjerava PAC potpis

korisnika, te ukoliko je PAC provjera uspješna, javlja aplikacijskom serveru da korisnik ima prava pristupanja servisima i uslugama, [25].

Upravo proces dodjele ulaznice opisan iznad, u kombinaciji s ranjivim predlošcima, omogućuje zloupotrebu certifikata predstavljajući običnog člana domene kao administratorskog računa. U idućem poglavlju je pokušano izvesti zloupotrebu KRBTGT ulaznica kako bi se ostvario administratorski pristup sustavu.

5. Istraživanje sigurnosnih izazova

Poglavlje 5 obuhvaća ostvarivanje administrativnog pristupa domeni koristeći običnog korisnika „vultest“ koji je kreiran u domeni master.lab. Sveukupno je općepoznato 13 napada na infrastrukturu javnog ključa, [26]:

- ESC1 - pogrešna konfiguracija predloška certifikata,
- ESC2 - pogrešna konfiguracija predloška certifikata,
- ESC3 - pogrešna konfiguracija predloška agenta za izdavanje certifikata,
- ESC4 - kontrola pristupa ranjivom predlošku certifikata,
- ESC5 - Ranjiva kontrola pristupa objektu PKI,
- ESC6 - EDITF_ATTRIBUTESUBJECTALTNAME2,
- ESC7 - Ranjiva kontrola pristupa izdavatelju certifikata,
- ESC8 - NTLM prijenos na AD CS HTTP krajnje točke,
- ESC9 - Bez sigurnosnog proširenja,
- ESC10 - Ranjivo preslikavanje certifikata,
- ESC11 - Preusmjeravanje NTLM-a na ICPR,
- ESC12 - Shell pristup ADCS CA s YubiHSM-om,
- ESC13 - Zlouporaba veze grupe OID vrijednošću.

Napadi opisani u radu su poznati pod imenima ESC1 i ESC3. Oba napada omogućuju administratorski pristup domeni, te se samim time smatraju kao maksimalno vertikalno ostvarivanje kontrole nad domenom. Napadi su testirani nad infrastrukturom podignutom u prethodnom poglavlju, te su komponente infrastrukture javnog ključa modificirane prema potrebama napada. Istraživanjem su obuhvaćena navedena dva napada iz više razloga. Obrađeni napadi ukazuju na specifične ranjivosti povezane s infrastrukturom javnih ključeva te ilustriraju kako naizgled minorna greška u konfiguraciji može rezultirati ozbiljnim sigurnosnim propustima. Konkretno, pogrešna konfiguracija certifikata ili agenta za izdavanje certifikata može omogućiti neovlašteno stjecanje administratorskih prava nad cijelom domenom. Ovo istraživanje naglašava važnost pravilne konfiguracije i sigurnosnih postavki u PKI sustavima, jer i najmanji propusti mogu imati dalekosežne posljedice po sigurnost cjelokupne IT infrastrukture. Kroz analizu ovih napada demonstrira se kako odstupanje od sigurnosnih preporuka, poput davanja prava domenskim korisnicima za izdavanje certifikata, može omogućiti napadačima da preuzmu kontrolu nad kritičnim dijelovima sustava, čime se dodatno naglašava potreba za rigoroznim sigurnosnim mjerama u upravljanju PKI sustavima.

5.1. Analiza ESC1 napada

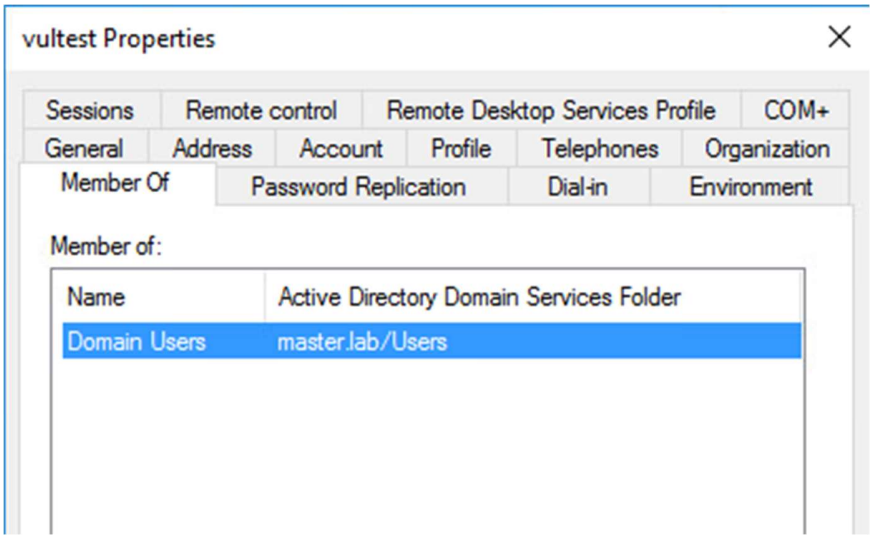
ESC1 napad je ostvarivanje administratorskih privilegija na način da se zatraži certifikat s predloška koji je ranjiv po tome što bilo koji autenticirani korisnik može samostalno, prilikom

izdavanja certifikata, popuniti polje alternativnog naziva subjekta (engl. *Subject Alternative Name - SAN*), [27].

Da bi se pogrešna konfiguracija predloška uspješno iskoristila, moraju se zadovoljiti sljedeći uvjeti, [27]:

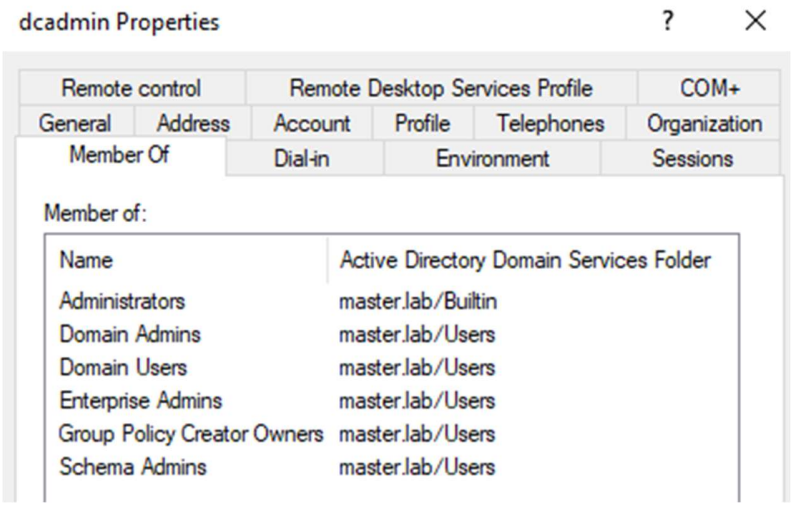
- Mogućnost izdavanja certifikata korisnicima s niskim pravima u domeni,
- Odobrenje upravitelja je onemogućeno,
- Nisu potrebni ovlašteni potpisi,
- Predložak certifikata definira EKU (engl. *Extended Key Usage*) koje omogućuju autentikaciju,
- Predložak certifikata omogućuje podnositeljima zahtjeva da specificiraju SAN u CSR-u (engl. C*ertificate signing request)*.

U ovom radu koristit će se korisnik *vultest* koji nije član niti jedne administrator grupe unutar domene. Slikom 13 je prikazano članstvo korisnika *vultest* unutar grupa u domeni, te je vidljivo da je korisnik jedino član grupe *Domain Users* u domeni *master.lab*.



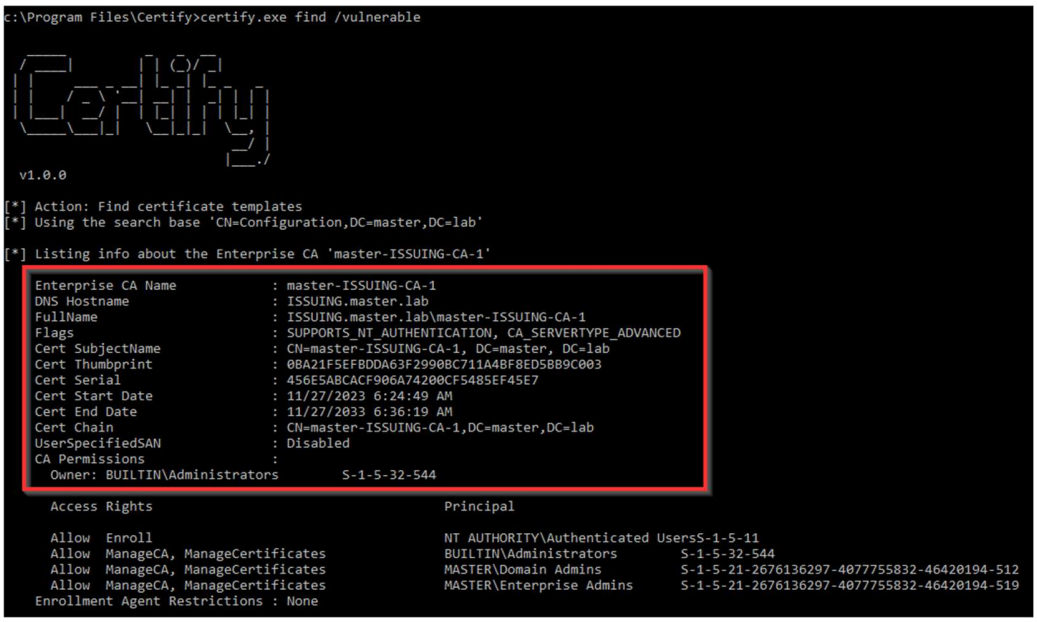
Slika 14. Članstvo u grupama korisnika *vultest* u domeni *master.lab*

Administratorska prava koja će se pokušati preuzeti su od korisnika *dcadmin* koji je član *Administrators* i *Domain Admins* grupa unutar domene što je prikazano slikom 14.



