Primjena kriptografskih tehnika u IoT-u

Žarinac, Zvonimir

VELEUČILIŠTE U BJELOVARU
PREDDIPLOMSKI STRUČNI STUDIJ RAČUNARSTVO

PRIMJENA KRIPTOGRAFSKIH TEHNIKA U IoT-U

Završni rad br. 12/RAČ/2021

Zvonimir Žarinac

Bjelovar, rujan 2021.

obrazac ZR - 001

Veleučilište u Bjelovaru

Trg E. Kvaternika 4, Bjelovar

1. DEFINIRANJE TEME ZAVRŠNOG RADA I POVJERENSTVA

Kandidat: **Žarinac Zvonimir** Datum: 01.09.2021. Matični broj: 001999

JMBAG: 0314020054

Kolegij: **SIGURNOST RAČUNALA I PODATAKA**

Naslov rada (tema): **Primjena kriptografskih tehnika u IoT-u**

Područje: **Tehničke znanosti** Polje: **Računarstvo**

Grana: **Programsko inženjerstvo**

Mentor: **Dario Vidić, mag.ing.el.techn.inf.** zvanje: **predavač**

Članovi Povjerenstva za ocjenjivanje i obranu završnog rada:

1. **Ivan Sekovanić, mag.ing.inf.et comm.techn., predsjednik**
2. **Dario Vidić, mag.ing.el.techn.inf., mentor**
3. **Krunoslav Husak, dipl.ing.rač., član**

2. ZADATAK ZAVRŠNOG RADA BROJ: 12/RAČ/2021

U radu će se prikazati primjena TLS enkripcije u komunikaciji s jednostavnim IoT uređajem (ESP8266 s DHT11 senzorom) u tri najčešće rabljena protokola za IoT: prikaz web sučelja/REST API putem HTTPS protokola, prikaz podataka putem MQTT protokola te slanje obavijesti, odnosno logova e-poštom putem SMTP protokola. U svrhu demonstracije složena je Windows domena s domenskim poslužiteljem, DNS poslužiteljem, CA poslužiteljima (root i intermediate) koji čine PKI infrastrukturu za izdavanje certifikata te Exchange 2016 poslužiteljem e-pošte. Mikroupravljač će se programirati koristeći Arduino IDE okružje.

Zadatak uručen: 01.09.2021. Mentor: **Dario Vidić, mag.ing.el.techn.inf.**

REPUBLIKA HRVATSKA VELEUČILIŠTE U BJELOVARU BJELOVAR

Sadržaj

1. UVOD

21. stoljeće karakteristično je po iznimnom rastu proširenosti i dostupnosti tehnologije, uz istovremeni pad cijene uređaja te rast brzine istih. Jedna od najbrže rastućih tehnologija upravo je IoT (engl. *Internet of Things*).

IoT uređaji osmišljeni su kako bi se svakodnevnim kućnim pomagalima, poput štednjaka, perilice rublja ili garažnih vrata, omogućio pristup na Internet te mogućnost obrade podataka i udaljenog upravljanja koristeći ugradbeni mikroupravljač, odnosno mikroračunalo ili više njih, kojim se najčešće upravlja pomoću aplikacije na pametnom telefonu.

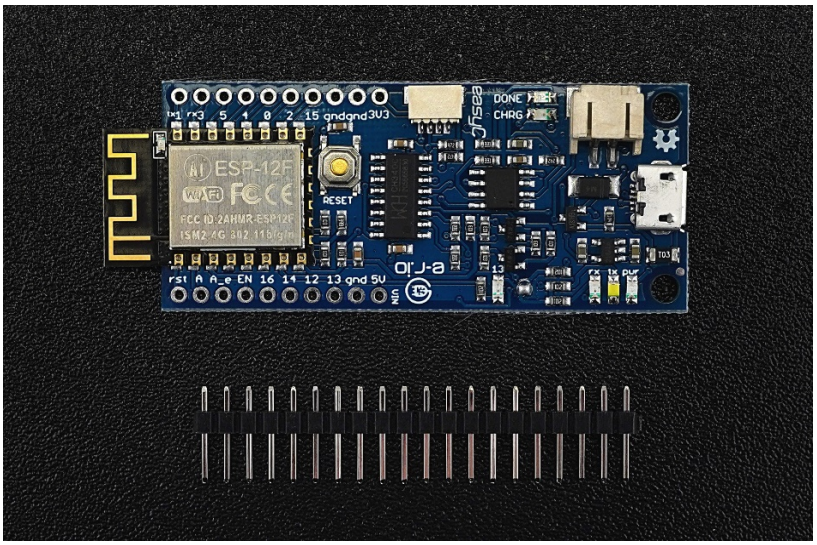
U procesu dizajna ugradbenog IoT rješenja, u obzir se moraju uzeti cijena, brzina i potrošnja energije, kako bi cijena dizajniranja uređaja, potrošnja energije i sredstva potrebna za implementaciju i održavanje sustava bili što niži, što utječe i na ukupnu cijenu vlasništva (engl. *Total Cost of Ownership*). Ukupna cijena vlasništva predstavlja cijenu rješenja, odnosno uređaja, zbrojenu s troškovima održavanja tijekom životnog vijeka uređaja ili rješenja. Prema statistici internetske stranice Statista, procjenjuje se da će broj veza IoT uređaja na mobilnim mrežama s trenutnih 12.4 milijardi veza porasti na 26.4 milijardi veza 2026. godine, što je rast od 113%. [1]

Vrijednost svjetskog tržišta IoT industrije sa 130 milijardi američkih dolara 2021. godine prema prognozi konzultantske tvrtke GlobalData porast će 2023. godine na čak 318 milijardi američkih dolara. [2] Uzimajući u obzir da sve više kako kućanskih, tako i sigurnosnih uređaja, poput pametnih brava, koristi IoT rješenja kao jezgru funkcionalnosti, potrebno je obratiti pažnju na sigurnost i pouzdanost IoT rješenja tijekom planiranja i dizajniranja u svrhu sprečavanja sigurnosnih napada na uređaje od izričite povjerljivosti, poput pametnih nadzornih kamera, te smanjenje potencijalnog poslovnog rizika, odnosno reputacije i financijskog rizika u slučaju potrebe isplate odštete kako za korisnika, tako i proizvođača IoT rješenja. U ovom radu demonstrirana je implementacija kriptiranja komunikacije s IoT uređajem i to u slučaju tri vrlo često korištena protokola: HTTPS, MQTT i SMTP.

2. DEFINICIJA POJMA INTERNET STVARI

Pojam Internet stvari opisuje mrežu fizičkih predmeta, odakle dolazi pojam „stvari“, u što spadaju predmeti od svakodnevnih kućanskih aparata, poput perilice rublja ili usisivača, sve do kompleksnih industrijskih strojeva i alata, poput tvornica automobila ili tvornica prehrambenih proizvoda, koji postaju dijelom mreže Internet stvari zahvaljujući ugrađenim senzorima i aktuatorima, ugradbenom sklopovlju i pristupu na Internet putem žične ili bežične veze, što omogućuje udaljeno upravljanje uređajem i obradu podataka izrađenih na uređaju ili skupljenih s uređaja.

IoT rješenje sastoji se od uređaja, poput kućanskog aparata ili industrijskog stroja, te od ugradbenog mikroupravljača, odnosno mikroračunala s pripadajućim senzorima i aktuatorima. Mikroupravljač koji će se koristiti u ovom radu je ESP8266 tvrtke Espressif. Ovaj mikroupravljač u obliku ESP-12F Wi-Fi modula koristi se u mikroupravljačkim razvojnim pločicama poput pločice Croduino Nova 2, prikazanoj na slici 2.1.

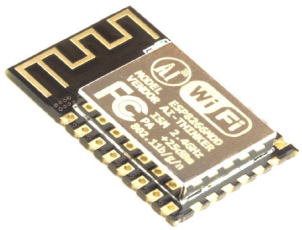


Slika 2.1: Mikroupravljačka pločica Croduino Nova 2. Izvor: https://e-radionica.com/media/catalog/product/cache/5/image/9df78eab33525d08d6e5fb8d27136e95/d/s/dsc01635.jpg

Specifikacije ESP8266 mikroupravljača su sljedeće [3]:

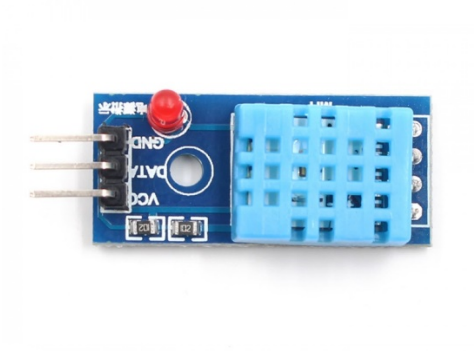
- Tensilica Xtensa LX106 procesor s podrškom za radni takt od 80MHz do 160MHz,
- radni napon od 3.3V,
- ulazni napon u rasponu od 7V do 12V,
- 16 digitalnih pinova opće namjene (GPIO),
- jedan analogni pin opće namjene (GPIO),
- jedan UART uređaj,
- jedan SPI uređaj,
- jedan I^2C uređaj,
- 4MB trajne Flash memorije,
- 64KB statičke radne memorije (SRAM).

U kombinaciji s podrškom za Wi-Fi standard za bežičnu mrežu čini ESP-12E/F Wi-Fi modul, koji podržava 802.11b/g/n bežične standarde, koji je prikazan kao samostalna komponenta na slici 2.2. Jedina razlika između ESP-12E i ESP-12F modula je vrsta antene. [4]



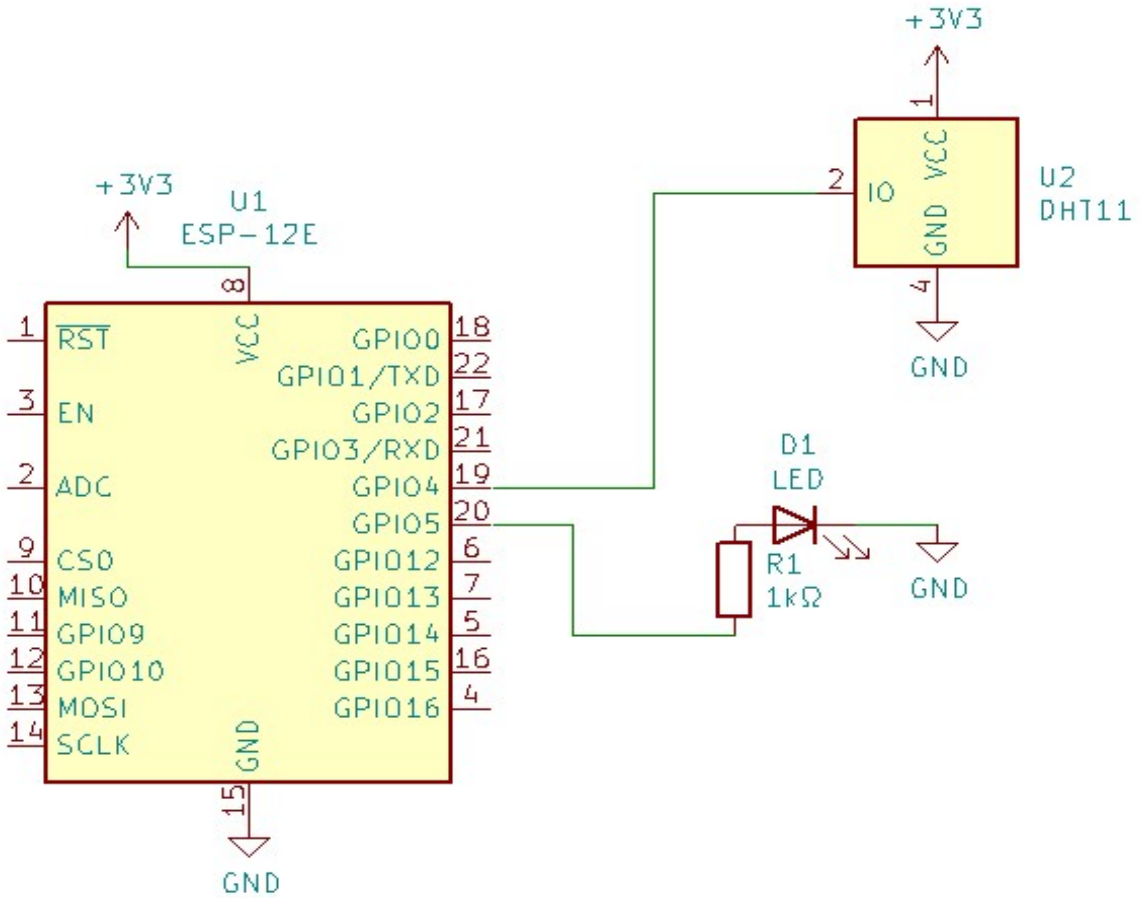
Slika 2.2: ESP-12E/F Wi-Fi modul. Izvor: https://components101.com/sites/default/files/components/ESP-12E-Module.jpg

IoT uređaj može biti i mikroupravljač s jednim ili više senzora ili aktuatora, što je slučaj i u ovom radu, gdje mikroupravljač ima priključen senzor DHT11, koji mjeri temperaturu i vlažnost zraka, prikazan na slici 2.3.



Slika 2.3: DHT11 senzor na tiskanoj pločici. Izvor: https://www.makerfabs.com/image/cache/makerfabs/DHT11%20Temperature%20Humidity%20Module/DHT11%20Temperature%20Humidity%20Module_1-1000x750.JPG

Mikroupravljački sklop korišten u ovom radu je iznimno jednostavan. Sastoji se od mikroupravljača ESP-12E, LED svjetleće diode bijele boje te pripadajućeg otpornika vrijednosti otpora od 1000 oma. Shema sklopa prikazana je u slici 2.4.



Slika 2.4: Shema mikroupravljačkog sklopa. Izvor: vlastiti rad u programu KiCad.

3. TEHNOLOGIJE UPOTREBLJENE U DEMONSTRACIJI

3.1 TLS – sigurnost transportnog sloja (Transport Layer Security)

TLS (engl. *Transport Layer Security*) je protokol čija je namjena uspostava sigurne komunikacije između dva sudionika koristeći certifikate temeljene na X.509 standardu. Nasljednik je, odnosno nadogradnja starijeg SSL (engl. *Secure Socket Layers*) protokola, koji ima istu namjenu, no kod TLS protokola koriste se drugačiji algoritmi za razmjenu tajnih ključeva.

3.1.1 Povijest i svrha nastanka TLS protokola

TLS protokol nastao je 1999. godine kao nadogradnja SSL 3.0 protokola koji je izradila tvrtka Netscape, poznata po pregledniku Netscape Navigator, koji je bio najkorišteniji internetski preglednik sve do izlaska preglednika Internet Explorer tvrtke Microsoft, koja je svoju tržišnu moć i rasprostranjenost operacijskog sustava Windows iskoristila kako bi postigla monopol na tržištu internetskih preglednika. [5] [6]

TLS protokol nastao je zbog potrebe za pouzdanijim protokolom za sigurnu komunikaciju nakon više sigurnosnih propusta u protokolu SSL 3.0; najveći od tih sigurnosnih propusta je POODLE napad, koji je otkriven i detaljno opisan od strane tvrtke Google. [7]

3.1.2 Načelo rada TLS protokola

TLS protokol sastoji se od dva podprotokola: protokol rukovanja (eng. *handshake protocol*) te protokol zapisa (eng. *record protocol*).

Protokol rukovanja koristi se za početno uspostavljanje komunikacije između pošiljatelja i primatelja te postavljanje parametara nadolazeće sigurne komunikacije, poput inačice protokola i algoritma za šifriranje koji će se koristiti za siguran prijenos podataka sve do kraja komunikacije. Nakon postavljanja parametara komunikacije, slijedi razmjena ključeva između pošiljatelja i primatelja kako bi se uspostavila sigurna veza. Razmjena ključeva u TLS protokolu verzije 1.3 izvodi se koristeći jedan od sljedeća tri protokola [8]:

- ECDHE (eng. *Elliptic-Curve Diffie-Herman Ephemeral*).

Ovaj protokol za razmjenu ključeva omogućuje sigurnu razmjenu za uspostavu komunikacije kroz nesiguran kanal. Protokol se temelji na algoritmu kriptografije eliptične krivulje (engl. *Elliptic Curve Cryptography*). [9]

Razlika između ECDH (engl. *Elliptic-Curve Diffie-Herman*) i ECDHE protokola je u tome što se prvi koristi za izradu trajnog ključa, vjerodostojnog na temelju npr. certifikata, dok se drugi koristi za privremene ključeve, kao u slučaju razmjene ključeva u protokolu rukovanja TLS protokola. [10]

- PSK

PSK (engl. *Pre-Shared Key*) simetrični je ključ koji nastaje i dijeli se između sudionika komunikacije koristeći sigurni kanal. [11]

- PSK u kombinaciji s ECDHE algoritmom

Ovdje se radi o istom simetričnom ključu koji je nastao usred prijašnje komunikacije u sigurnom kanalu, no povrh toga se šifrira ECDHE algoritmom. [11]

3.2 PKI – infrastruktura javnog ključa (Public Key Infrastructure)

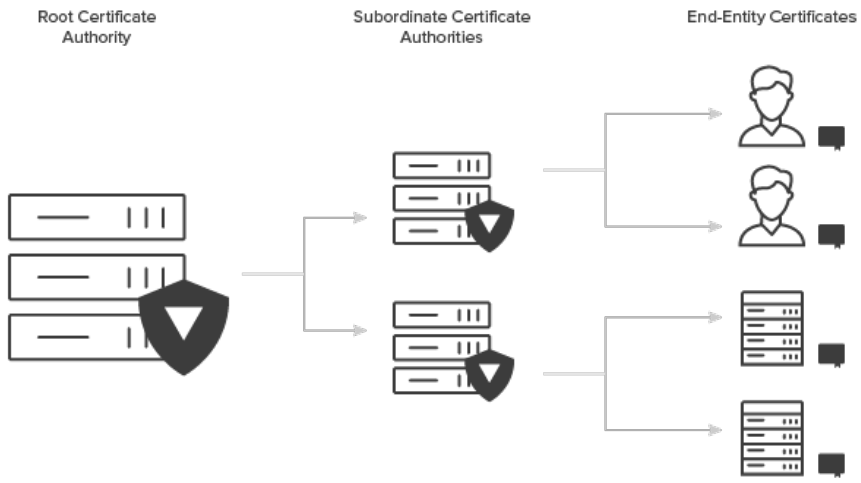
PKI je skup pravila i tijela koji čini infrastrukturu za izradu, upravljanje, distribuciju i opoziv digitalnih certifikata i upravljanje enkripcije javnim ključem. Najprepoznatljivija namjena PKI infrastrukture je za izradu i provjeru vjerodostojnosti SSL certifikata, koji se koriste za kriptiranje komunikacije pri slanju i primanju e-pošte ili pristupu web stranicama ili uslugama za internet bankarstvo. U ovom radu PKI infrastruktura bit će korištena za kriptiranje komunikacije između IoT uređaja i poslužitelja, što je u ovom slučaju krajnji korisnik.

3.2.1 Certifikati u PKI infrastrukturi

PKI infrastruktura upravlja enkripcijskim ključevima putem izdavanja i upravljanja digitalnim certifikatima. Digitalni certifikati u PKI infrastrukturi regulirani su standardom X.509, koji je opisan u poglavlju 3.2.1.1.

Digitalni certifikat nastaje od strane certifikacijskog tijela (engl. *Certification Authority*). PKI infrastruktura sastoji se od korijenskog tijela koje sadržava privatni ključ infrastrukture i najviša je točka u lancu povjerenja (engl. *trust chain*).

Posredničko ili izdavačko (engl. *intermediate* ili *issuing*) tijelo izdaje certifikate krajnjim korisnicima te postiže legitimitet za izdavanje certifikata i vjerodostojnost pomoću certifikata koji je potpisan od strane korijenskog tijela. Preporučeno je korištenje dva posrednička tijela u sigurnosne svrhe, kao i u svrhe visoke dostupnosti, kako bi se iznenadnim prestankom rada jednog od tijela nesmetano nastavilo izdavanje certifikata, što je ilustrirano na slici 3.1. U slučaju gubitka vjerodostojnosti korijenskog certifikacijskog tijela kao posljedice napada, cijela PKI infrastruktura gubi svoju vjerodostojnost i otvara vrata izdavanju zlonamjernih certifikata. [12]



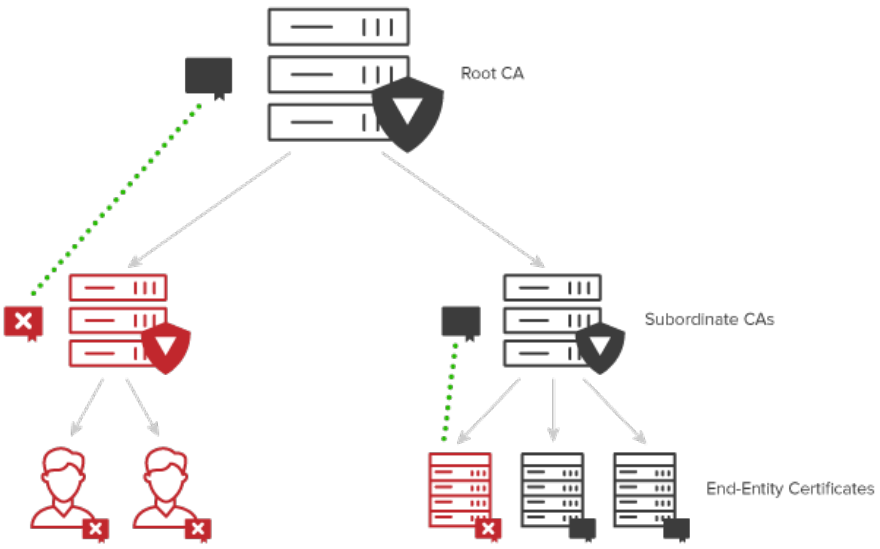
Slika 3.1: Struktura certifikacijskih tijela u PKI infrastrukturi. Izvor: https://www.keyfactor.com/wp-content/uploads/PKI-CA-Hierarchies-and-Root-CAs.png

Digitalni certifikat u PKI infrastrukturi izdaje se na sljedeći način:

- izrađuju se privatni ključ i pripadajući javni ključ,
- certifikacijsko tijelo zatražuje identifikacijske atribute,
- javni ključ i atributi šifriraju se u zahtjev za potpis i zahtjev se potpisuje od strane certifikacijskog tijela,
- certifikat se izdaje od strane posredničkog tijela i potpisuje privatnim ključem posredničkog tijela.

U slučaju gubljenja vjerodostojnosti jednog od posredničkih tijela zbog npr. unutarnjeg napada, PKI infrastruktura izdaje popis certifikata koje je potrebno smatrati nevjerodostojnima: popis opozvanih certifikata (eng. *Certificate Revocation List*), kao što je prikazano ilustracijom na slici 3.2. u slučaju kompromitiranog posredničkog, odnosno izdavačkog tijela.

Takvi popisi, kao i certifikati, imaju definiran rok valjanosti. U slučaju isteka roka valjanosti popisa, svaki certifikat izdan od strane posredničkog certifikacijskog tijela više se ne smatra i ne smije se smatrati važećim. [13]



Slika 3.2: Ilustracija CRL liste. Izvor: https://www.keyfactor.com/wp-content/uploads/PKI-Certificate-Revocation-Lists.png

3.2.2 Opis X.509 standarda

Standard X.509 opisuje standard digitalnog certifikata u PKI infrastrukturi, a osmišljen je od strane Međunarodne telekomunikacijske unije – sektora za standardizaciju telekomunikacija (ITU-T, engl. *International Telecommunications Union – Telecommunication Standardization Sector*), tijela Ujedinjenih naroda za informacijske i komunikacijske tehnologije, koja je također standardizirala H.264 metodu kodiranja i dekodiranja videozapisa, koja se koristi za izradu videozapisa na pametnim telefonima, video kamerama i internetskim stranicama za dijeljenje videozapisa. Prva verzija X.509 standarda objavljena je 1988. godine. Aktualna verzija 9 standarda objavljena je u listopadu 2019. godine.

Prema popisu u članku o X.509 standardu izrađenom od strane certifikacijskog tijela Sectigo, javni i privatni ključevi izrađuju se jednim od sljedeća tri algoritma [14]:

- RSA (engl. *Rivest-Shamir-Adleman*) algoritam.

  RSA algoritam koristi se za asimetričnu kriptografiju, što znači da se kriptografija temelji na dva različita ključa: javnom ključu i privatnom ključu. [15]
- Kriptografija eliptične krivulje. (engl. *ECC, Elliptic curve cryptography*).
- Algoritram digitalnog potpisa. (engl. *DSA, Digital signature algorithm*).

  DSA algoritam koristi se za izradu digitalnog potpisa. Digitalni potpis šifrirana je vrijednost kalkulirana pomoću željenog podatka i javnog ključa poznatog isključivo osobi koja je autor potpisa. Standard je propisan od strane američkog Nacionalnog instituta za standarde i tehnologiju (engl. *National Institute of Standards and Technology, NIST*) u kolovozu 1991. godine. [16]

3.3 SMTP – Simple Mail Transfer Protocol

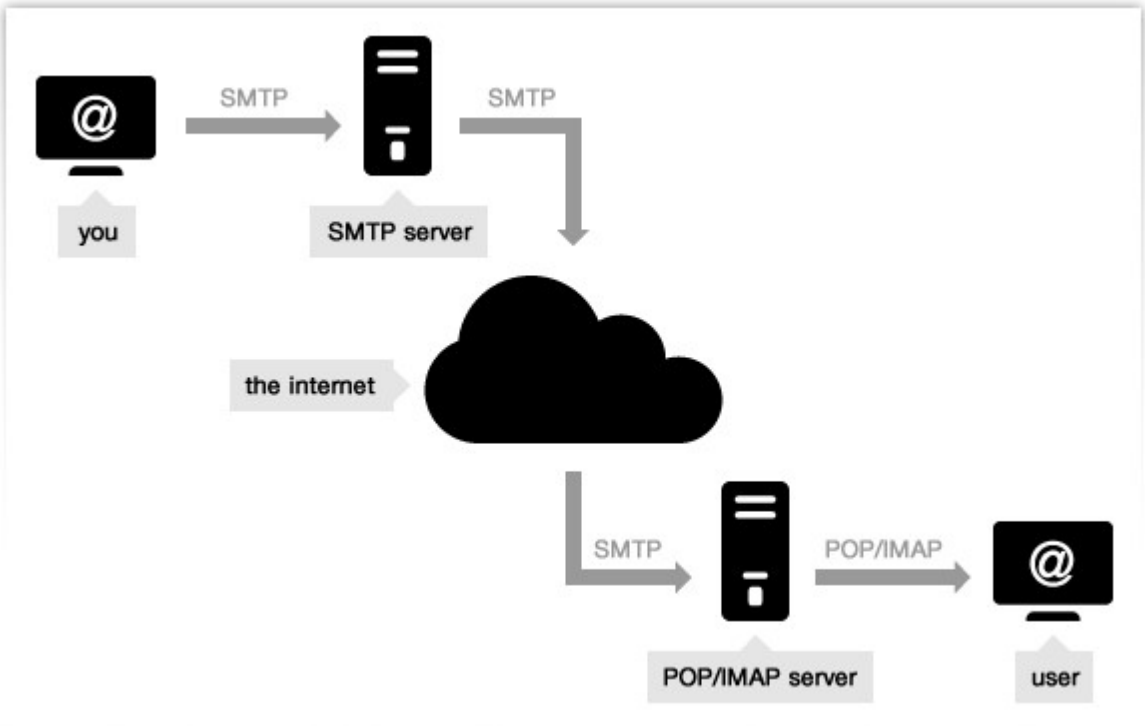
3.3.1 Povijest SMTP protokola

SMTP protokol namijenjen je za prijenos e-pošte putem Interneta. Protokoli i sustavi za slanje i primanje e-pošte postojali su i prije nego što je SMTP protokol prvi put objavljen i opisan dokumentom „RFC 788: Simple Mail Transfer Protocol“. Jednim od prvih sustava za razmjenu e-pošte smatra se *MAILBOX* sustav korišten u Institutu za tehnologiju američke savezne države Massachusetts (engl. *Massachusetts Institute of Tecbnology, MIT*).