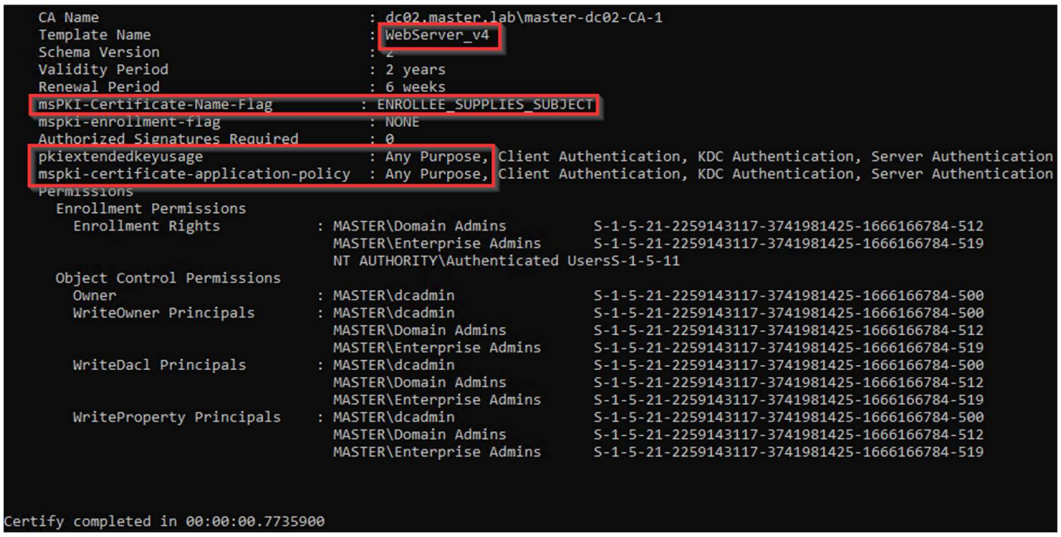
Slika 15. Članstvo u grupama korisnika *dcadmin* u domeni *master.lab*

Kako bi se provjerili ostali uvjeti za iskorištavanjem ranjivosti koristit će se alat *certify.exe*. *Certify.exe* pruža širok spektar funkcionalnosti za reviziju infrastrukture javnog ključa, uključujući mogućnost zahtjeva za novim certifikatima za trenutačno autenticiranog korisnika ili računalo. *Certify* je alat napisan u programskom jeziku C# koji prikazuje korisne konfiguracije i informacije o infrastrukturi u okruženjima infrastrukture javnog ključa, što će se prikazati u ovom radu. Slikom 4 pokrenuta je inicijalna naredba u alatu *certify* kojom se dobivaju informacije o certificirajućem tijelu u domeni. Inicijalna naredba koja će se koristiti je ***Certify.exe find /vulnerable*** , [28].



Slika 16. Prikaz rezultata naredbe *Certify.exe find /vulnerable*

Iz slike 15 je moguće iščitati naziv glavnog certificirajućeg tijela, DNS (engl. *Domain Name System*) zapis servera, informacije o vršnom certifikatu, te vrijeme trajanja vršnog certifikata. Također, istom naredbom se dobiva informacija postoje li ranjivi certificirajući predlošci te detalji na koji su način napada ranjivi što je prikazano slikom 16.



Slika 17. Pronalazak ranjivog predloška naredbom *Certify.exe find /vulnerable*

U ovom slučaju alat *certify.exe* je pronašao ranjivi predložak ***WebServer_v4*** nad kojim je moguće popunjavati SAN što se vidi iz vrijednosti atributa *msPKI-Certificate-Name-Flag* koji ima vrijednost *ENROLEE_SUPPLIES_SUBJECT*. Dodatno je sa slike 16 moguće vidjeti da svi autenticirani korisnici u domeni imaju pravo zatražiti certifikat s predloška *WebServer_v4*.

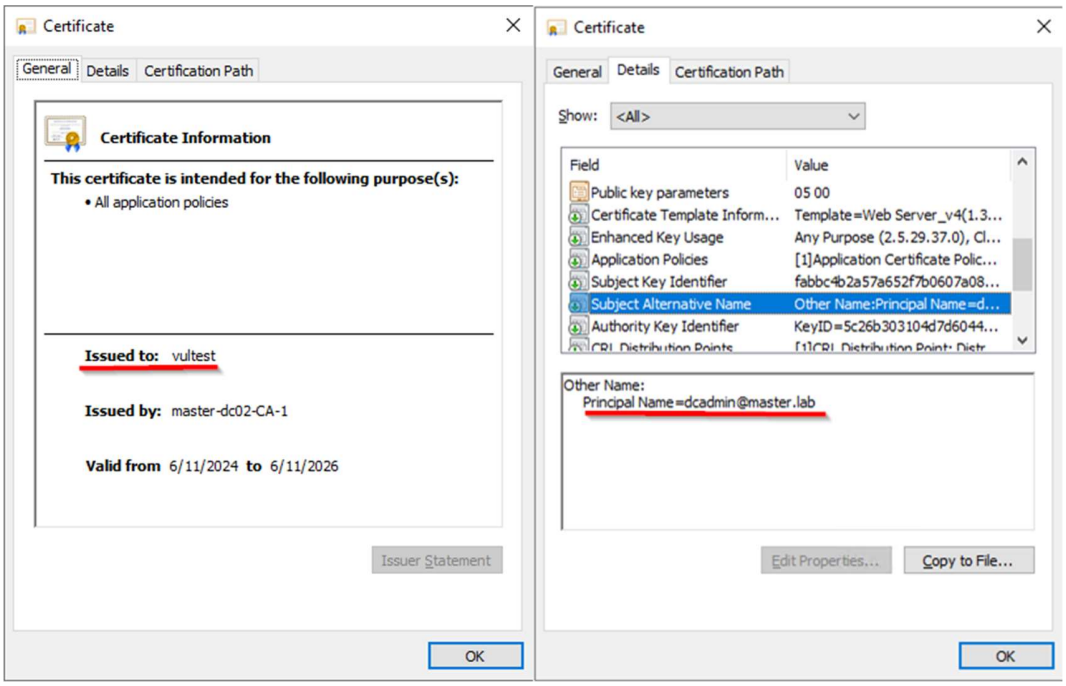
Naredbom ***Certify.exe request /ca:dc02.master.lab\master-dc02-CA-1 /template:WebServer_v4 /altname:dcadmin@master.lab*** je zatraženo izdavanje certifikata sa *WebServer_v4* predloška u ime korisnika *dcadmin@master.lab* , [26].

Slikom 17 je prikazano generiranje certifikata i privatnog ključa certifikata za korisnika *vultest*, te certifikat ima popunjeno polje *AltName* s imenom domenskog administratora *dcadmin*.

```
C:\Tools>Certify.exe request /ca:dc02.master.lab\master-dc02-CA-1 /template:WebServer_v4 /altname:dcadmin@master.lab

  _____          _   _  __
 / ____|        | | (_)/ _|
| |     ___ _ __| |_ _| |_ _   _
| |    / _ \ '__| __| |  _| | | |
| |___|  __/ |  | |_| | | | |_| |
 \_____\___|_|   \__|_|_|  \__, |
                            __/ |
                           |___./
  v1.0.0

[*] Action: Request a Certificates

[*] Current user context    : MASTER\vultest
[*] No subject name specified, using current context as subject.

[*] Template                : WebServer_v4
[*] Subject                 : CN=vultest, CN=Users, DC=master, DC=lab
[*] AltName                 : dcadmin@master.lab

[*] Certificate Authority   : dc02.master.lab\master-dc02-CA-1

[*] CA Response             : The certificate had been issued.
[*] Request ID              : 10

[*] cert.pem         :
```

Slika 18. Izdavanje certifikata u ime korisnika *dcadmin*

Dodatno, izdani certifikat je slikom 18 ispod prikazan grafički, gdje je vidljivo pod generalnim informacijama da je certifikat zatražio korisnik *vultest*, dok u detaljima certifikata u SAN polju se populirala vrijednost *PrincipalName=dcadmin@master.lab* koja omogućuje naknadno oponašanje admininstratora *dcadmin* prilikom autorizacije na domenski kontroler.



Slika 19. Grafički prikaz izdanog certifikata

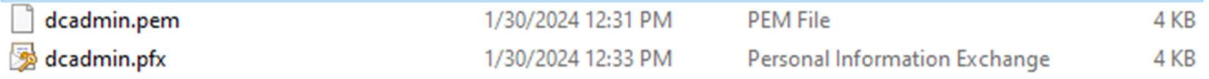
Certifikat je izdan u .pem (engl. *Privacy-Enhanced Mail* - PEM) formatu kojem je svrha pohrana i slanje kriptografskih ključeva, certifikata i drugih podataka, temeljen na skupu standarda IETF-a (engl. *The Internet Engineering Task Force*) iz 1993. Sveukupno, ova ekstenzija sadrži samo certifikat, dok je privatni ključ generiran zasebno. PEM format dodatno osigurava pohranu, kontrolu i upravljanje certifikatom jer je privatan ključ moguće izvesti samo na onom računalu na kojem je zatraženo izdavanje certifikata, [29]. Slikom 19 je prikazan skup simbola koji predstavljaju zasebno privatan ključ, te zasebno novoizdani certifikat.

Slika 20. Novokreirani certifikat i odgovarajući privatan ključ

Nakon što je certifikat s alternativnim imenom kreiran, skup simbola prikazan slikom iznad je potrebno spremiti u dokument s ekstenzijom .pem. Korištenjem alata *OpenSSL* je moguće pretvoriti certifikat iz .pem formata u .pfx format korištenjem iduće naredbe:

- ***openssl pkcs12 -in dcadmin.pem -keyex -CSP "Microsoft Enhanced Cryptographic Provider v1.0" -export -out dcadmin.pfx***, [30]

Slikom 20 je prikazan izgled dobivenih dokumenata pokretanjem naredbi prikazanih iznad.