Bitna razlika između implementacije sustava *MAILBOX* i današnje implementacije je ta da ranih šezdesetih godina prošlog stoljeća još uvijek nisu postojale ni računalne mreže ni adrese e-pošte, budući da je prva računalna mreža američkog Ministarstva obrane, *ARPANET*, puštena u rad tek 1969. godine, što znači da su se poruke u *MAILBOX* sustavu mogle razmjenjivati isključivo unutar jednog računala. Upravo je u *ARPANET* mreži poslana prva poruka e-pošte i to 1971. godine izradom prvog klijenta za e-poštu, čiji je autor Ray Tomlinson.

Nakon objave standarda SMTP protokola "RFC 788", razvijen je prvi poslužitelj za SMTP protokol, koji je napravljen u svrhu prijenosa elektroničke pošte između računala koja koriste SMTP protokol. Taj poslužitelj naziva se *Sendmail*, koji se i dalje razvija i aktivno koristi. [17]

SMTP protokol uobičajeno se koristi za slanje e-pošte i prijenos iste između SMTP poslužitelja na različitim domenama, npr. za prijenos e-pošte pošiljatelja s internet servisa *Gmail* prema internet servisu primatelja *ProtonMail*. Takav scenarij prikazan je na slici 3.3. SMTP protokol zajedno s POP3 ili IMAP4 protokolom čini skup protokola koji je potreban za organizaciju, prikaz, primanje i slanje elektroničke pošte.



Slika 3.3: Ilustracija slanja e-pošte s poslužitelja u jednoj domeni poslužitelju na drugoj domeni. Izvor: https://i.imgur.com/eN1fcuV.png

3.4 *MQTT – MQ Telemetry Transport*

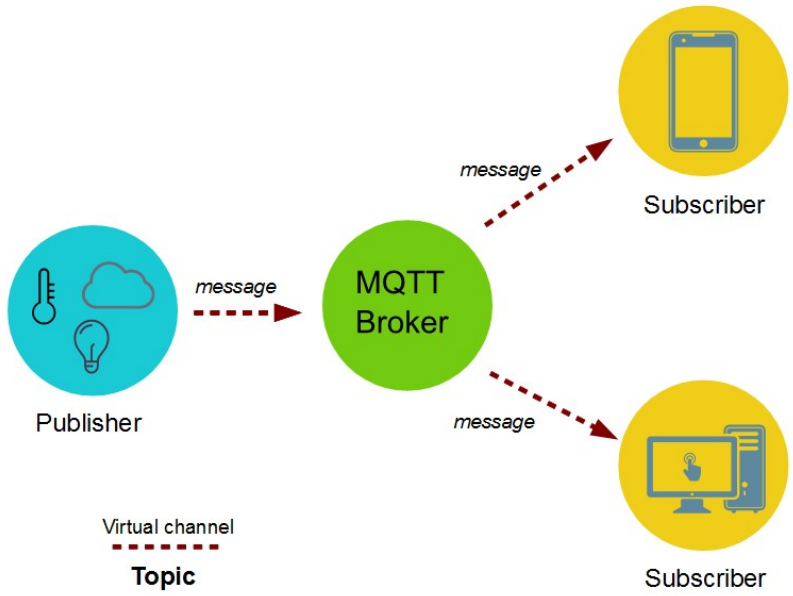
3.4.1 Povijest i namjena MQTT protokola

MQTT protokol izumili su 1999. godine Andy Stanford-Clark iz tvrtke *IBM* i Arlen Nipper iz tvrtke *Arcom*. MQTT protokol osmišljen je u svrhu razmjene podataka u scenarijima gdje je brzina, odnosno propusnost mreže ograničena, što ga čini bržim i lakšim od npr. HTTP protokola u tim uvjetima. Prednost MQTT protokola također je jednostavnost implementacije na klijentskoj strani.

Ovaj je protokol razvijen u svrhu komunikacije s naftnim cjevovodima pomoću satelitske veze, gdje je potreban protokol koji može raditi sa što manjom potrebnom propusnošću, što utječe na potrošnju baterije uređaja koji šalje podatke.

MQTT protokol objavljen je kao slobodan protokol tek 2010. godine i to u verziji 3.1. Prijašnje verzije tvrtka IBM koristila je isključivo u vlastite svrhe. [18]

Slika 3.4. prikazuje uobičajenu strukturu uporabe MQTT protokola. IoT uređaj je objavitelj podataka (engl. *publisher*), koji podatak šalje posredniku (engl. *broker*). Pretplatnici (engl. *subscriber*), što može biti aplikacija na pametnom telefonu ili programska podrška na računalu, preuzimaju te podatke.



Slika 3.4: Struktura rada MQTT protokola. Izvor: https://www.hw-group.com/files/styles/large/public/support/9198-mqtt-univerzalni-protokol-pro-cloudove-a-iot-aplikace/mqttpublishersubscriber.png?itok=w_Ak8FLx

3.5 HTTPS – HyperText Transfer Protocol Secure

3.5.1 Povijest i namjena HTTPS protokola

HTTPS protokol nastao je na temeljima HTTP protokola, namijenjenog za prikaz internetskih stranica. HTTP protokol, koji ne koristi kriptografiju, sredinom devedesetih godina prošlog stoljeća bio je prikladan za prikaz uobičajenih internetskih stranica, poput internetskih portala, enciklopedija i osobnih stranica, no pojavom usluga za internet bankarstvo i trgovinu, ukazala se potreba za protokolom koji omogućuje sigurnu komunikaciju koju nije moguće presresti, što bi spriječilo npr. krađu osobnih podataka ili bankovnih kartica. Tvrtka Netscape, poznata po protokolu SSL, spomenutom u poglavlju 3.1., odlučila je spojiti taj protokol s HTTP protokolom. Rezultat te kombinacije je HTTPS protokol, koji omogućava prikaz web stranica pomoću sigurne, kriptirane komunikacije koju nije moguće presresti.

Tik nakon nastanka, 1995. godine, taj protokol prvotno je bio namijenjen za obradu kartičnih plaćanja. Sredinom prvog desetljeća 21. stoljeća, HTTPS protokol počeo se koristiti i za prijave na internetske stranice poput foruma.

U sljedećem desetljeću tvrtka *Google* implementirala je podršku za HTTPS protokol u svojoj internetskoj tražilici, zajedno i s ostalim servisima, poput usluge e-pošte *Gmail* te usluge *online* obrade teksta *Google Docs*, što su kasnije učinile i tvrtke *Facebook* i *Twitter*.

U 2021. godini HTTPS protokol koristi se kao zadani protokol u većini internetskih stranica te se smatra jedinim sigurnim protokolom od strane autora najkorištenijih internetskih preglednika, *Google Chrome* i *Mozilla Firefox*. Stranice koje još uvijek ne koriste HTTPS protokol postavljene su niže u rezultatima tražilice *Google* u usporedbi sa stranicama koje koriste HTTPS protokol, što narušava njihovu dostupnost. [19]

4. OPIS PROBNOG OKRUŽENJA

Za uspješnu demonstraciju primjene kriptografije koristit će se probno okruženje sa svim potrebnim servisima, opisanim u cjelini 4.1. Poslužiteljski dio sastoji se od virtualnih poslužitelja koji su potrebni za rad računalne mreže, a klijentski dio je mikroupravljač, koji će rabiti usluge poslužiteljskog dijela u svrhu demonstracije.

4.1 Poslužiteljski dio

Poslužiteljski dio sastoji se od pet poslužitelja temeljenih na operacijskom sustavu Microsoft Windows Server različitih verzija. Virtualni poslužitelji pokreću se na Microsoft Hyper-V hipervizoru (engl. *hypervisor*). Svi poslužitelji pridruženi su u Active Directory računalnu domenu naziva *asintec.hr*. Domenski poslužitelj s operacijskim sustavom Microsoft Windows Server 2019 Standard uz domenske usluge pruža i uslugu DNS servisa, budući da je taj servis neophodan za funkcionalnost domene. DNS poslužitelj sadržava zapise za domenski naziv, odnosno adresu *asintec.hr* i pokazuje prema IP adresama mikroupravljača i poslužitelja. IP adrese i DNS nazivi poslužitelja i mikroupravljača navedeni su u tablici niže.

Budući da probno okruženje ne sadrži DHCP servis za automatsku dodjelu IP adrese, koriste se ručno postavljene IP adrese u programu mikroupravljača te na poslužiteljima. Cjelokupno probno okruženje koristi podmrežu neovisnu od ostatka mreže i to bez pristupa Internetu, što izolira cjelokupnu mrežu od npr. pisača koji automatski instaliraju upravljačke programe i pojednostavljuje realizaciju Active Directory domene.

Za uspješnu primjenu TLS protokola za kriptiranje komunikacije svakim od obrađenih protokola potrebna su dva certifikacijska tijela. Korijensko certifikacijsko tijelo nalazi se na vrhu lanca povjerenja (engl. *trust chain*) te potpisuje i provjerava vjerodostojnost certifikata za posredničko certifikacijsko tijelo, koje na kraju izdaje i provjerava vjerodostojnost certifikata za krajnje korisnike.

Unatoč preporuci korištenja dva posrednička, odnosno izdavačka certifikacijska tijela u poglavlju 3.2.1., ovdje se koristi samo jedno tijelo zbog jednostavnosti implementacije i ograničene količine radne memorije na poslužitelju virtualnih strojeva.

Certifikacijska tijela realizirana su na operacijskom sustavu Microsoft Windows Server 2016 Standard instalacijom značajke za certifikacijska tijela. Certifikacijska tijela nalaze se na dva odvojena poslužitelja, a nakon izdavanja certifikata s korijenskog tijela za posredničko tijelo, poslužitelj s korijenskim tijelom bit će ugašen zbog sigurnosnih razloga.

Certifikati za korijensko i izdavačko tijelo izdani su s rokom valjanosti od deset godina, a certifikati za web poslužitelje, što uključuje MQTT i SMTP poslužitelje, izdani su s rokom valjanosti od jedne godine. MQTT poslužitelj instaliran je na poslužitelj s operacijskim sustavom CentOS 7, temeljenim na jezgri Linux.

Unutrašnji sustav e-pošte pokreće se na programskoj podršci Microsoft Exchange Server 2016 Cumulative Update 21, također na operacijskom sustavu Microsoft Windows Server 2016 Standard. Adresa *esp8266.out@asintec.hr* dodijeljena je mikroupravljaču za slanje e-pošte koja se šalje na adresu *esp8266.log@asintec.hr*.

Cjelokupnim okruženjem upravlja se kroz OOB (engl. *Out-Of-Band Management*) računalo koje sadrži dodatne alate za MMC (engl. *Microsoft Management Console*) značajku operacijskog sustava Windows. Nazivi računala te pripadajuće IP adrese i DNS zapisi prikazani su u tablici 4.1.

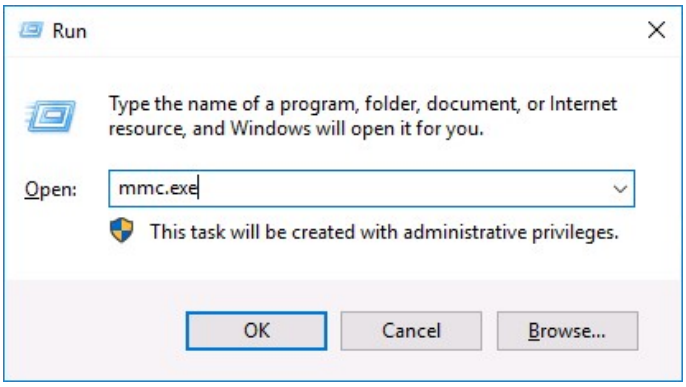
Tablica 4.1. Popis računala u probnom okruženju s IP adresama, DNS nazivima i namjenama.