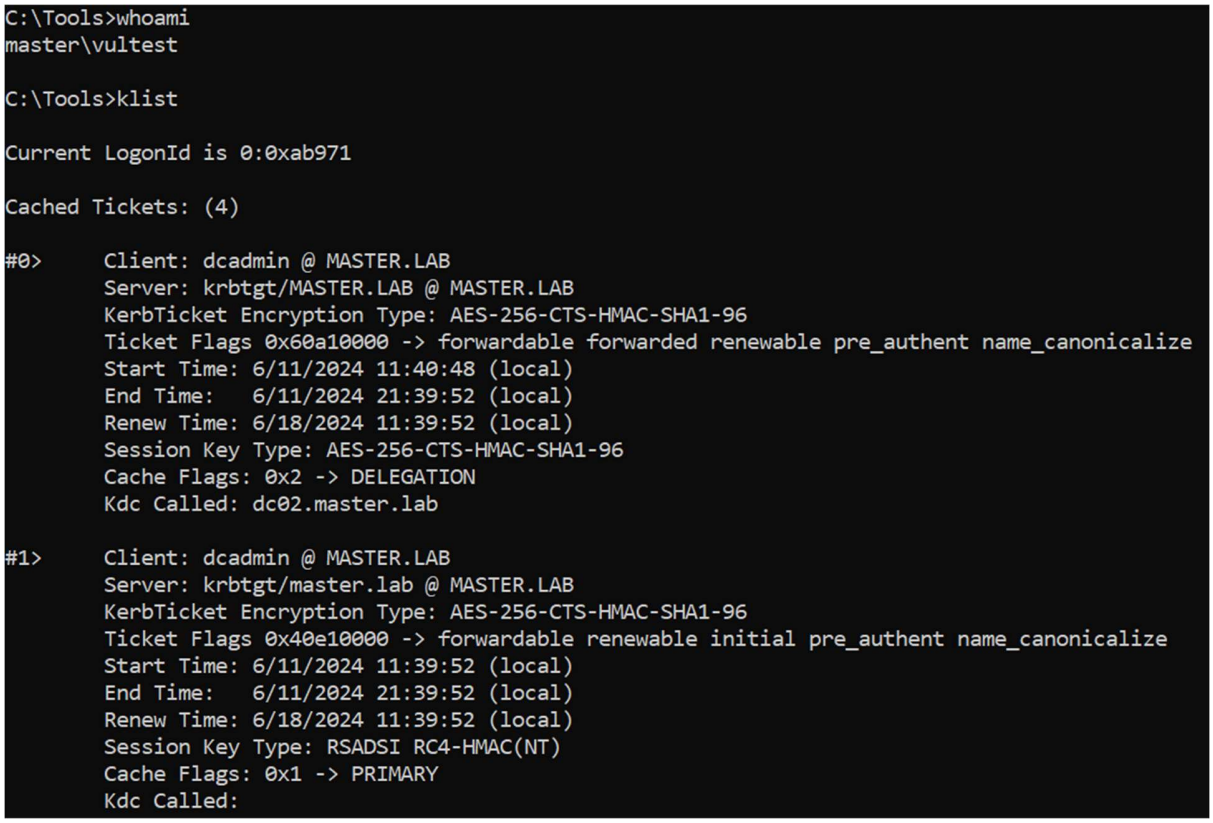
Slika 21. .PEM i .PFX datoteke

.PFX (engl. *Personal Information Exchange*) format, poznat pod imenom *PKCS#12*, certifikata sadrži i privatan ključ i certifikat, te će se taj format koristiti prilikom oponašanja administratorskog računa za povezivanje na domenski kontroler putem *Powershell* sesije, [30].

Idući korak zahtjeva korištenje alata Rubeus.exe kojim je moguće zatražiti takozvani krbtgt ulaznicu koji omogućuje predstavljanje korisnika kao administrator prilikom autorizacije na domenski kontroler, [31]. Slikom 21 je prikazano uspješno preuzimanje krbtgt ulaznice za korisnika *dcadmin* u domeni *master.lab*.

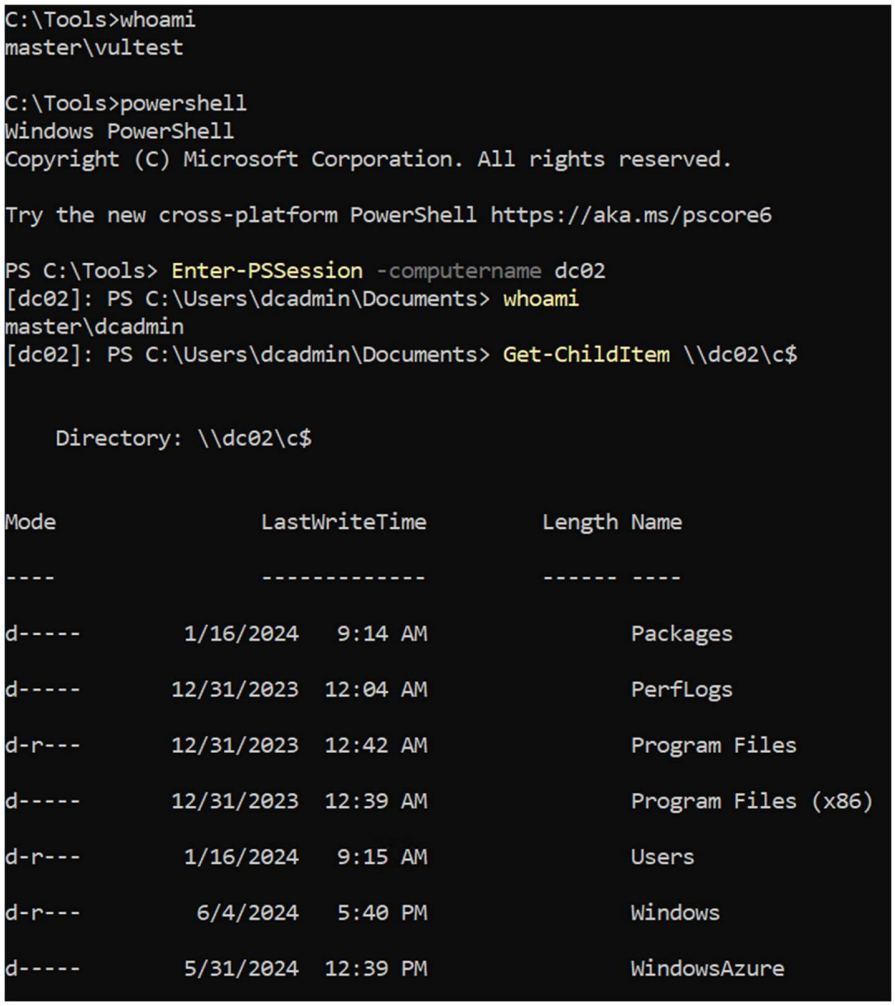
Slika 22. KRBTGT ulaznica za oponašanje domenskog admina dcadmin

Naredbom *klist* se dobiva informacija o trenutno aktivnim kerberos ulaznicama. Slikom 22 je prikazano kako trenutno autenticirani korisnik *vultest* raspolaže *kerberos* ulaznicama za administratora *dcadmin@master.lab*.



Slika 23. Naredba *klist*

Slikom 23 je dokazana elevacija prava napadom ESC1. Prvo je pokrenuta naredba *whoami* kojom je vidljivo da je trenutno aktivan korisnik *vultest*. Nakon pokretanja *powershell* sesije te spajanja na server dc02 naknadno je ponovno pokrenuta naredba *whoami* te je sad aktivan korisnik *dcadmin* koji ima mogućnost pristupanja disku C na domenskom kontroleru.



Slika 24. Dokaz elevacije prava napadom ESC1

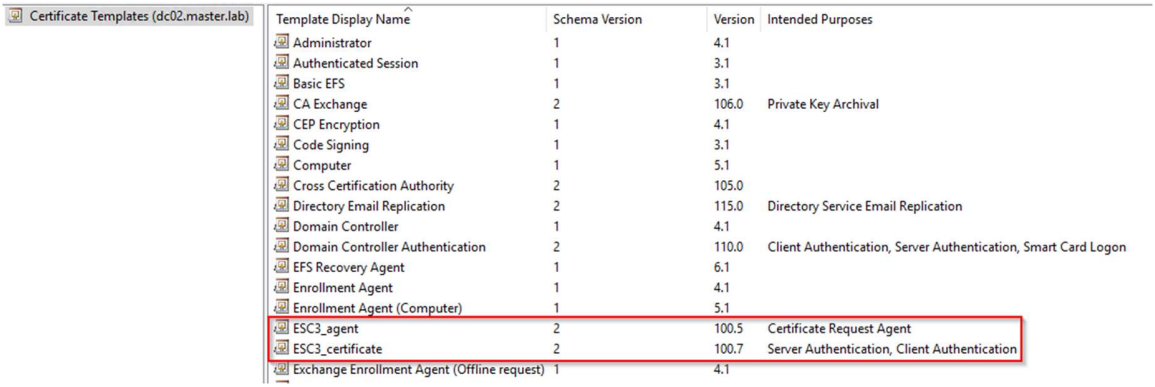
5.2. Analiza ESC3 napada

ESC3 napad je po velikom broju koraka identičan ESC1 napadu. Glavna razlika je u tome što se u ESC3 napadu koristi dodatan predložak koji ima mogućnost potpisivanja ostalih tipova certifikata, tj. Ima EKU vrijednost *Certificate Request Agent* koji je u Microsoftovoj dokumentaciji opisan kao tijelo koje ima mogućnost izdavanja certifikata u ime drugog korisnika, [32].

Da bi se pogrešna konfiguracija predloška uspješno iskoristila, moraju se zadovoljiti sljedeći uvjeti, [32]:

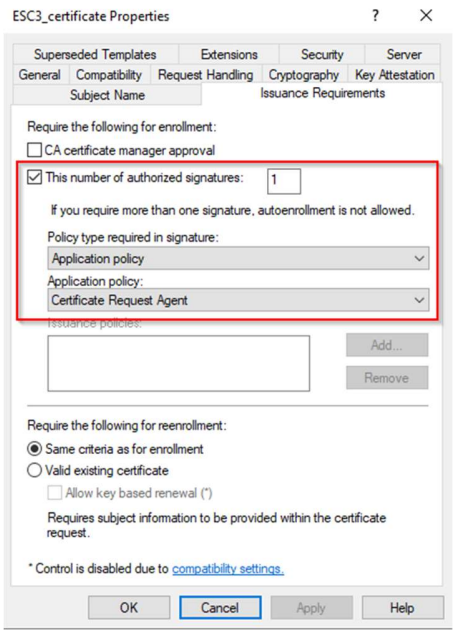
- Mogućnost izdavanja certifikata korisnicima s niskim pravima u domeni,
- Odobrenje upravitelja je onemogućeno,
- Nisu potrebni ovlašteni potpisi,
- Predložak certifikata uključuje *Certificate Request Agent* EKU, koji omogućuje zahtjev certifikata u ime drugih korisnika ili uređaja.

U svrhu odrađivanja napada ESC3 kreirana su dva nova predloška pod imenima *ESC3_agent* i *ESC3_certificate* kao što je vidljivo ispod u slici 24.



Slika 25. Novokreirani predlošci za ESC3 napad

ESC_agent predložak sadrži *Certificate Request Agent* EKU, dok je *ESC3_certificate* predložak definiran na način da certifikat može biti izdan jedino od korisnika koji raspolaže sa certifikatom koji je potpisan na predlošku *ESC3_agent*. Navedena karakteristika povezivanja funkcionalnosti certifikata se definira na krajnjem certifikatu, te je prikazano slikom 25, [32].

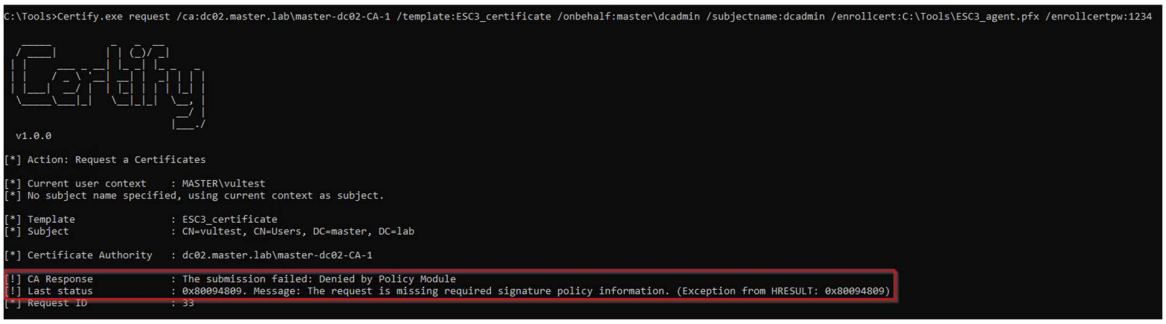


Slika 26. Postavke *ESC3_certificate* predloška

Nakon što je postavljena konfiguracija predložaka potrebnih za ESC3 napad, prvi korak je s alatom *certify.exe* zatražiti certifikat s predloška *ESC3_Agent*. S korisnikom *vultest* unutar CMD sučelja se pokreće naredba ***Certify.exe request /ca:dc02.master.lab\master-dc02-CA-1 /template:ESC3_agent*** kojom se dobije certifikat s predloška *ESC3_agent* što je vidljivo na slici 26, [33].

Slika 27. Izdavanje certifikata s predloška *ESC3_agent*

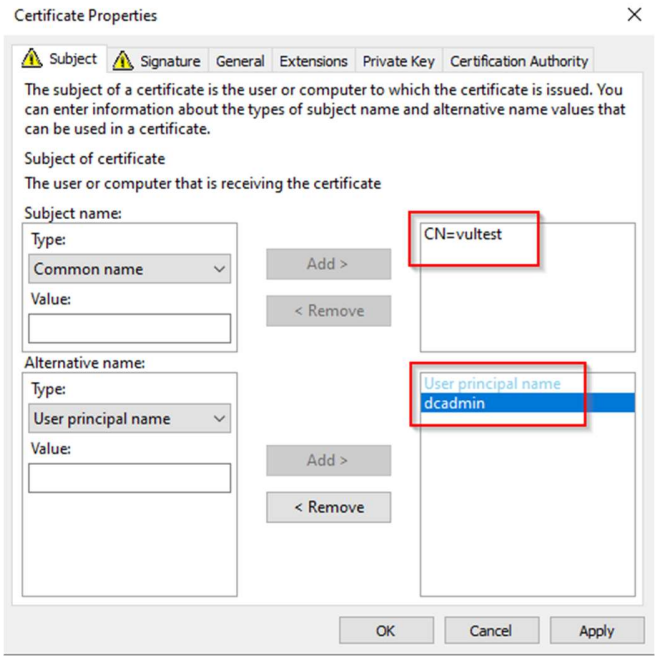
Budući da je konfiguracija predloška *ESC3_certificate* definirana na način da jedino korisnici s certifikatom izdanim s predloška *ESC3_agent* mogu zatražiti certifikat s predloška *ESC3_certificate*, idućom naredbom je dodana linija u kojoj se definira putanja certifikata *ESC3_agent*, te se forsira sustav da se certifikat izdaje u ime administratorskog računa *dcadmin*. Naredba koja će se koristiti je ***Certify.exe request /ca:dc02.master.lab\master-dc02-CA-1 /template:ESC3_certificate /onbehalf:master\dcadmin /enrollcert:C:\Tools\ESC3_agent.pfx /enrollcertpw:1234*** , što je prikazano slikom 27, [33].



Slika 28. Neuspješno izdavanje certifikata s predloška *ESC3_certificate*

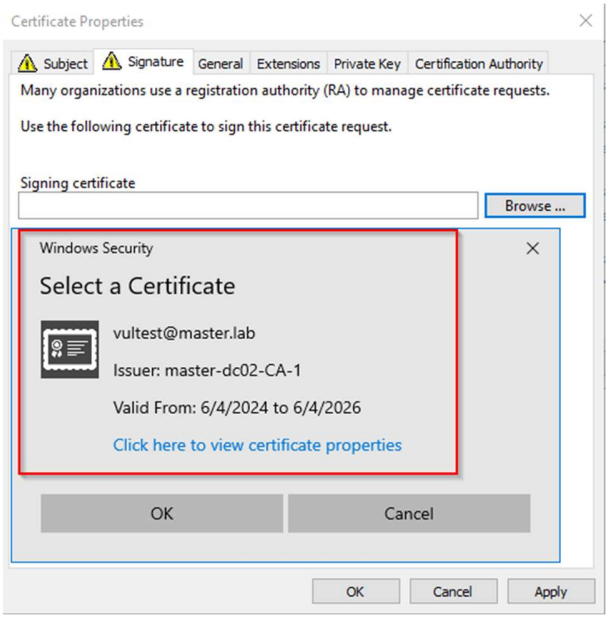
Pokušaj izdavanja certifikata s predloška *ESC3_certificate* je neuspješan s opisom problematike *Denied by Policy Module*. Istraženo je da je razlog odbijanja nemogućnost povezivanja funkcionalnosti dvaju certifikata izdanih sa *ESC3_agent* i *ESC3_certificate* predložaka. Idući pokušaj je izdavanje certifikata preko grafičkog sučelja gdje se ručno unose podaci o aktivnom računu *vultest*, te informacije o administratorskom računu *dcadmin* koji se pokušava oponašati. Slikom 28 prikazano je grafičko sučelje izdavanja certifikata, te sve informacije koje je potrebno unijeti kako bi se certifikat naknadno mogao iskoristiti prilikom oponašanja administratorskog računa. Informacije koje je potrebno unijeti prilikom izdavanja certifikata su [33]:

- Ime trenutnog korisnika (engl. *Common Name*),
- Glavno ime administratorskog računa (engl. *User principal name* - UPN),
- Lokacija certifikata *ESC3_agent* koji je nužan za izdavanje certifikata *ESC3_certificate*.



Slika 29. Grafički prikaz unošenja podataka prilikom izdavanja certifikata *ESC3_certificate*

Dodatno, slikom 29 je prikazano definiranje *ESC3_agent* certifikata prilikom zahtijevanja certifikata s predloška *ESC3_certificate*.