Naziv stroja	IP adresa	DNS naziv	Namjena
ASI-DC01	10.80.44.1	-	Poslužitelj DNS usluge i domene
ASI-RCA	10.80.44.2	-	Korijensko certifikacijsko tijelo
ASI-ICA	10.80.44.3	-	Posredničko certifikacijsko tijelo
ASI-MAIL01	10.80.44.4	mail.asintec.hr	Poslužitelj e-pošte
ASI-OOB-1	10.80.44.50	-	OOB računalo
ASI-MQTT	10.80.44.60	mqtt.asintec.hr	MQTT poslužitelj
ESP8266	10.80.45.1	https-demo.asintec.hr	ESP8266 mikroupravljač – HTTPS
ESP8266	10.80.45.2	mqtt-demo.asintec.hr	ESP8266 mikroupravljač – MQTT
ESP8266	10.80.45.3	smtp-demo.asintec.hr	ESP8266 mikroupravljač – SMTP

4.2 *Proces izdavanja i izvoza certifikata u Microsoft Active Directory računalnoj domeni*

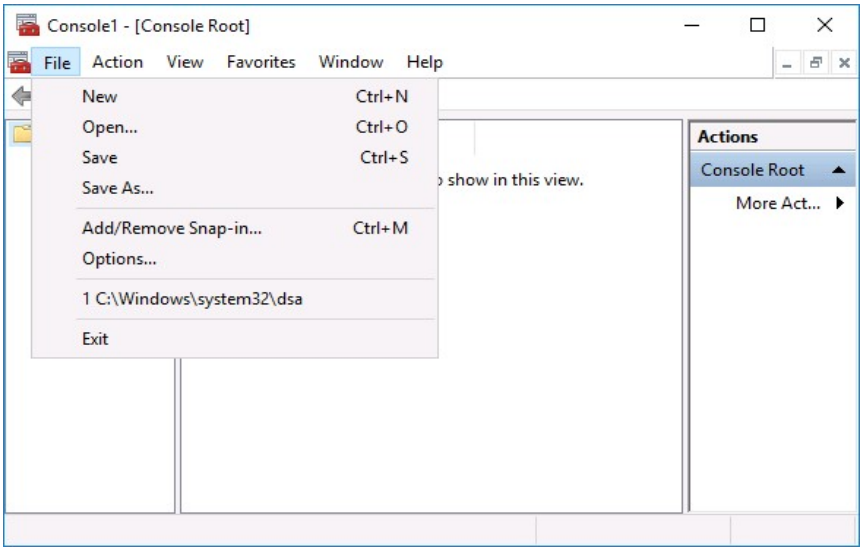
4.2.1 Izdavanje certifikata

Izdavanje certifikata vrši se kroz dodatni alat značajke MMC operacijskog sustava Windows. Značajka MMC pokreće se otvaranjem prozora Pokreni pritiskom tipki Windows i tipke R istovremeno ili pretragom u tražilici operacijskog sustava. U tekstni otvir *Otvori* potrebno je upisati *mmc.exe*, kao što je prikazano na slici 4.1.



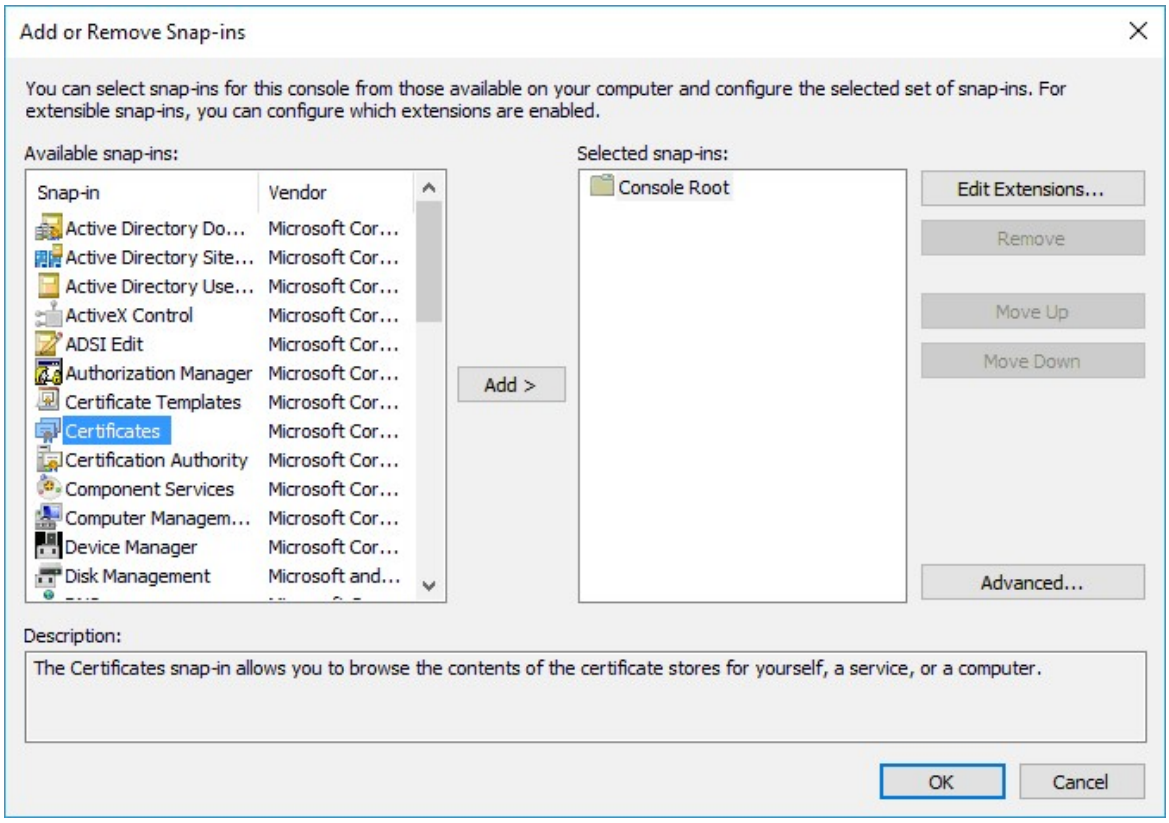
Slika 4.1: Prozor Pokreni u sustavu Windows. Izvor: vlastita preslika rada.

U novootvorenom prozoru potrebno je kliknuti na stavku izbornika *File* pa kliknuti na opciju *Add or remove Snap-in* ili pritisnuti tipke *Ctrl* i *M* istovremeno, što je prikazano na slici 4.2.



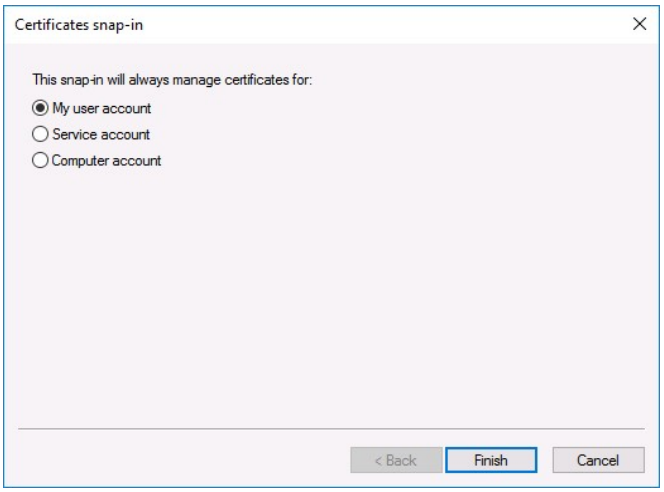
Slika 4.2: Stavke izbornika File prozora značajke MMC. Izvor: vlastita preslika rada.

U novootvorenom prozoru u lijevom stupcu potrebno je označiti dodatni alat za certifikate (engl. *Certificates*) te pritiskom na gumb *Add* > dodati alat u trenutnu konzolu, što je prikazano na slici 4.3.



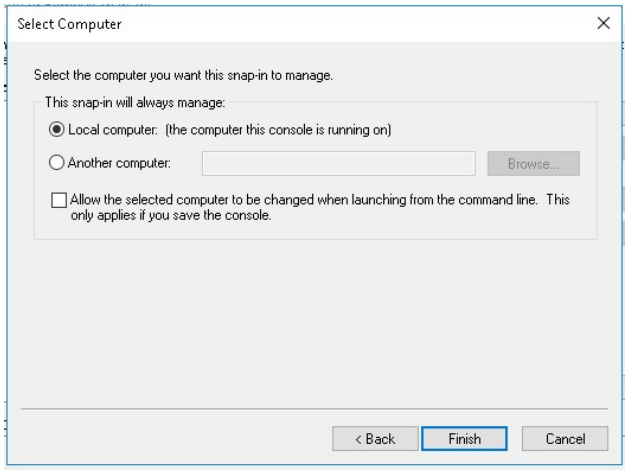
Slika 4.3: Prozor za dodavanje dodatnih alata u konzolu značajke MMC. Izvor: vlastita preslika rada.

Novi prozor omogućuje pokretanje dodatnog alata kao servisni račun ili račun računala u domeni. U slučaju da je potrebno izraditi korisnički certifikat, zadana opcija *My user account* ostaje označena, kao što je prikazano na slici 4.4. Certifikat za sva tri scenarija opisana u poglavlju 5 izdat će se kao certifikat za *web* poslužitelj, stoga je potrebno označiti opciju za račun računala, odnosno *Computer account*.



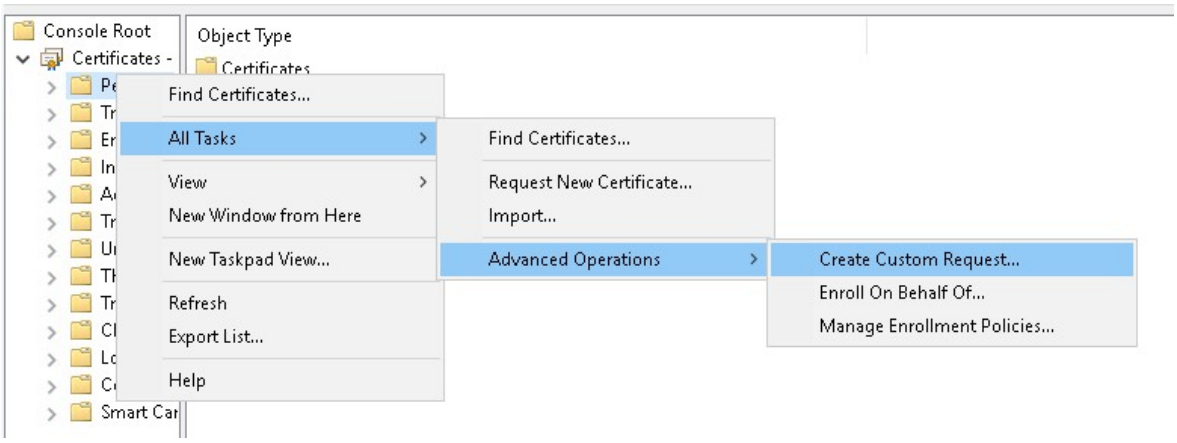
Slika 4.4: Prozor za pokretanje dodatnog alata kao servisni ili račun računala u domeni. Izvor: vlastita preslika rada.

U sljedećem prozoru odabire se račun pod kojim će se pokrenuti konzola za certifikate. To može biti lokalno računalo ili drugo računalo u domeni. Za potrebe izdavanja certifikata za demonstraciju nije potrebno ništa mijenjati pa će opcija za lokalno računalo ostati označena, kao što je prikazano na slici 4.5.



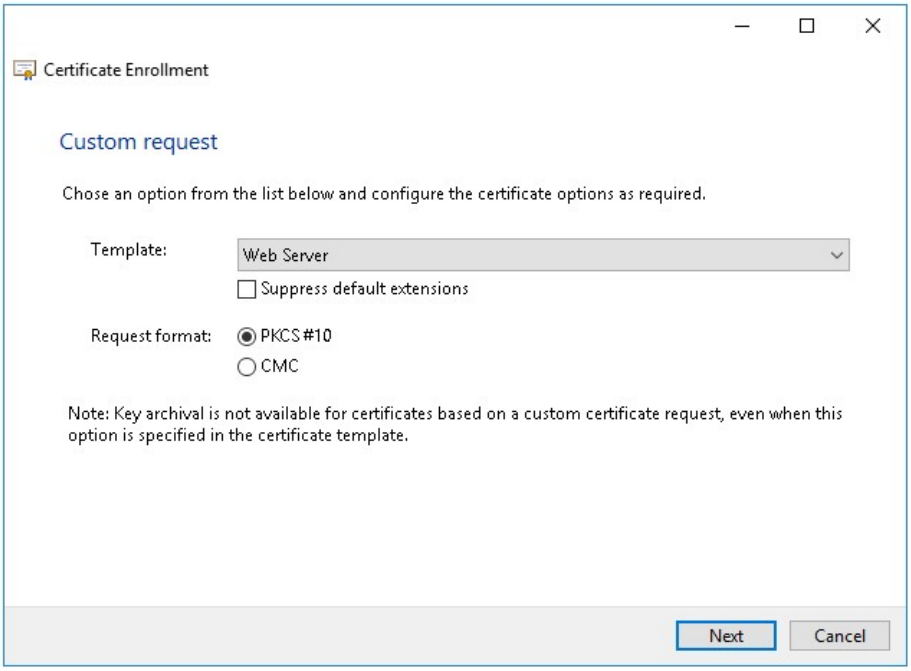
Slika 4.5: Prozor za odabir računala za pokretanje dodatnog alata. Izvor: vlastita preslika rada.