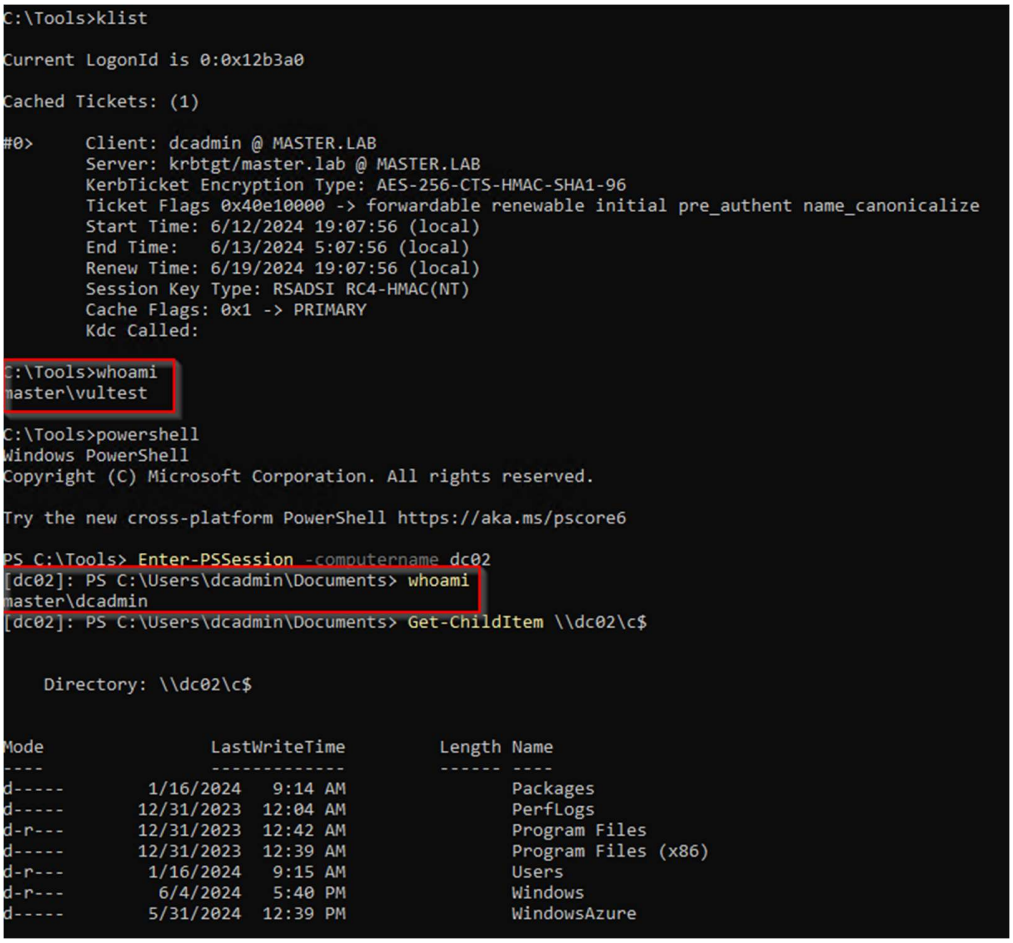


Slika 30. Dodavanje *ESC3_agent* certifikata prilikom izdavanja certifikata s predloška *ESC3_certificate*

Certifikat *ESC3_certificate* je uspješno izdan s definiranim SAN poljem u obliku *Principal Name=dcadmin*. Na kraju, certifikat je potrebno izvesti u .pfx oblik, te pomoću *Rubeus* alata zatražiti KRBTGT ulaznicu koja omogućuje pristup domenskom kontroleru koristeći administrativni račun *dcadmin*. Naredba korištena za dobivanje KRBTGT ulaznice je identična kao i u ESC1 napadu, a to je ***Rubeus.exe asktgt /user:"dcadmin" /certificate:"ESC3_certificate.pfx" /password:"1234" /ptt*** . Rezultat naredbe je prikazan slikom 30, [33].

Slika 31. Oponašanje administratorskog računa s KRBTGT ulaznicom

Za kraj napada, kao dokaz uspješnosti izvedenog, pokrenute su naredbe *klist* i *whoami*, te je uspješno pristupljeno domenskom kontroleru oponašajući administrativni račun *dcadmin*. Dokaz elevacije prava je prikazan slikom 31.



Slika 32. Elevacija prava napadom ESC3

6. Budući trendovi razvoja infrastrukture javnog ključa

Infrastruktura javnog ključa kontinuirano doživljava značajne promjene i inovacije kako bi odgovorila na sve složenije izazove suvremenog digitalnog svijeta. U ovom poglavlju istražuju se tri ključna aspekta koja oblikuju budući razvoj PKI-a, a to su napredak umjetne inteligencije, integracija *blockchain* tehnologije i uloga kvantne kriptografije, [34].

U pogledu umjetne inteligencije, istražuje se njezina sve veća primjena za automatizaciju procesa, analitiku i poboljšanje sigurnosti PKI sustava. Umjetna inteligencija omogućuje bržu i precizniju provjeru identiteta, autentikaciju korisnika i otkrivanje nepravilnosti u komunikaciji, čime se povećava efikasnost i pouzdanost PKI-a, [34].

Analizirat će se integracija *blockchain* tehnologije u PKI infrastrukturu koja donosi decentralizaciju, transparentnost i veću sigurnost od prijetnji. *Blockchain* omogućuje distribuiranu pohranu ključeva i certifikata, eliminirajući rizik od napada i stvarajući otpornost na neautorizirane promjene, [34].

Istražit će se uloga kvantne kriptografije u osiguravanju dugoročne sigurnosti PKI-a pred izazovima koje donosi razvoj kvantnih računala. Kvantna kriptografija koristi principe neodređenosti kvantne mehanike kako bi osigurala sigurnu razmjenu ključeva, čineći ih otpornima na kvantne napade koji bi mogli ugroziti tradicionalne kriptografske metode, [34].

Ovi ključni aspekti zajedno oblikuju budućnost PKI-a, osiguravajući sigurnu, transparentnu i inovativnu digitalnu budućnost u doba neprekidnog razvoja informacijskih tehnologija, [34].

6.1. PKI i umjetna inteligencija

U svijetu informacijskih tehnologija, jedna stvar je sigurna - nepredvidljivost. Brza evolucija tehnologije i stalni napredak umjetne inteligencije (engl. *Artificial Intelligence* - AI), zajedno s drugim inovacijama, oblikuju put napretka infrastrukture javnog ključa. Dok se PKI već godinama dokazuje kao nezaobilazan alat za osiguravanje digitalnih identiteta, potpisa i enkripcije, razvoj umjetne inteligencije i drugih tehnoloških alata donosi nove izazove i otvara vrata neočekivanim rješenjima, [35].

Uz razvoj umjetne inteligencije, predviđanje budućih trendova u infrastrukturi javnog ključa postaje sve izazovnije. AI donosi nove mogućnosti, ali i potencijalne sigurnosne prijetnje koje bi mogle zahtijevati inovativne pristupe u osiguravanju PKI sustava. Unatoč brojnim izazovima, postoje načini na koje će infrastruktura javnog ključa uspjeti popratiti razvoj umjetne inteligencije. AI će omogućiti optimizaciju i automatizaciju ključnih procesa u PKI sustavima, što će povećati učinkovitost i smanjiti potencijalne ljudske pogreške. Uz to, PKI će moći koristiti sposobnost umjetne inteligencije za otkrivanje i obranu od naprednih sigurnosnih prijetnji, kao što su krađa privatnih ključeva ili lažni identiteti, [35].

Nedavna istraživanja pokazuju da kibernetički napadači sve više koriste umjetnu inteligenciju za unapređenje svojih tehnika. Na primjer, [35]:

- Automatizacija zlonamjernih aktivnosti - Kibernetički kriminalci mogu koristiti generativnu umjetnu inteligenciju za stvaranje naprednog zlonamjernog softvera koji dinamički mijenja svoj kod ili ponašanje kako bi izbjegao detekciju. Ovi napredni oblici zlonamjernog softvera su teži za predvidjeti i kontrolirati, što značajno povećava rizik od široko rasprostranjenih sistemskih poremećaja i velikih narušavanja sigurnosti podataka,
- Napredni napadi socijalnog inženjeringa (engl. *Phishing attack*) - Generativna umjetna inteligencija može učiti i oponašati stil pisanja i osobne podatke korisnika, čime phishing napadi postaju znatno uvjerljiviji. Prilagođene phishing poruke, koje se čine kao da dolaze od pouzdanih kontakata ili uglednih institucija, mogu zavarati pojedince da otkriju osjetljive informacije, predstavljajući ozbiljnu prijetnju osobnoj i korporativnoj kibernetičkoj sigurnosti,
- Realistične digitalne manipulacije (engl. *deepfakes*): Generativna umjetna inteligencija omogućava zlonamjernim akterima stvaranje visoko uvjerljivih krivotvorina slika, zvuka i videa. *Deepfake*-ovi predstavljaju ozbiljan rizik za kampanje dezinformacija, prijevare i lažno predstavljanje.

S druge strane, PKI može pridonijeti u zaštiti od novih prijetnji koje su nastale dolaskom AI tehnologije. Skupina ključnih industrijskih subjekata, uključujući Adobe, Microsoft i DigiCert, ukazuje na razvoj standarda poznatog pod nazivom *Coalition for Content Provenance and Authenticity* (C2PA). Ova inicijativa je uvela otvoreni standard usmjeren na rješavanje izazova vezanih uz verifikaciju i autentifikaciju digitalnih datoteka. Korištenjem infrastrukture javnih ključeva, C2PA stvara neosporivi lanac dokazivanja, omogućujući korisnicima razlikovanje autentičnih medijskih sadržaja od onih krivotvorenih. Specifikacija ovog standarda omogućava korisnicima identifikaciju izvora, autora, datuma nastanka, lokacije i svih izmjena unutar digitalne datoteke. Primarni cilj ove norme je promicanje transparentnosti i pouzdanosti digitalnih medijskih datoteka, posebno u kontekstu rastućih izazova pri razlikovanju sadržaja generiranog umjetnom inteligencijom od stvarnog sadržaja, [35].

Umjetna inteligencija ima potencijal da bude primijenjena i kao sredstvo za izvršenje, ali i za obranu od kibernetičkih napada. AI može omogućiti sofisticirane napade, ali istovremeno pruža napredne alate za prevenciju i detekciju tih prijetnji. Međutim, presudno je da organizacije prepoznaju potencijalne rizike povezane s primjenom AI te odmah započnu s implementacijom odgovarajućih sigurnosnih mjera. Važno je napomenuti da, unatoč značajnom napretku AI tehnologije, ljudski faktor ostaje nezamjenjiv u cjelokupnom procesu upravljanja kibernetičkom sigurnošću, [35].