Desnim klikom miša na mapu *Personal* u korijenskom pregledu mapa i odabirom opcije *Create Custom Request...* u podizborniku *All Tasks* te *Advanced Operations*, certifikacijskim tijelima predaje se zahtjev za novi certifikat, što je prikazano u slici 4.6.



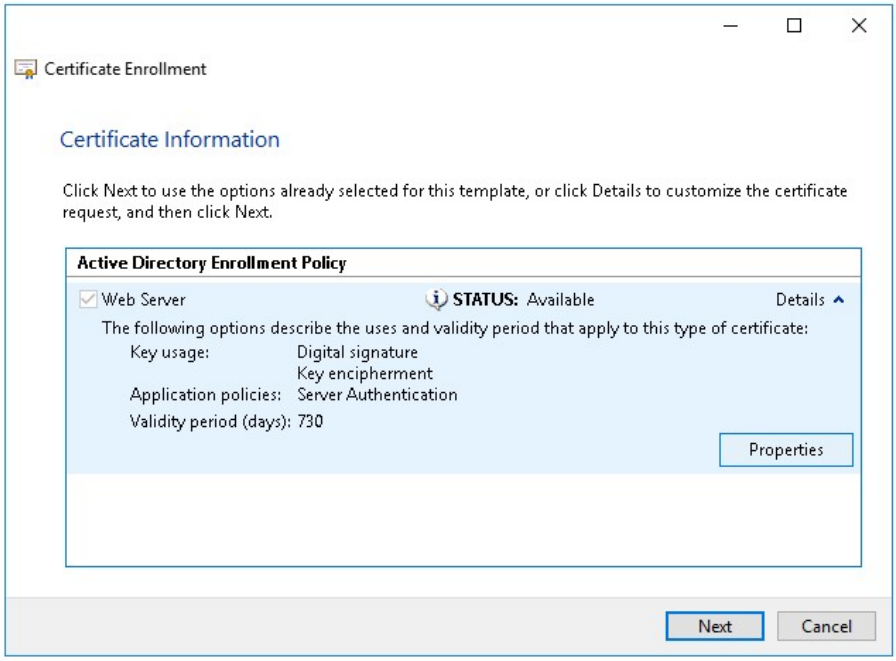
Slika 4.6: Opcija za zahtjev novog certifikata. Izvor: vlastita preslika rada.

U prozoru *Custom request, koji je prikazan na slici 4.7.,* odabire se vrsta predloška za certifikat te format zahtjeva certifikata koji će se poslije obraditi na posredničkom certifikacijskom tijelu. Odabran je predložak za web poslužitelj (engl. *Web Server*), a format zahtjeva ostavljen je na zadanu opciju, *PKCS #10*.

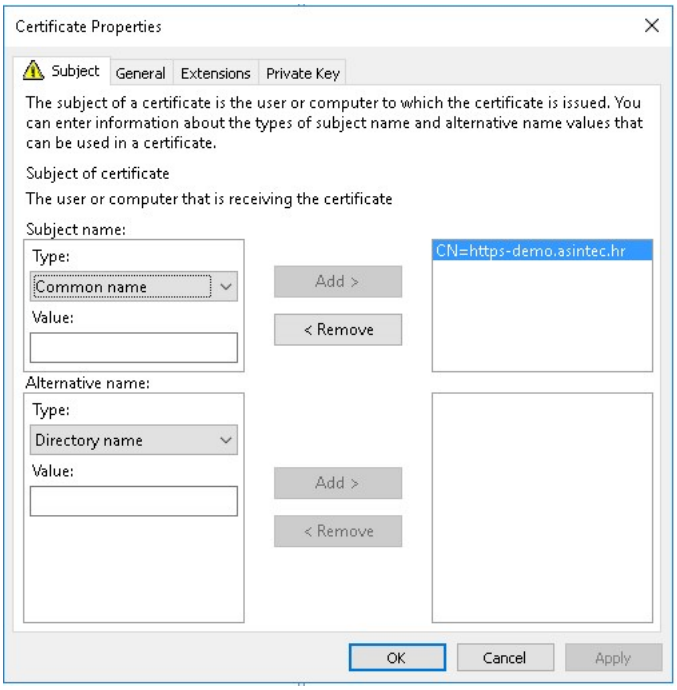


Slika 4.7: Prozor za odabir predloška i formata zahtjeva certifikata. Izvor: vlastita preslika rada.

U prozoru *Certificate Information*, prikazanom na slici 4.8. proširenjem stavke *Web Server* klikom na gumb pored teksta *Details*, klikom na gumb *Properties* unose se atributi. Unijet će se samo uobičajeni naziv (engl. *Common Name, CN*), odnosno domenski naziv poslužitelja, što je prikazano na slici 4.9. Identifikacijski podaci popunjuju se u slučaju izdavanja za produkcijske svrhe, no za potrebe testiranja i eksperimentiranja to nije potrebno ispunjavati.

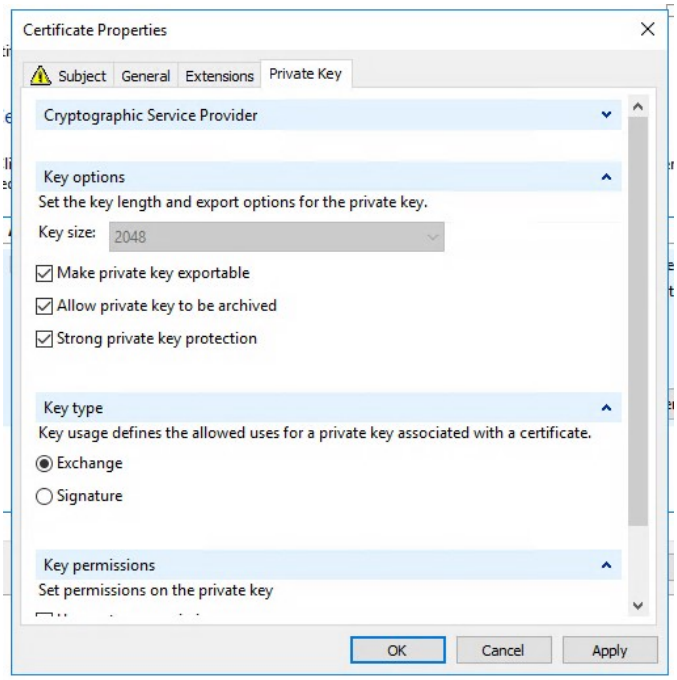


Slika 4.8: Prozor s informacijama certifikata. Izvor: vlastita preslika rada.



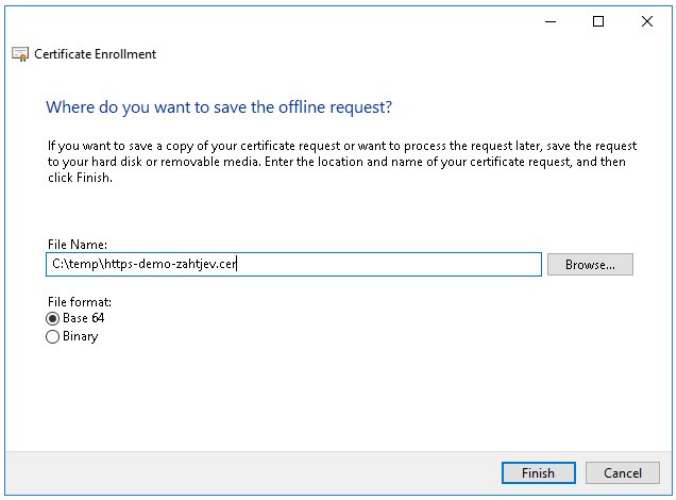
Slika 4.9: Prozor za unos atributa certifikata. Izvor: vlastita preslika rada.

Nakon unosa atributa, potrebno je omogućiti izvoz privatnog ključa certifikata, što će biti potrebno u programskom kodu za demonstraciju.



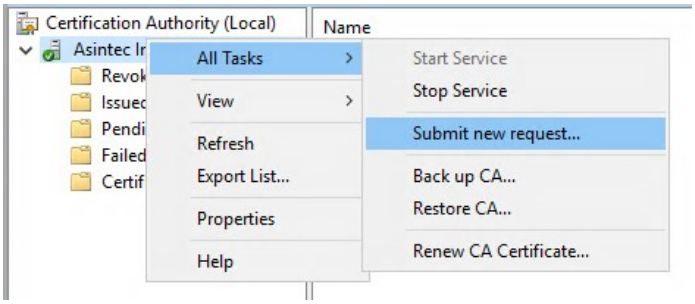
Slika 4.10: Postavke privatnog ključa. Izvor: vlastita preslika rada.

Certifikat je potrebno spremiti kao datoteku u računalu. Ponuđeni oblici za spremanje su u formatu znakovnog sustava *Base64* te u binarnom obliku, što ostaje nepromijenjeno. Također je potrebno unijeti putanju u koju će se spremiti zahtjev za certifikat, što je prikazano na slici 4.11.

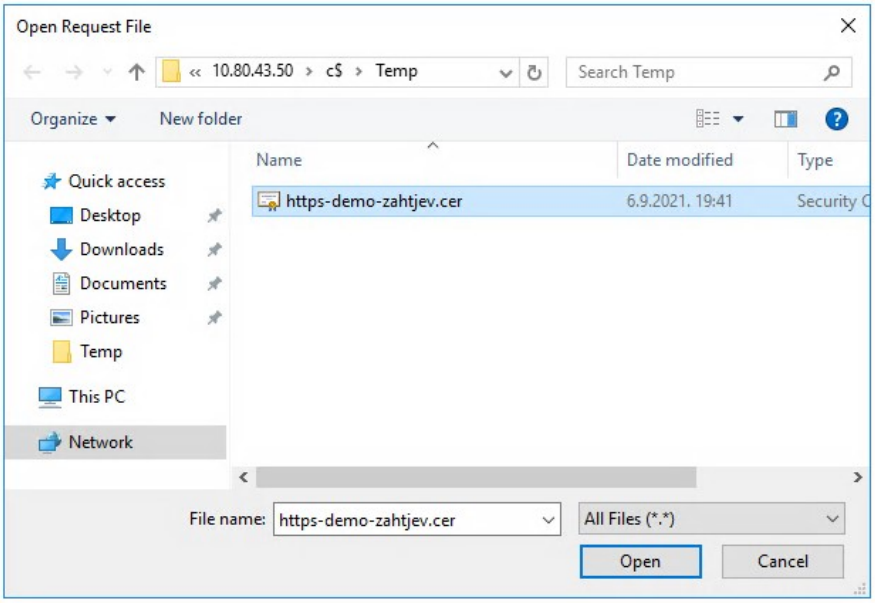


Slika 4.11: Prozor za spremanje zahtjeva certifikata na računalo. Izvor: vlastita preslika rada.

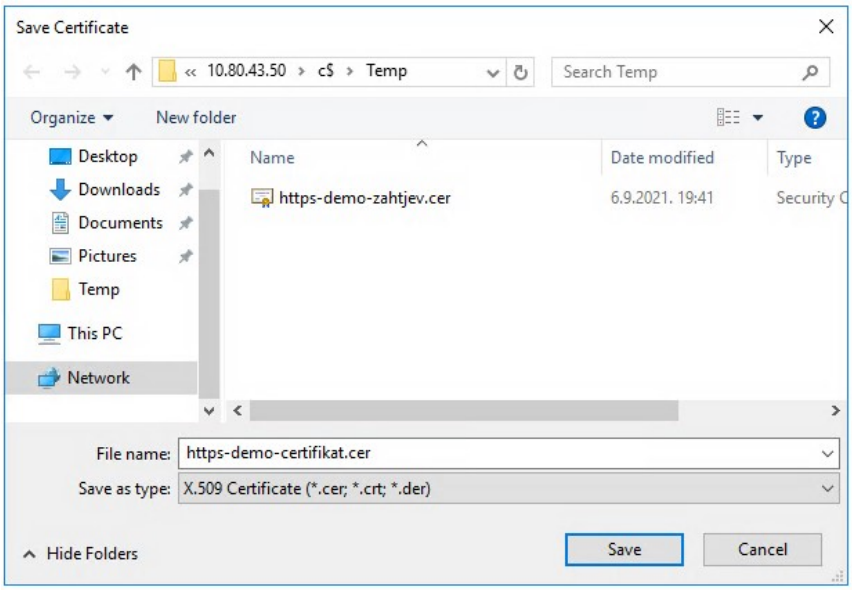
Obrada zahtjeva na posredničkom certifikacijskom tijelu započinje se tako što se stvorena datoteka otvori na posredničkom certifikacijskom tijelu odabirom opcije *Submit new request...*, otvaranjem zahtjeva te spremanjem novoizrađenog certifikata, kao što je prikazano na slikama 4.12., 4.13. i 4.14.



Slika 4.12: Opcija za obradu zahtjeva za certifikat pomoću datoteke sa zahtjevom. Izvor: vlastita preslika rada.



Slika 4.13: Prozor za otvaranje datoteke zahtjeva za certifikat. Izvor: vlastita preslika rada.

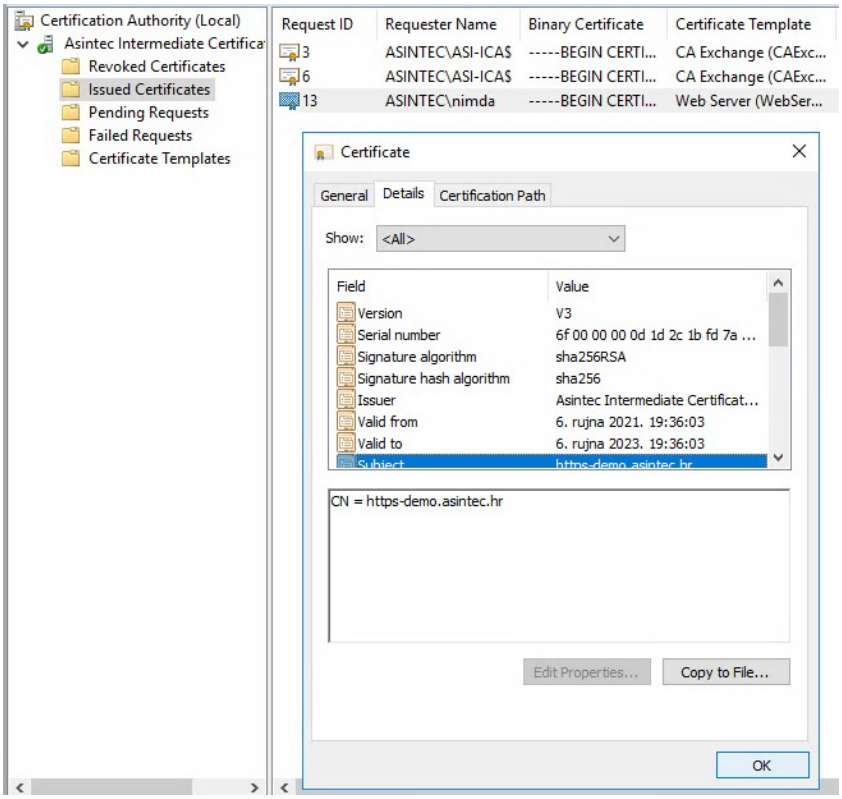


Slika 4.14: Prozor za spremanje novoizrađenog certifikata. Izvor: vlastita preslika rada.

4.2.2 Izvoz certifikata

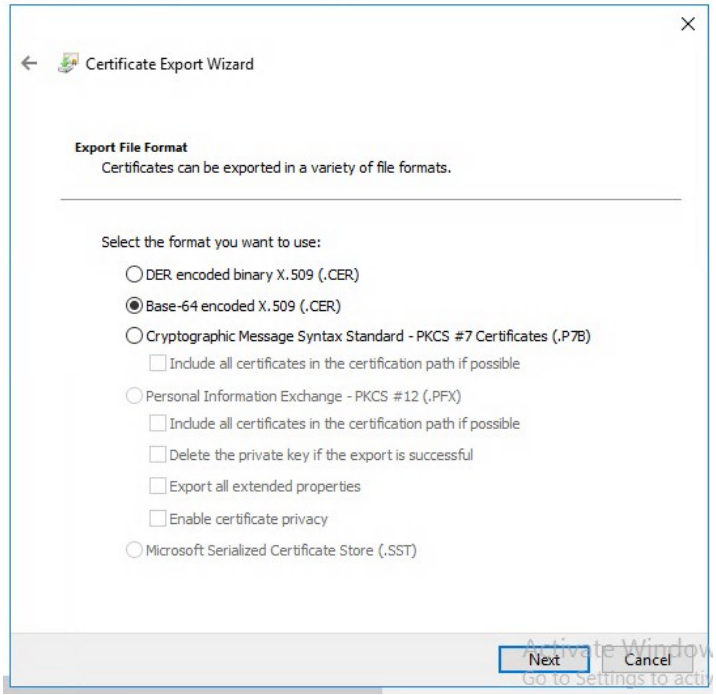
Spremanjem certifikata na posredničko korijensko tijelo, certifikat je spreman za korištenje s bilo kojim računalom ili mikroupravljačem s mogućnošću korištenja certifikata za uspostavu kriptirane komunikacije.

U slučaju da zahtjev nije izdan pomoću načina opisanog u potpoglavlju iznad, zahtjev za izdavanjem certifikata automatski se obrađuje te je izvoz certifikata potrebno obaviti na posredničkom korijenskom tijelu i to na način da se u popisu izdanih certifikata dvoklikom lijeve tipke miša otvori certifikat koji je potrebno izvesti, nakon čega se otvara prozor s informacijama o certifikatu, što je prikazano na slici 4.15. Potrebno je kliknuti na gumb *Copy to File...* kako bi se započeo proces izvoza certifikata.

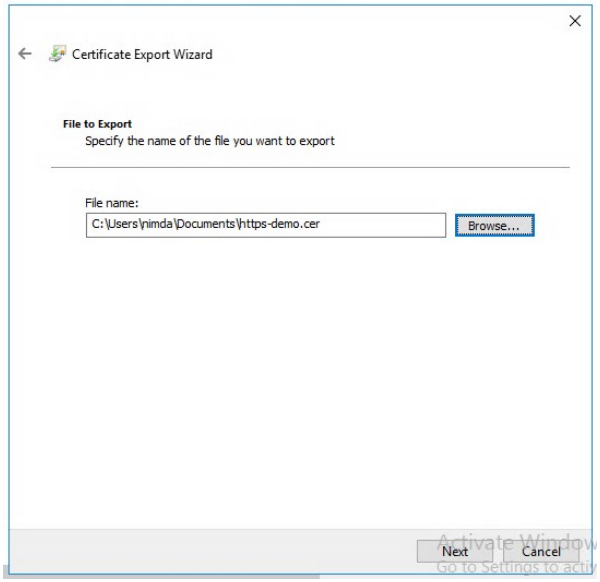


Slika 4.15: Prozor s informacijama certifikata. Izvor: vlastita preslika rada.

Ponuđena su tri formata za izvoz certifikata. Prvim formatom se certifikat izvozi u binarnom formatu, drugi u formatu znakovnog sustava *Base64*, a treći u PKCS#7 formatu (engl. *Public-Key Cryptography Standards*). Potrebno je odabrati drugi format kako bi certifikat bio primjenjiv na web poslužitelju kao što je prikazano na slici 4.16, te naposljetku odabrati naziv datoteke u koju će se certifikat spremiti, što je prikazano na slici 4.17. U slučaju da je potrebno izvesti i privatni ključ, odabire se treći format.



Slika 4.16: Prozor za odabir formata certifikata. Izvor: vlastita preslika rada.



Slika 4.17: Prozor za odabir lokacije datoteke certifikata. Izvor: vlastita preslika rada.

Otvaranjem certifikata u uređivaču teksta vidi se certifikat, koji je kodiran u znakovnom sustavu *Base64*, što prikazuje slika 4.17. Sve što je potrebno kako bi se certifikat koristio na mikroračunalu je kopirati i zalijepiti sadržaj certifikata u programski kod.

5. DEMONSTRACIJA PRIMJENE PROTOKOLA

5.1 *Primjena kriptiranja pomoću HTTPS protokola*

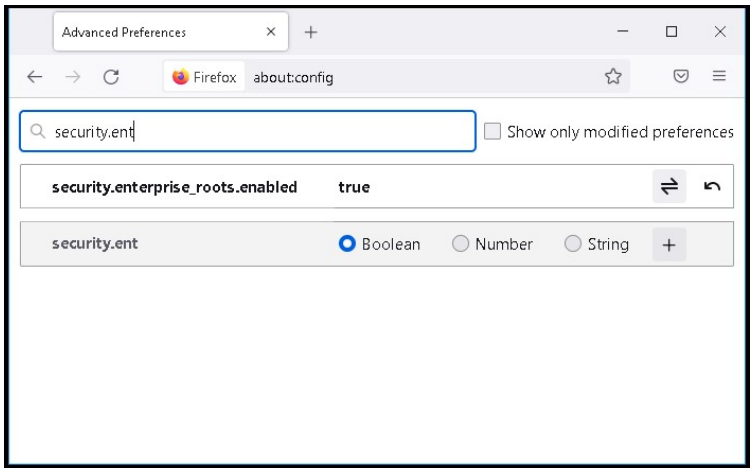
Za potrebe ove demonstracije certifikat je izvezen u PKCS#12 formatu iz razloga što je potreban privatni ključ certifikata. U tom slučaju certifikat i njegov privatni ključ zaštićeni su lozinkom. Opcija za izvoz u taj format ponuđena je samo ako se izvozi i privatni ključ te nije dostupna u ostalim formatima opisanim 4.2.2., iz razloga što ostali formati nisu predviđeni za spremanje privatnog ključa.

Razdvajanje datoteke u certifikat i privatni ključ vrši se korištenjem programske podrške *OpenSSL*. Niže je opisan primjer na operacijskom sustavu Linux Mint.

Programski kod 5.1: Izvoz certifikata i privatnog ključa s programskom podrškom OpenSSL.

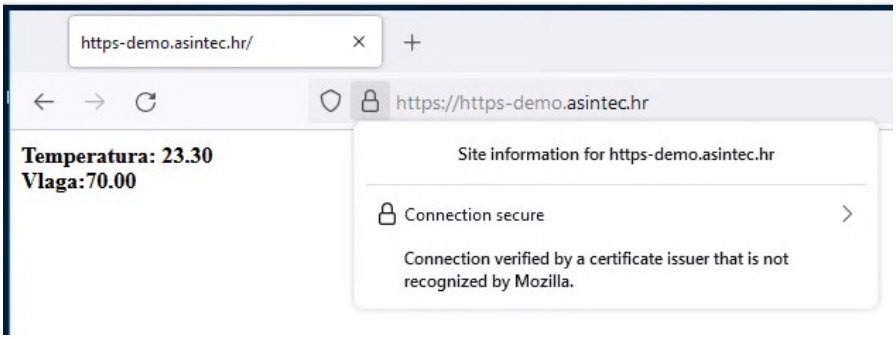
```
zvono@ALP-LENV14:~/Desktop$ openssl pkcs12 -in https-demo-cert-priv.pfx -out https-demo-key.key

Enter Import Password: ****

Enter PEM pass phrase: ****

Verifying - Enter PEM pass phrase: ****

zvono@ALP-LENV14:~/Desktop$ openssl pkcs12 -in https-demo-cert-priv.pfx -clcerts -nokeys -out https-demo-cer

Enter Import Password: ****

zvono@ALP-LENV14:~/Desktop$ openssl rsa -in https-demo-key.key -out https-demo-key-decrypted.key

Enter pass phrase for https-demo-key.key: ****

writing RSA key

zvono@ALP-LENV14:~/Desktop$
```

Prije nego je moguće posjetiti internetsku stranicu mikroupravljača, u web pregledniku Firefox potrebno je omogućiti opciju *security.enterprise_roots.enabled*, koja omogućuje pregledniku korištenje certifikata spremljenih u operacijski sustav, kako bi preglednik provjerio i potvrdio vjerodostojnost certifikacijskih tijela.



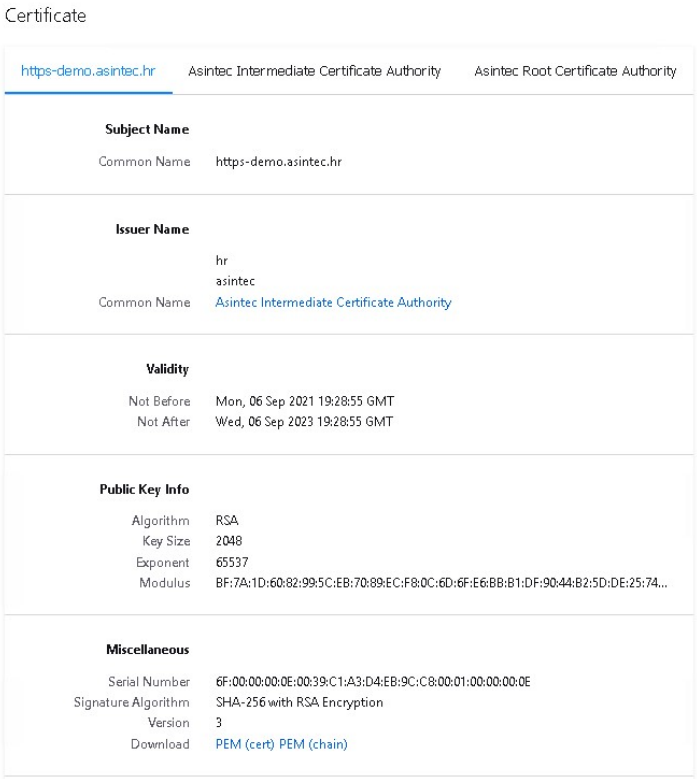
Slika 5.1: Uključivanje opcije za korištenje certifikata operacijskog sustava. Izvor: vlastita preslika rada.

Program za mikroupravljač sastoji se od koda u prilogu. Otvaranjem poveznice *https://https-demo.asintec.hr* sa virtualnog računala *ASI-OOB-1* uspostavlja se sigurna HTTPS veza s mikroupravljačem, koji na web stranici svojeg poslužitelja prikazuje vrijednosti temperature i vlage sa senzora DHT11. Klikom na lokot pored adresne trake vidljiva je primjena TLS enkripcije, što potvrđuje web preglednik na slici 5.2.