6.2. PKI i Blockchain tehnologija

Blockchain je tehnologija prezentirana tehnološkom svijetu 2008. godine. *Blockchain* predstavlja javni, nepromjenjivi registar koji se kontinuirano širi s novim zapisima. Svaki blok u

lancu sadrži zaglavlje, koje obično uključuje hash prethodnog bloka, vremensku oznaku i podatke o transakcijama. *Blockchain* funkcionira kao decentralizirana mreža zasnovana na *peer-to-peer* tehnologiji, koja se sastoji od punih i lakih čvorova. Lagani čvorovi pohranjuju samo zaglavlja blokova, dok puni čvorovi potvrđuju i distribuiraju nove transakcije te čuvaju cjelokupnu kopiju lanca blokova, [34].

Poslovanje se oslanja na precizne i pravovremene informacije. Što se brže i točnije informacije prenose, to je bolje za poslovne procese. *Blockchain* tehnologija je izuzetno pogodna za pružanje ovih informacija, jer omogućuje trenutan, zajednički i transparentan uvid u podatke pohranjene u nepromjenjivoj knjizi, kojoj mogu pristupiti samo ovlašteni članovi mreže. *Blockchain* mreža omogućava praćenje narudžbi, plaćanja, računa, proizvodnje i drugih poslovnih aktivnosti. Zahvaljujući zajedničkom pristupu istim podacima, svi članovi mreže imaju potpuni uvid u transakcije od početka do kraja, što povećava povjerenje i otvara nove mogućnosti za poboljšanje učinkovitosti, [37].

Glavne prednosti *Blockchain* tehnologije su, [37]:

- Tehnologija distribuirane knjige
  - Transakcije se bilježe jednom
  - Svi korisnici imaju ista prava pristupa
- Nepromjenjivost zapisa
  - Jednom zabilježena transakcija u zajedničkoj knjizi ne može biti izmijenjena ili izbrisana od strane nijednog sudionika
  - U slučaju greške prilikom transakcije unosi se nova transakcija koja poništava prethodnu, pri čemu obje transakcije ostaju dostupne za pregled
- Pametni ugovori
  - Skup pravila pohranjen na *Blockchain*-u
  - Automatsko izvršavanje
  - Specificira uvjete dogovorene između dva tijela, te nakon što se pravila ispune automatski izvršava ono što je ugovorom definirano.

Više od polovice svjetskih implementacija *blockchain* tehnologije koristi digitalne potpise. Ono što PKI donosi digitalnom potpisu je mogućnost provjere autentičnosti vlasništva ključa. *Blockchain* sam po sebi ne pruža tu funkcionalnost. S druge strane, *blockchain* doprinosi inovativnoj i distribuiranoj metodi stvaranja i održavanja nepromjenjivosti digitalne knjige. Iako *blockchain* ne garantira legitimitet unosa u blok ili identifikaciju sudionika transakcija u glavnoj knjizi, omogućuje sigurnost da podaci nisu izmijenjeni od trenutka zapisa, [38].

PKI omogućuje potpisivanje podataka koji se šalju, ali ne utječe na način pohrane tih podataka u različitim tvrtkama. Obično postoji više nepovezanih skladišta podataka, a komunikacija se odvija samo kada jedno od njih inicira kontakt, što ne osigurava dostupnost podataka u stvarnom vremenu. S druge strane, *blockchain* aktivno održava jedinstvenu kopiju podataka, kojom se upravlja putem konsenzusa potpisa između uključenih strana. Modifikacije podataka se definiraju i postaju dostupne svim sudionicima uz minimalan rizik od neovlaštenih

izmjena. U suštini, kombinacija *blockchain* tehnologije i PKI-a omogućuje učinkovitu koordinaciju i usklađenost između više organizacija, [38].

Budući da b*lockchain* i PKI sadrže prednosti koje su međusobno komplementarne, javlja se ideja o kombinaciji dvaju tehnologija i stvaranju b*lockchain* baziranog PKI okruženja. Izgradnja decentraliziranih PKI sustava korištenjem *blockchain* tehnologije uklanja potencijalne točke neuspjeha koje se javljaju pri korištenju certifikacijskih autoriteta. Ako su autoriteti ugroženi, cijeli lanci certifikata mogu biti kompromitirani. Osim toga, PKI baziran na *blockchain*-u, kao javni zapisnik koji omogućuje samo dodavanje podataka, inherentno pruža transparentnost certifikata, slično kao što je Google implementirao za poboljšanje sigurnosti PKI-a temeljenog na CA kroz javno evidentiranje i praćenje certifikata, [39].

PKI temeljen na blockchainu također nudi potencijalne prednosti u odnosu na PKI temeljen na WoT (engl. *Web of Trust*) modelu, gdje je uspostavljanje povjerenja značajna prepreka ulasku. Potrebni su veliki napori za izgradnju mreže koja može dokazati pouzdanost značajnom dijelu korisnika. U PKI sustavu temeljenom na blockchainu, entiteti ne zahtijevaju članove koji potvrđuju legitimnost mreže, čime se eliminira potreba implementiranja mrežno kompliciranih karakteristika kako bi se funkcioniralo kao dio mreže, [40].

6.3. PKI i kvantna kriptografija

U posljednjih nekoliko godina prijetnja kvantnih računala postala je sve značajnija. Brza obrada podataka koju omogućavaju kvantna računala ugrožava sigurnost sustava koji se oslanjaju na klasične kriptografske algoritme. Prema procjenama *Cloud Security Alliance*-a, 14. Travnja 2030. godine snaga kvantnih računala će biti takva da će moći kompromitirati današnje sigurnosne tehnologije koje se baziraju na kriptografiji. Ovdje se direktno odnosi na proboj ekripcija koje se danas koriste, poput AES (engl. *Advanced Encryption Standard*), RSA (engl. *Rivest-Shamir-Adleman*) i Diffie—Hellman enkripcije. Infrastruktura javnih ključeva oslanja se na asimetrične kriptografske algoritme i široko se koristi u mnogim sektorima, stoga je ključno osigurati njenu otpornost. Neophodno je zamijeniti tradicionalne kriptografske algoritme postkvantnim kriptografskim algoritmima ili hibridnim rješenjima, [41].

Brojne organizacije, poput Microsoft-a, IBM-a, Intel-a i raznih vladinih organizacija, aktivno rade na osposobljavanju kvantnog računala. Određeni tipovi kvantnih računala, koristeći kvantne algoritme poput Shorovog algoritma, [42], mogu brzo faktorizirati jednadžbe koje uključuju velike proste brojeve. Ove jednadžbe su temelj zaštite većine tradicionalnih kriptografskih sustava s javnim ključem. Dok tradicionalna binarna računala teško faktoriziraju velike proste brojeve, kvantna računala s dovoljno "qubita" mogu ovaj proces obaviti u vrlo kratkom vremenu, od nekoliko minuta do nekoliko dana, [41],

Potrebno je pripremiti se za budućnost pronalaženjem novih rješenja, poput integracije postkvantnih kriptografskih (engl. *Post-quantum cryptography* - PQC) algoritama, kako bi se osigurala otpornost na kvantna računala. Nacionalni institut za standarde i tehnologiju (engl. *National Institute of Standards and Technology* - NIST) pokrenuo je projekt standardizacije PQC algoritama s ciljem razvijanja sigurnih kvantno otpornih kriptografskih metoda koje mogu

zamijeniti klasične algoritme koji se trenutno koriste za autentifikaciju, sigurnu komunikaciju i prijenos podataka u različitim područjima, [43].

Postkvantni kriptografski sustavi mogu pružiti učinkovitu zaštitu protiv kompromitiranih kriptosustava. Stoga je ključni cilj u razvoju kvantno otpornog PKI-ja prijelaz s klasičnih asimetričnih kriptografskih algoritama na PQC algoritme. Međutim, ova nadogradnja zahtijeva značajno vrijeme i resurse. Kao prvi važan korak u osiguravanju informacijske i kibernetičke sigurnosti u postkvantnoj eri može se razmotriti korištenje hibridnih digitalnih certifikata. Ovo rješenje pruža dodatnu motivaciju za razvoj i implementaciju hibridnih shema, budući da nedavno razvijene PQC tehnike još nisu dovoljno dugo proučavane, te uspješni napadi mogu nastati u bilo kojem trenutku, što povećava rizik njihove nesigurnosti. U hibridnom pristupu, tradicionalni algoritam i jedan ili više postkvantnih algoritama koriste se paralelno. Ovo osigurava povjerljivost i autentičnost podataka sve dok barem jedan algoritam ostane siguran. Takva hibridna rješenja već su uvedena za PKI, a neka od njih su već u komercijalnoj upotrebi, [44].

Također je bitno uzeti u obzir da postkvantni algoritmi imaju specifične zahtjeve za pohranom i resursima, različite od klasičnih algoritama. Ovi algoritmi koriste znatno veće javne i privatne ključeve, koji moraju biti adekvatno pohranjeni unutar implementiranog sustava. Nadalje, zbog toga što se ove sheme oslanjaju na matematičke probleme i teoriju kodiranja za svoju sigurnost, njihova implementacija je računalno zahtjevnija i dugotrajnija. Razlike u složenosti između postkvantnih i klasičnih algoritama mogu biti značajne. Neke aplikacije koje trenutno koriste PKI zahtijevat će opsežan redizajn za primjenu PQC algoritama, dok su druge aplikacije već kompatibilne s kvantno sigurnim algoritmima u svom trenutnom obliku, [44].

Enkripcija korištena u protokolu TLS je posebno izložena prijetnjama kvantnih računala, ali se pokazuje kao dobro prilagođena za integraciju kvantno otpornim algoritmima i hibridnim rješenjima koja mogu ublažiti te prijetnje. TLS omogućuje jednostavnu integraciju postkvantnih algoritama budući da TLS strukture podataka podržavaju certifikate veličine do 16,7MB. Postkvantna razmjena ključeva je već uvedena u pregovorima koji podržavaju transportne protokole i korištena je u komercijalnim aplikacijama poput *OpenSSL open-source* alata koji je korišten u ovom radu prilikom proboja PKI sustava, [43].