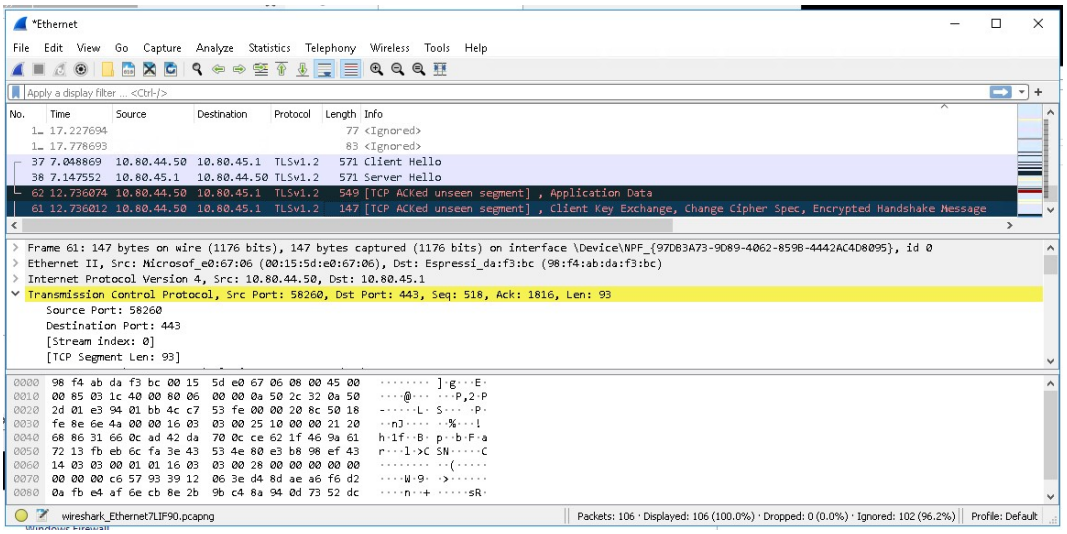
Slika 5.2: Potvrda sigurne veze u web pregledniku. Izvor: vlastita preslika rada.

Isto je vidljivo pristupom na poveznice https://https-demo.asintec.hr/ugasi i https://https-demo.asintec.hr/upali, koje služe za upravljanje LED diodom. Klikom na strelicu u desnom dijelu prozorčića te klikom na gumb za prikaz više informacija (engl. *More Information*) prikazuju se informacije o certifikatu navedene stranice te cjelokupan lanac povjerenja, odnosno certifikati posredničkog i korijenskog certifikacijskog tijela.



Slika 5.3: Prikaz lanca povjerenja PKI infrastrukture u pregledniku Firefox. Izvor: vlastita preslika rada.

Korištenjem programske podrške *Wireshark* vidljiv je mrežni promet između računala i mikroupravljača, što pokazuje slika 5.4. Vidljivi su koraci uspostavljanja komunikacije: pozdravna poruka, razmjena ključeva, postavljanje algoritma, rukovanje (engl. *handshake*) te na kraju slanje podataka.



Slika 5.4: Prikaz mrežnog prometa između računala i mikroupravljača u programskoj podršci Wireshark. Izvor: vlastita preslika rada.

5.2 Primjena kriptiranja pomoću MQTT protokola

Slično kao i u slučaju demonstracije uz pomoć HTTPS protokola, izdan je certifikat s uključenom opcijom izvoza privatnog ključa, ovaj put za domenski naziv mqtt.asintec.hr. Također su odvojeni certifikat i privatni ključ, uključujući podešavanje MQTT poslužitelja koje omogućuje vezu pomoću TLS protokola, za što je potreban certifikat i privatni ključ.

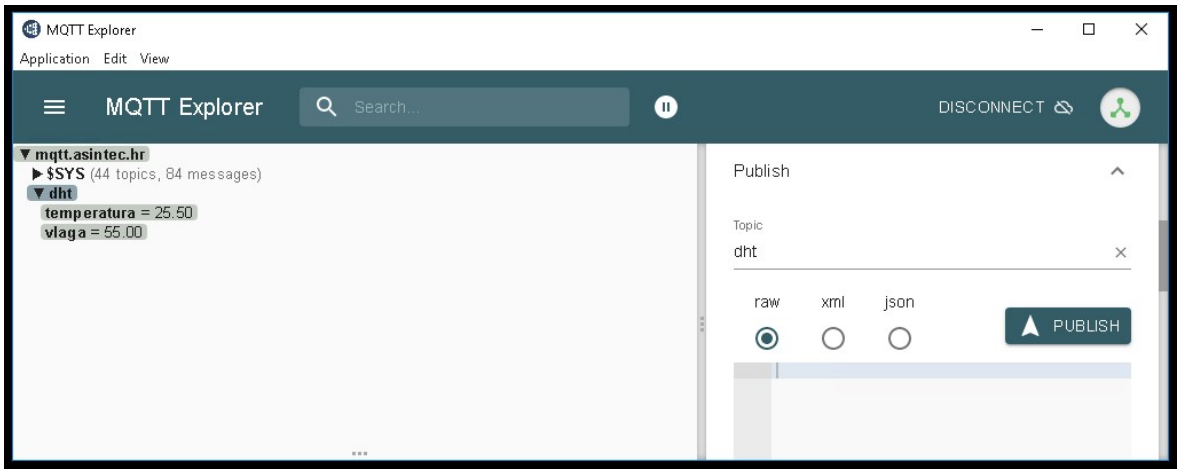
Za provjeru vjerodostojnosti cjelokupnog lanca povjerenja napravljen je izvoz certifikata posredničkog korijenskog tijela, koji je potrebno ubaciti u MQTT poslužitelj i programski kod mikroupravljača za uspješnu vezu između poslužitelja i mikroupravljača.

U operacijskom sustavu CentOS Linux 7 instaliran je MQTT poslužitelj *Eclipse Mosquitto*, čija se konfiguracijska datoteka nalazi u putanji */etc/mosquitto/mosquitto.conf*. Certifikati i privatni ključ certifikata poslužitelja u formatu znakovnog sustava *Base64* nalaze se u putanji */etc/certs*. Certifikat posredničkog tijela nalazi se u datoteci *ica-cert.cer*, certifikat MQTT poslužitelja u datoteci *mqtt-cert.cer*, a nešifrirani privatni ključ certifikata MQTT poslužitelja u datoteci *mqtt-key-d.key*.

Programski kod 5.2: Izdvojene promjene u konfiguraciji MQTT poslužitelja.

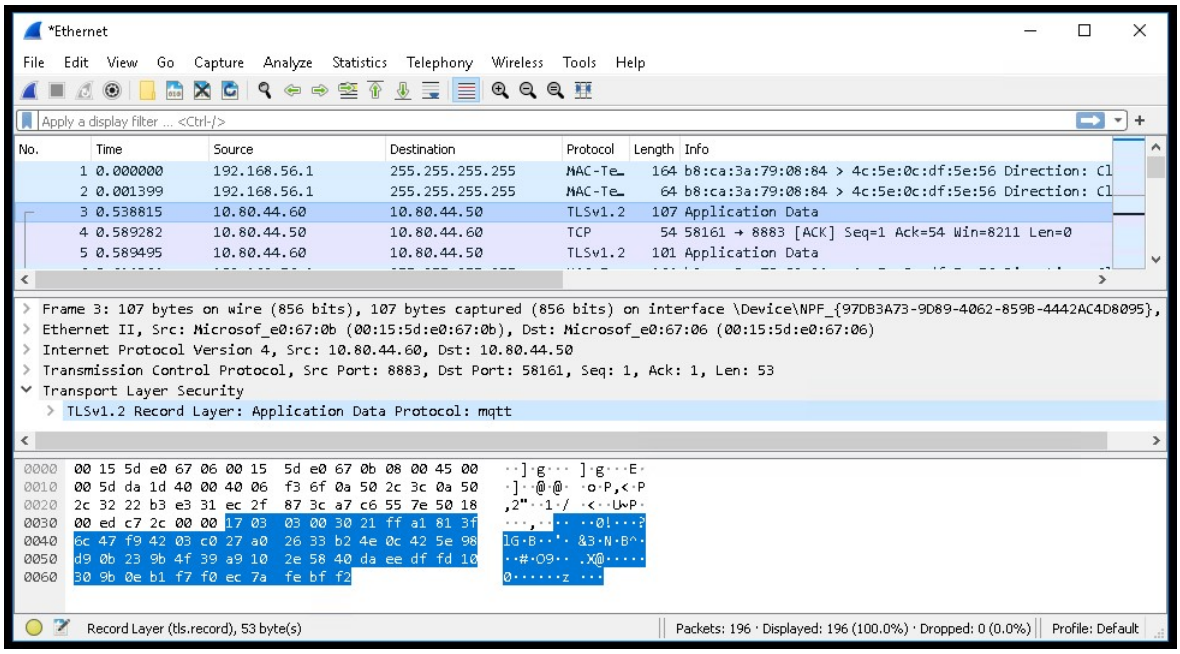
```
# Port to use for the default listener.
port 8883
# cafile defines the path to a file containing the CA
certificates.
cafile /etc/certs/ica-cert.cer
# Path to the PEM encoded server certificate.
certfile /etc/certs/mqtt-cert.cer
# Path to the PEM encoded keyfile.
keyfile /etc/certs/mqtt-key-d.key
```

U programskom kodu 5.2. nalaze se izmjene u konfiguracijskoj datoteci MQTT poslužitelja. Prema preporuci autora poslužitelja, priključnica MQTT poslužitelja mijenja se s 1883 na 8883 ukoliko je uključen TLS protokol. Navedene su datoteke koje sadržavaju certifikate posredničkog tijela i MQTT poslužitelja te privatni ključ certifikata MQTT poslužitelja. Program na mikroupravljaču svaku sekundu postavlja vrijednost tema *dht/temperatura* i *dht/vlaga* na vrijednosti dobivene s DHT11 senzora. Pregled podataka na poslužitelju vrši se programskom podrškom *MQTT Explorer*.



Slika 5.4: Prikaz podataka poslužitelja u programskoj podršci MQTT Explorer. Izvor: vlastita preslika rada.

Korištenjem programske podrške *Wireshark* na računalu *ASI-OOB-1* moguće je dobiti potpun pregled dolaznog i izlaznog mrežnog prometa. Slika 5.5. prikazuje jedan od mrežnih paketa razmjenjenih između MQTT poslužitelja i računala *ASI-OOB-1*, što potvrđuje ispravnost TLS komunikacije između računala.

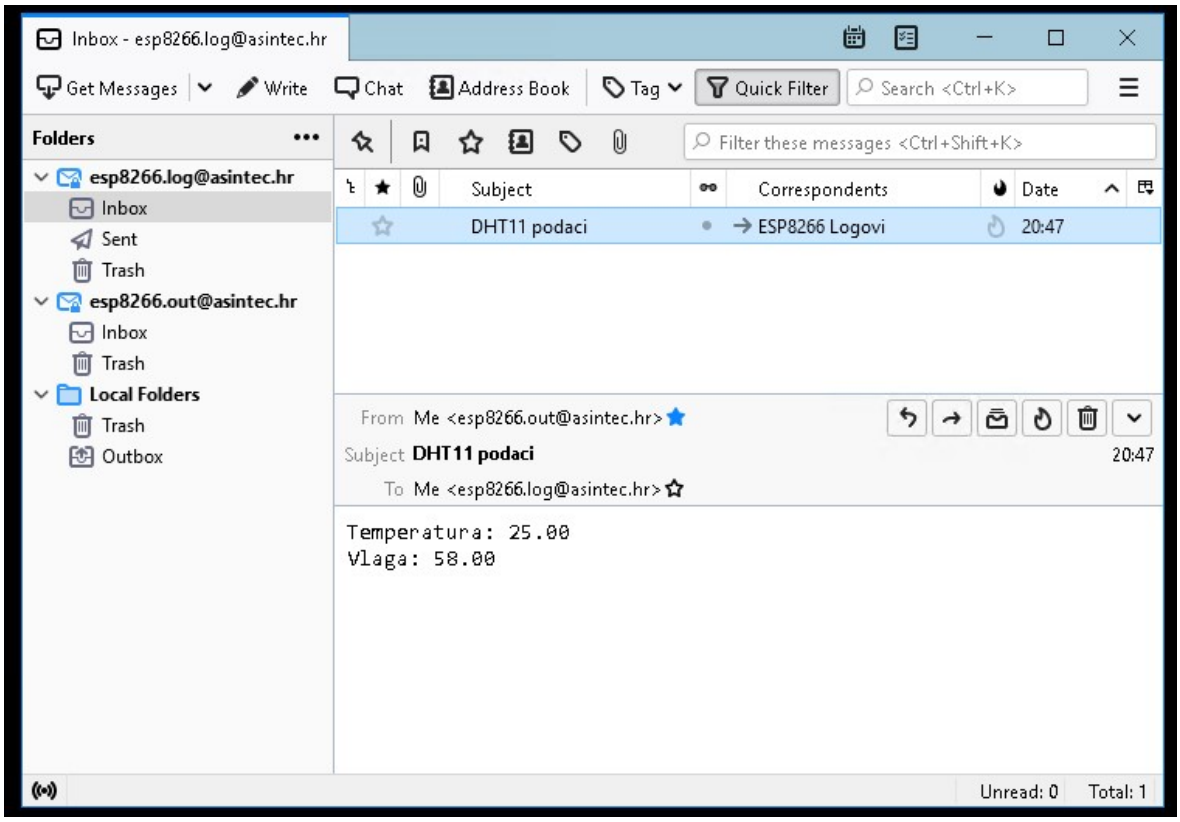


Slika 5.5: Prikaz mrežnog paketa poslanog prema računalu ASI-OOB-1 s MQTT poslužitelja. Izvor: vlastita preslika rada.

5.3 Primjena kriptiranja pomoću SMTP protokola

Za slanje pošte pomoću SMTP protokola, u programskom kodu mikroupravljača, za razliku od prošla dva protokola, nije potrebno spremiti certifikate i privatni ključ. Biblioteka *ESP-Mail-Client* u programskom okruženju *Arduino IDE* ima implementiran mehanizam za slanje e-pošte prema poslužiteljima s obaveznom kriptiranom komunikacijom pomoću TLS protokola.