6.4. PKI i homomorfna kriptografija

Napredak u tehnologijama šifriranja značajno je poboljšao sigurnost dijeljenja i pohrane podataka. Ipak, tradicionalne sheme šifriranja suočavaju se s ograničenjima u primjeni unutar računalstva u oblaku, što otvara potencijalne sigurnosne rizike. Zbog tih, ali i drugih čimbenika, stručnjaci u područjima telekomunikacija i kibernetičke sigurnosti sve više usmjeravaju pozornost na razvoj homomorfne enkripcije, [45].

Homomorfni sustavi šifriranja omogućuju analizu i obradu podataka izravno na šifriranom tekstu, bez potrebe za dešifriranjem osnovnih podataka. Na taj način, šifrirani podaci ostaju

zaštićeni tijekom obrade, što pruža dodatni sloj sigurnosti u okruženjima računalstva u oblaku, [45].

Slično kao i kod tradicionalne enkripcije, homomorfne sheme šifriranja koriste javni ključ za šifriranje podataka. Međutim, za razliku od tradicionalnih metoda, homomorfni kriptosustavi primjenjuju naprednije matematičke algoritme kako bi osigurali otpornost podataka na potencijalne napade, [45].

Tradicionalne metode šifriranja, poput AES i RSA kriptosustava, prepoznate su kao učinkoviti i sigurni sustavi za pohranu šifriranih podataka. Iako su pouzdani, ovi sustavi suočavaju se s izazovima kada je riječ o obradi i pristupu pohranjenim podacima, što može ugroziti sigurnost u određenim scenarijima, [45].

Nasuprot tome, homomorfna enkripcija, iako se oslanja na složenije algoritme, omogućuje lakši pristup podacima. Primjerice, poslužitelj u oblaku može izvoditi operacije nad šifriranim podacima i izravno vratiti šifrirane rezultate vlasniku podataka. Ovaj pristup eliminira potrebu za dešifriranjem podataka tijekom obrade, čime se uklanjaju potencijalne sigurnosne slabosti u komunikaciji između vlasnika podataka i poslužitelja, [45].

Prednosti homomorfnih sustava su, [45]:

- Očuvanje privatnosti podataka bez ometanja funkcionalnosti i obrade,
- Kvalitetno rješenje za problematiku sigurnosti zajedničkog dijeljenja podataka,
- Nadilazi sigurnosna rješenja u mobilnom rubnom računarstvu zbog heterogenosti podataka, te njihove obrade,
- složeni matematički problemi koji se koriste u homomorfnoj enkripciji do sada nisu riješeni, što ovu tehnologiju čini gotovo neprobojnim čak i za kvantna računala.

Nedostaci navedenih sustava više proizlaze iz aspekta standardizacije i obrazovanja zaposlenika nego iz samih kriptografskih metoda. S kriptografske perspektive, glavni nedostatak je nemogućnost određivanja korisničkih odnosa, što zahtijeva obrnuti inženjering kako bi se ta informacija razumjela koji u ovakvom sustavu nije lako izvediv, [45].

7. Zaključak

Sigurnosni aspekti infrastrukture javnog ključa (PKI) unutar Microsoft Windows okruženja igraju ključnu ulogu u osiguravanju integriteta, povjerljivosti i autentičnosti digitalnih podataka. Ovaj rad je detaljno istražio različite aspekte PKI-a, uključujući tehničku implementaciju, praktičnu primjenu te sigurnosne prijetnje i izazove koje mogu ugroziti integritet sustava. Poseban fokus stavljen je na primjenu Active Directory Certificate Services (AD CS) kao temeljnog dijela Microsoft Windows infrastrukture.

Kroz istraživanje i analizu provedenih sigurnosnih proboja otkriveno je da, unatoč visokom stupnju sigurnosti koje PKI nudi, postoje specifične ranjivosti koje treba pažljivo adresirati. Identificirani su ključni sigurnosni rizici, uključujući loše upravljanje certifikatima, softverske ranjivosti te prijetnje socijalnog inženjeringa. Preporučene su mjere zaštite koje obuhvaćaju stroge sigurnosne politike, redovita ažuriranja sustava, edukaciju korisnika i implementaciju dodatnih sigurnosnih mehanizama kao što su multifaktorska autentifikacija i revizija sigurnosnih logova.

Budući trendovi u razvoju PKI-a pokazuju napredak u automatizaciji upravljanja certifikatima, integraciji s tehnologijama poput umjetne inteligencije i strojnog učenja te poboljšanje sigurnosnih standarda. Organizacije koje koriste Microsoft Windows trebaju kontinuirano pratiti ove trendove i prilagođavati svoje PKI sustave kako bi osigurale maksimalnu sigurnost i učinkovitost.

U zaključku, PKI na Microsoft Windows platformi pruža robustan okvir za osiguranje digitalne komunikacije i podataka, ali zahtijeva pažljivu implementaciju i upravljanje. Kontinuirana edukacija, redovita ažuriranja i prilagodba sigurnosnih politika ključni su za održavanje visokog stupnja sigurnosti u suočavanju sa sve sofisticiranijim cyber prijetnjama.

Literatura

[1] Boldyreva, A., Fischlin, M., Palacio, A., Warinschi, B. Closer Look at PKI: Security and Efficiency. U: Okamoto, T., Wang, X. (ur.) *Public Key Cryptography – PKC 2007.* Berlin: Springer; 2007. pp. 458-475.

[2] Bosworth, K.P., Tedeschi, N. Public Key Infrastructures — the Next Generation. *BT Technology Journal*. 2001;19(2): 44–59. Preuzeto sa: https://doi.org/10.1023/A:1011982014166 [Pristupljeno: Travanj 2023.]

[3] A. Jain, G. Khare, A. Rajan, N. Manjhi, D. Pathy and A. Rawat. Implementation issues and challenges with PKI infrastructure and its integration with in-house developed IT applications. U: *2014 Conference on IT in Business, Industry and Government (CSIBIG)*. Indore: IEEE; 2014. pp. 1-5.

[4] D. E. Sintyaningrum, Muladi and M. Ashar. The Encryption of Electronic Professional Certificate by Using Digital Signature and QR Code. U: *2021 International Conference on Converging Technology in Electrical and Information Engineering (ICCTEIE)*. Bandar Lampung: IEEE; 2021. pp. 19-24.

[5] Digital signatures and certificates. *Microsoft* Preuzeto s: https://support.microsoft.com/en-us/office/digital-signatures-and-certificates-8186cd15-e7ac-4a16-8597-22bd163e8e96#:~:text=A%20digital%20signature%20is%20an,%2C%20macros%2C%20or%20electronic%20documents [Pristupljeno Lipanj 2023.]

[6] *FINA.* Preuzeto s: https://www.fina.hr/sto-je-to-digitalni-certifikati [Pristupljeno: Lipanj 2023.]

[7] Goldwasser S., Micali S. i Rivest R. A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks. *SIAM J. Comput*. 1998;17(2): 281-307 Preuzeto sa: https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/Digital%20Signatures/A_Digital_Signature_Scheme_Secure_Against_Adaptive_Chosen-Message_Attack.pdf [Pristupljeno: Travanj 2023.]

[8] *Cloudflare.* Preuzeto s: https://www.cloudflare.com/learning/ssl/what-is-encryption/ (Pristupljeno: Lipanj 2023)

[9] A. Rojanapasakorn and C. Sathitwiriyawong. A performance study of over-issuing delta-CRLs with distribution points. *18th International Conference on Advanced Information Networking and Applications*. Fukuoka: AINA; 2004. pp. 178-181.

[10] A. Jain, G. Khare, A. Rajan, N. Manjhi, D. Pathy and A. Rawat. Implementation issues and challenges with PKI infrastructure and its integration with in-house developed IT applications. *2014 Conference on IT in Business, Industry and Government (CSIBIG).* Indore: IEEE; 2014, pp. 1-5.

[11] *AWS.* Preuzeto s: https://aws.amazon.com/what-is/ssl-certificate/ [Pristupljeno: Lipanj 2023.]

[12] *kenwalger.com.* Preuzeto s: https://www.kenwalger.com/blog/tag/openssl/ [Pristupljeno: Lipanj 2023.]

[13] *Fortinet.* Preuzeto s: https://www.fortinet.com/resources/cyberglossary/what-is-a-vpn [Pristupljeno: Lipanj 2023.]

[14] *GlobalSign.* Preuzeto s: https://www.globalsign.com/en/blog/using-digital-certificates-for-mobile-authentication [Pristupljeno: Lipanj 2023.]

[15] *Digicert* Preuzeto s: https://www.digicert.com/resources/solution-brief/why-digital-certificates-are-essential-for-managing-mobile-devices-05-04-20.pdf [Pristupljeno: Lipanj 2023.]

[16] A. Jain, G. Khare, A. Rajan, N. Manjhi, D. Pathy and A. Rawat. Implementation issues and challenges with PKI infrastructure and its integration with in-house developed IT applications. U: *2014 Conference on IT in Business, Industry and Government (CSIBIG).* Indore: IEEE; 2014, pp. 1-5

[17] L. Leinweber, F. G. Wolff, C. Papachristou and F. L. Merat. A minimal protocol with public key cryptography for identification and privacy in RFID tags. U: *2009 International Symposium on Signals, Circuits and Systems.* Iasi: IEEE, 2009, pp. 1-4

[18] *Encryption Consulting.* Preuzeto s: https://www.encryptionconsulting.com/cloud-based-public-key-infrastructure-architecture/ [Pristupljeno: Rujan 2024.]

[19] *Microsoft*. Preuzeto s: https://learn.microsoft.com/en-us/mem/intune/protect/microsoft-cloud-pki-overview [Pristupljeno: Rujan 2024.]

[20] *TimothyGruber.* Preuzeto s: https://timothygruber.com/pki/deploy-a-pki-on-windows-server-2016-part-1/ [Pristupljeno: Listopad 2023.]

[21] *Microsoft.* Preuzeto s: https://techcommunity.microsoft.com/t5/ask-the-directory-services-team/designing-and-implementing-a-pki-part-iii-certificate-templates/ba-p/397860 [Pristupljeno: Listopad 2023.]

[22] *ScienceDirect.* Preuzeto s: https://www.sciencedirect.com/topics/computer-science/certificate-template#:~:text=Computer%20Certificate%20Templates%20are%20intended,computer%20certificates%20for%20EAP%20authentication. [Pristupljeno: Listopad 2023.]

[23] *Encryption Consulting.* Preuzeto s: https://www.encryptionconsulting.com/understanding-active-directory-certificate-services-containers-in-active-directory/ [Pristupljeno: Listopad 2023.]

[24] *Encryption. Consulting.* Preuzeto s: https://www.encryptionconsulting.com/ports-required-for-active-directory-and-pki/ [Pristupljeno: Listopad 2023.]

[25] *ADSecurity.* Preuzeto s: https://adsecurity.org/?p=4056 [Pristupljeno: Studeni 2023.]

[26] *HackTricks.* Preuzeto s: https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/ad-certificates/domain-escalation [Pristupljeno: Travanj 2024.]

[27] *HideAndSec.* Preuzeto s: https://hideandsec.sh/books/cheatsheets-82c/page/active-directory-certificate-services [Pristupljeno: Travanj 2024.]

[28] *Worksoft.* Preuzeto s: https://docs.worksoft.com/Worksoft_Certify/Certify_Process_Execution_and_Results/Getting_Started/Understanding_Certify.exe.htm [Pristupljeno: Travanj 2024.]

[29] *GeeksForGeeks.* Preuzeto s: https://www.geeksforgeeks.org/privacy-enhanced-mail-pem-and-its-working/ [Pristupljeno: Travanj 2024.]

[30] *IBM.* Preuzeto s: https://www.ibm.com/support/pages/node/356111?mhsrc=ibmsearch_a&mhq=%26period%3Bpem%20%26period%3Bpfx [Pristupljeno: Travanj 2024.]

[31] *Microsoft.* Preuzeto s: https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=HackTool:Win64/Rubeus&threatId=-2147123253#:~:text=Rubeus%20is%20a%20command%2Dline,pass%2Dthe%2Dticket%20attacks. [Pristupljeno: Travanj 2024.]

[32] *SpecterOps.* Preuzeto s: https://posts.specterops.io/certified-pre-owned-d95910965cd2 [Pristupljeno: Svibanj 2024.]

[33] *HideAndSec.* Preuzeto s: https://hideandsec.sh/books/cheatsheets-82c/page/active-directory-certificate-services [Pristupljeno: Svibanj 2024.]

[34] *Acmetek.* Preuzeto s: https://www.acmetek.com/the-future-of-pki-emerging-trends-and-innovations-shaping-cybersecurity/ [Pristupljeno: Lipanj 2024.]

[35] *Digicert.* Preuzeto s: https://www.digicert.com/blog/the-future-role-of-ai-in-cybersecurity [Pristupljeno: Lipanj 2024.]

[36] *Medium.* Preuzeto s: https://medium.com/seminal/public-key-infrastructure-using-blockchain-technology-eeda83fa8df4 [Pristupljeno: Srpanj 2024.]

[37] *IBM.* Preuzeto s: https://www.ibm.com/topics/blockchain#:~:text=Blockchain%20is%20a%20shared%2C%20immutable,patents%2C%20copyrights%2C%20branding). [Pristupljeno: Srpanj 2024.]

[38] A. Singla and E. Bertino. Blockchain-Based PKI Solutions for IoT. U:*2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC).* Philadelphia: IEEE; 2018, pp. 9-15

[39] *Google*. Preuzeto s: https://docs.google.com/document/d/1FP5J5Sfsg0OR9P4YT0q1dM02iavhi8ix1mZlZe_z-ls/edit [Pristupljeno: Srpanj 2024.]

[40] Axon, L., and M. Goldsmith. PB-PKI: a Privacy-Aware Blockchain-Based PKI. U:*14th International Conference on Security and Cryptography (SECRYPT 2017)*. Oxford: SCITEPRESS; 2016, pp. 56-64

[41] *Cloud Security Alliance.* Preuzeto s: https://cloudsecurityalliance.org/research/topics/quantum-safe-security [Pristupljeno: Srpanj 2024.]

[42] *QuTech Academy*. Preuzeto s: https://www.qutube.nl/quantum-algorithms/shors-algorithm [Pristupljeno: Srpanj 2024.]

[43] Alagic, G. , Cooper, D. , Dang, Q. , Dang, T. , Kelsey, J. , Lichtinger, J. , Liu, Y. , Miller, C. , Moody, D. , Peralta, R. , Perlner, R. , Robinson, A. , Smith-Tone, D. and Apon, D. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. U: *NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD* [Pristupljeno: Srpanj 2024.] Preuzeto sa: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413-upd1.pdf

[44] *KeyFactor.* Preuzeto s: https://www.keyfactor.com/blog/preparing-for-a-quantum-world-examining-the-migration-path-of-hybrid-certificates/ [Pristupljeno: Srpanj 2024.]

[45] *KeyFactor*. Preuzeto s: https://www.keyfactor.com/blog/what-is-homomorphic-encryption/ [Pristupljeno: Rujan 2024.]

Popis slika

Popis kratica

PKI	(Public Key Infrastructure) infrastruktura javnog ključa
ANSI	(American National Standards Institute) Američki nacionalni institut za standarde
CA	(Certificate Authority) certificirajuće tijelo
SSL	(Secure Sockets Layer) metoda kriptiranja *web* prometa
CRL	(Certificate revocation list) lista povučenih certifikata
OCSP	(Online Certificate Status Protocol) protokol za provjeru statusa aktivnih certifikata
SCVP	(Simple Certificate Validation Protocol) protokol za jednostavnu validaciju certifikata
QR-CODE	(Quick Response code) kod s brzom provjerom
FINA	Financijska agencija
HTTP	(Hypertext Transfer Protocol) protokol za prijenos informacija na *web*-u
CDP	(Certificate Distribution Point) točka izdavanja certifikata
HTTPS	(Hypertext transfer protocol secure) protokol za kriptiranu komunikaciju
GDPR	(General Data Protection Regulation) opća uredba o zaštiti podataka
SSL/TLS	(Secure Sockets Layer/Transport Layer Security) protokoli za kriptiranu razmjenu informacija
OSI	(Open Systems Interconnection) model za arhitekturu mreže
TCP/IP	(Transmission Control Protocol/Internet Protocol) model za arhitekturu mreže
VPN	(Virtual Private Network) virtualna privatna mreža
Wi-Fi	(Wireless Fidelity) bežično umrežavanje
MDM	(Mobile Device Management) upravljanje mobilnim uređajima
EMM	(Enterprise Mobility Management) upravljanje mobilnošću poduzeća
IoT	(Internet of Things) internet stvari
MQTT	(Message Queuing Telemetry Transport) telemetrijski prijenos poruka u redu čekanja
CoAP	(Constrained Application Protocol) protokol ograničene aplikacije
REST	(Representational State Transfer) prijenos reprezentativnog stanja

BLE	(Bluetooth Low Energy) niskoenergetski *Bluetooth*
LoRa	(Long Range Wide Area Networking) mreža velikog dometa
ADCS	(Active Directory Certificate Services) usluge certifikata aktivnog direktorija
Mmc	(Microsoft management center) *Microsoft*-ovo upravljačko središte
KDC	(Key distribution center) centar za distribuciju ključeva
OID	(Object Identifier) identifikator objekta
AIA	(Authority Information Access) pristup informacijama o ovlasti
CDP	(Certificate Revocation List Distribution Point) točka distribucije popisa opozvanih certifikata
KRA	(Key Recovery Agent) agent za oporavak ključeva
RPC	(Remote Procedure Call) protokol za poziv udaljene procedure
TGT	(Ticket-Granting Ticket) ulaznica za izdavanje ulaznica
NTLM	(New Technology LAN Manager) kriptografski format
TGS	(Ticket-Granting Service) usluga za izdavanje ulaznica
TTL	(Time to Leave) vrijednost trajanja *DNS* zapisa
PAC	(Privileged Attribute Certificate) certifikat s privilegiranim atributima
SAN	(Subject Alternative Name) alternativno ime subjekta
EKU	(Extended Key Usage) proširena funkcionalnost ključa
CSR	(Certificate signing request) zahtjev za potpisivanjem certifikata
DNS	(Domain Name System) servis za prevođenje IP adresa
AltName	(Alternative Name) alternativno ime
PEM	(Privacy-Enhanced Mail) elektronička pošta s poboljšanom privatnošću
IETF	(Internet Engineering Task Force) radna grupa za internetsko inženjerstvo
PFX	(Personal Information Exchange) ekstenzija za osobnu razmjenu informacija
UPN	(User Principal Name) glavno ime korisnika
AI	(Artificial Intelligence) umjetna inteligencija
C2PA	(Coalition for Content Provenance and Authenticity) koalicija za porijeklo i autentičnost sadržaja
WoT	(Web of Trust) decentralizirani sustav provjere identiteta

PQC	(Post-quantum cryptography) postkvantna kriptografija
NIST	(National Institute of Standards and Technology) nacionalni institut standarda i tehnologije

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad (*vrsta rada*) isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom Sigurnosni aspekti infrastrukture javnog ključa na arhitekturi Microsoft Windows, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 11.09.2024.

Antun Mlinar
(ime i prezime, *potpis*)