Svakih 45 sekundi šalje se poruka e-pošte s podacima očitanim sa senzora DHT11 sa adrese esp8266.out@asintec.hr na adresu esp8266.log@asintec.hr. Slika 5.6. prikazuje klijent e-pošte *Mozilla Thunderbird* pokrenut na računalu *ASI-OOB-1*, koji ima postavljene obje adrese e-pošte, gdje je vidljiva pristigla poruka e-pošte u pretincu primajuće adrese.



Slika 5.6: Pretinac dolazne pošte adrese esp8266.log@asintec.hr u klijentu e-pošte Mozilla Thunderbird. Izvor: vlastita preslika rada.

Dodatni podaci o poruci e-pošte prikazuju se pogledom zaglavlja poruke, koje se može prikazati odabirom opcije *View Source...* u klijentu e-pošte *Mozilla Thunderbird*. U programskom kodu 5.3. izdvojeni su najbitniji parametri koji potvrđuju da je izvor poruke upravo s mikroupravljača.

```
Received: from ASI-MAIL01.asintec.hr (10.80.44.4) by ASI-
MAIL01.asintec.hr
 (10.80.44.4) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.2308.8
via Mailbox
 Transport; Fri, 10 Sep 2021 20:47:22 +0200
Received: from asintec.hr (10.80.45.3) by ASI-MAIL01.asintec.hr
(10.80.44.4)
 with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256) id 15.1.2308.8;
Fri, 10 Sep
 2021 20:47:22 +0200
From: ESP8266 Izlazni <esp8266.out@asintec.hr>
To: ESP8266 Logovi <esp8266.log@asintec.hr>
Subject: DHT11 podaci
```

Programski kod 5.3: Izvadak zaglavlja poruke e-pošte.

U prvom parametru nalazi se DNS naziv i IP adresa poslužitelja, zajedno s algoritmom korištenim za kriptiranu komunikaciju i datumom, dok se u drugom parametru nalazi IP adresa mikroupravljača, koja je navedena u tablici 1, zajedno s algoritmom korištenim za kriptiranu komunikaciju i datumom, što potvrđuje da je izvor poruke mikroupravljač. U trećem parametru nalazi se pošiljatelj poruke, a u četvrtom parametru primatelj poruke, dok se u zadnjem, petom parametru nalazi naslov poruke.

6. ZAKLJUČAK

Demonstracijom funkcionalnosti svakog od tri često korištena protokola u radu IoT uređaja potvrđuje se teza da je zahvaljujući uspješnom razvoju programskih okruženjima i biblioteka, koji su jednostavni za korištenje, implementiranje sigurnosti u IoT uređaju jednostavno i brzo. Navedeni IoT uređaj, odnosno mikroupravljač niske je cijene i potrošnje energije, no s niskim taktom procesora od 80 MHz i dalje dovoljno brzo izvršava zadatke i u kombinaciji s kompleksnim kriptografskim algoritmima, kao što su oni koji se koriste u radu TLS protokola.

Stranica u demonstraciji HTTPS protokola otvorila se u svega nekoliko sekundi, podaci u demonstraciji MQTT protokola prikazani su na poslužitelju u realnom vremenu, a e-pošta u demonstraciji SMTP protokola postala je vidljiva u klijentu e-pošte za svega deset sekundi, što je ponovno dokaz da je sigurnost IoT uređaja moguće potpuno implementirati uz malo uloženog vremena uz i dalje prihvatljive performanse uređaja.

Izdavanjem certifikata pri poznatijem certifikacijskom tijelu, kao što su *DigiCert*, *COMODO* ili *Let's Encrypt*, IoT rješenje spremno je za široku primjenu i izvan dosega unutarnje mreže, odnosno može biti dostupno i na Internetu, zato što u tom slučaju krajnji korisnik ne mora instalirati certifikate unutarnjih certifikacijskih tijela u operacijski sustav i/ili preglednik, budući da se certifikati poznatijih certifikacijskih tijela isporučuju s operacijskim sustavom i preglednikom te redovito ažuriraju.

Dodatni sloj zaštite, odnosno sigurnosti ostvaruje se implementacijom autentikacije pristupa pomoću korisničkog imena i zaporke koristeći neku od implementacija direktorija osnovanog na protokolu LDAP (engl. *Lightweight Directory Access Protocol*), npr. besplatna implementacija *OpenLDAP* ili implementacija tvrtke *Microsoft*, poznatija kao skraćenica AD LDS (engl. *Active Directory Lightweight Directory Services*), uz pomoć koje je autorizaciju moguće ostvariti i u testnom okruženju poput onoga koje je opisano u demonstraciji.

7. LITERATURA

[1] Statista, Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/, 2021. Pristupljeno 28. kolovoza 2021.

[2] Windpower Engineering Development, Global IoT market to reach $318 billion by 2023, says GlobalData. https://www.windpowerengineering.com/global-iot-market-to-reach-318-billion-by-2023-says-globaldata/, 2018. Pristupljeno 28. kolovoza 2021.

[3] Expressif, ESP8266EX Datasheet Version 6.6, https://www.espressif.com/sites/default/files/documentation/0a-esp8266ex_datasheet_en.pdf, listopad 2020. Pristupljeno 28. kolovoza 2021.

[4] Elecrow, WiFi module-The Difference Between ESP-12E and ESP-12F, https://www.elecrow.com/blog/things-you-should-know-about-esp8266-wifi-module.html, kolovoz 2021. Pristupljeno 28. kolovoza 2021.

[5] The United States Department of Justice, U.S. v. Microsoft: Court's Findings of Fact, https://www.justice.gov/atr/us-v-microsoft-courts-findings-fact, studeni 1999. Pristupljeno 29. kolovoza 2021.

[6] Digicert, The Evolution of SSL and TLS, https://www.digicert.com/blog/evolution-of-ssl, 2015. Pristupljeno 29. kolovoza 2021.

[7] Google, This POODLE Bites: Exploiting the SSL 3.0 Fallback, https://www.openssl.org/~bodo/ssl-poodle.pdf, rujan 2014. Pristupljeno 30. kolovoza 2021.

[8] Internet Engineering Task Force, The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446), https://www.rfc-editor.org/rfc/pdfrfc/rfc8446.txt.pdf, kolovoz 2018. Pristupljeno 29. kolovoza 2021.

[9] Nina Kuzmić, Lea Kuzminski, Renata Mesaroš, ECC kriptografija (Eliptične krivulje), https://security.foi.hr/wiki/index.php/ECC_kriptografija_(Elipti%C4%8Dne_krivulje).html . siječanj 2013. Pristupljeno 30. kolovoza. 2021.

[10] Svetlin Nakov, Practical Cryptography for Developers, ECDH Key Exchange, https://cryptobook.nakov.com/asymmetric-key-ciphers/ecdh-key-exchange. 2019. Pristupljeno 30. kolovoza 2021.

[11] Internet Engineering Task Force, Pre-Shared Key Ciphersuites for Transport Layer Security (TLS), https://datatracker.ietf.org/doc/html/rfc4279, prosinac 2005. Dostupno 10. rujna 2021.

[12] SecureW2, Root vs Intermediate Certificates and CAs. https://www.securew2.com/blog/root-vs-intermediate-certificates-cas, 2021. Pristupljeno 29. kolovoza 2021.

[13] Keyfactor, What is PKI and How Does it Work?, https://www.keyfactor.com/resources/what-is-pki/. 2021. Pristupljeno 30. kolovoza 2021.

[14] Sectigo, What Is An X.509 Certificate & How Does It Work?, https://sectigo.com/resource-library/what-is-x509-certificate, siječanj 2021. Pristupljeno 30. kolovoza 2021.

[15] GeeksForGeeks, RSA Algorithm in Cryptography, https://www.geeksforgeeks.org/rsa-algorithm-cryptography/. siječanj 2021. Pristupljeno 30. kolovoza 2021.

[16] Dr. Herong Yang, Introduction of DSA (Digital Signature Algorithm), http://www.herongyang.com/Cryptography/DSA-Introduction-What-Is-DSA-Digital-Signature-Algorithm.html, 2021. Pristupljeno 30. kolovoza 2021.

[17] Mailtrap by Railsware, Diana Lepilkina, Simple Mail Transfer Protocol, https://mailtrap.io/blog/smtp/, srpanj 2020. Pristupljeno 30. kolovoza 2021.

[18] HiveMQ, Introducting the MQTT Protocol – MQTT Essentials: Part 1, https://www.hivemq.com/blog/mqtt-essentials-part-1-introducing-mqtt/, 12. siječanj 2015. Pristupljeno 10. rujna 2021.

[19] Jeff Kaufman, History of HTTPS Usage, https://www.jefftk.com/p/history-of-https-usage, 8. ožujak 2018. Pristupljeno 10. rujna 2021.

8. OZNAKE I KRATICE

AD - Active Directory

CA - Certificate Authority

CN – Common Name

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name System

DSA – Digital Signature Algorithm

ECC – Elliptic Curve Cryptography

ECDH – Elliptic-Curve Diffie-Herrman

ECDHE – Elliptic-Curve Diffie-Herrman Ephemeral

HTTP – HyperText Transfer Protocol

HTTPS - HyperText Transfer Protocol Secure

IBM – International Business Machines

IDE – Integrated Development Environment

IMAP4 – Internet Mail Access Protocol, verzija 4

IP - Internet Protocol

LED – Light Emitting Diode

LDAP – Lightweight Directory Access Protocol

MMC – Microsoft Management Console

MQTT - MQ Telemetry Transport

OOB - Out-Of-Band Management

PKCS – Public Key Cryptography Standards

PKI – Public Key Infrastructure

POODLE – Padding Oracle On Downgrading Legacy Encryption

POP3 – Post Office Protocol, verzija 3

SMTP – Simple Mail Transfer Protocol

SSL - Secure Sockets Layer

TLS - Transport Layer Security

Wi-Fi – Wireless Fidelity

9. SAŽETAK

Naslov: Primjena kriptografskih tehnika u IoT-u

Ovaj rad bavi se implementacijom kriptiranja komunikacije IoT uređaja osnovanog na ESP8266 mikroupravljaču. Procedura i koraci implementacije opisani su koristeći tri često korištena protokola, a to su: HTTPS protokol za upravljanje uređajem, MQTT protokol za prikaz podataka te SMTP protokol za slanje obavijesti putem e-pošte. Demonstracija je provedena koristeći uređaj osnovan na ESP8266 mikroupravljaču koji je programiran koristeći Arduino IDE razvojno okruženje te domenu osnovanu na operacijskom sustavu Microsoft Windows, koja ima ulogu PKI infrastrukture male fiktivne tvrtke. Infrastruktura upravlja certifikatima koji se koriste za kriptiranje komunikacije. Domena također sadrži unutarnji DNS poslužitelj koji sadrži domenske nazive upisane u certifikate koji se koriste za demonstraciju implementacije kriptiranja.

Ključne riječi: Internet stvari, SMTP, MQTT, HTTPS, certifikat.

10. ABSTRACT

Title: Use of cryptographic techniques in IoT

This paper discusses the implementation of communication encryption of an IoT device based on the ESP8266 microcontroller. The procedure of the implementation is described for the three widely used protocols in IoT devices: HTTPS for controlling the device, MQTT for data display and SMTP for e-mail notifications. The demonstration is carried out using a device based on the ESP8266 microcontroller programmed in the Arduino IDE environment and a Microsoft Windows domain, which is used as the PKI infrastructure of a fictional small company and manages certificates used for encryption, together with an internal DNS server, which contains the domain names populated in certificates which will be used for the demonstration of the encryption implementation.

Keywords: Internet of Things, SMTP, MQTT, HTTPS, certificate.

IZJAVA O AUTORSTVU ZAVRŠNOG RADA

Pod punom odgovornošću izjavljujem da sam ovaj rad izradio/la samostalno, poštujući načela akademske čestitosti, pravila struke te pravila i norme standardnog hrvatskog jezika. Rad je moje autorsko djelo i svi su preuzeti citati i parafraze u njemu primjereno označeni.

Mjesto i datum	Ime i prezime studenta/ice	Potpis studenta/ice
U Bjelovaru, 6. listopada 2021.	Zvonimir Žarinac	Ž.

Prema Odluci Veleučilišta u Bjelovaru, a u skladu sa Zakonom o znanstvenoj djelatnosti i visokom obrazovanju, elektroničke inačice završnih radova studenata Veleučilišta u Bjelovaru bit će pohranjene i javno dostupne u internetskoj bazi Nacionalne i sveučilišne knjižnice u Zagrebu. Ukoliko ste suglasni da tekst Vašeg završnog rada u cijelosti bude javno objavljen, molimo Vas da to potvrdite potpisom.

Suglasnost za objavljivanje elektroničke inačice završnog rada u javno dostupnom nacionalnom repozitoriju

Zvonimir Žadnac

ime i prezime studenta/ice

Dajem suglasnost da se radi promicanja otvorenog i slobodnog pristupa znanju i informacijama cjeloviti tekst mojeg završnog rada pohrani u repozitorij Nacionalne i sveučilišne knjižnice u Zagrebu i time učini javno dostupnim.

Svojim potpisom potvrđujem istovjetnost tiskane i elektroničke inačice završnog rada.

U Bjelovaru, 6. listopada 2021.

Ž

potpis studenta/ice