Korisničko uputstvo

PKI infrastruktura – instalacija neophodnih certifikata Ovjerioca i software-a, i upotreba certifikata na USB Tokenu

Sadržaj

Uvod

„JP BH POŠTA“ d.o.o. Sarajevo je uspostavila infrastrukturu javnih kriptografskih ključeva – Public Key Infrastructure – PKI i djeluje kao ovjerilac u skladu s Zakonom o elektronskom potpisu. Kao ovjerilac, „JP BH POŠTA“ d.o.o. pruža usluge izdavanja kvalificiranih elektronskih potvrda i upravljanja njihovim životnim ciklusom, kao i izdavanja kvalificiranih elektronskih vremenskih žigova pod imenom: Ovjerilac JP BH POŠTA.

Za uspješno korištenje kvalificirane elektronske potrvde (digitalnog certifikata) Ovjerioca JP BH Pošta potrebno je da su obezbjeđeni slijedeći preduslovi:

1. instalirani CA certifikati Ovjerioca JP BH Pošta na računaru korisnika
2. instaliran driver za token (tzv. middleware software)
3. posjedovanje PIN koda za pristup tokenu
4. Pristup Internetu za provjeru CRL liste

Kvalificirane elektronske potvrde koje izdaje Ovjerilac JP BH Pošta mogu se koristiti za potpisivanje elektronskih dokumenata kao i za autentikaciju prilikom pristupa nekoj računarskoj platformi (računar, server, web aplikacija i sl.). Digitalni dokumenti se mogu potpisati u okviru aplikacija poput Microsoft Office, Acrobat Reader, kao i aplikacija koje su namjenski razvijene za pružanje specifičnih servisa na Internetu (prijava poreza, podnošenje zahtjeva prema organima uprave,...). Internet servisi koji daju uslugu na teritoriji BiH prihvatanjem kvalificirane elektronske potvrde Ovjerioca JP BH Pošta izvršili su sigurnu identifikaciju osobe koja je pristupila servisu.

1 Instalacija certifikata Ovjerioca JP BH Pošta

Da bi se uspješno koristili certifikati Ovjerioca potrebno je na korisničkom računaru učitati certifikate CA servera kao pouzdane (uspostavljanje relacije povjerenja). Instalacija certifikata CA servera izvodi se na način koji je opisan u nastavku.

1.1 *Preuzimanje certifikata sa web stranice*

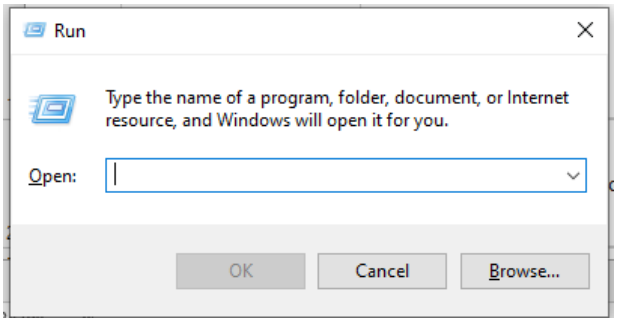
Certifikati CA servera Ovjerioca JP BH Pošta dostupni su na zvaničnoj web stranici „JP BH Pošta“ d.o.o. Potrebno je sa navedene lokacije preuzeti datoteke bhp-rootca.zip, bhp-subca.zip i bhp-subca2.zip, te iste dekompresovati (raspakovati) na nekoj privremenoj lokaciji (npr. Downloads folder) upotrebom nekog od alata za tkz. zipovanje datoteka (WinZip, 7-zip i sl.). Nakon procesa dekompresije u folderu će se pojaviti datoteke BHP-RootCA.der, BHP-SubCA.der i BHP-SubCA2.der.

1.2 Otvaranje MMC konzole – pomoćnog alata za učitavanje certifikata CA servera

Učitavanje certifikata CA servera Ovjerioca JP BH Pošta može se izvršiti na više načina. U ovom uputstvu učitavanje certifikata izvršićemo uz pomoć MMC konzole. MMC konzola je pomoćni Microsoft alat, u okviru samog operativnog sistema računara, koji omogućava pristup pojedinim funkcionalnostima. Za uspješno učitavanje certifikata CA servera Ovjerioca JP BH Pošta, upotrebom MMC konzole, potrebno je na računaru imati privilegije administratora.

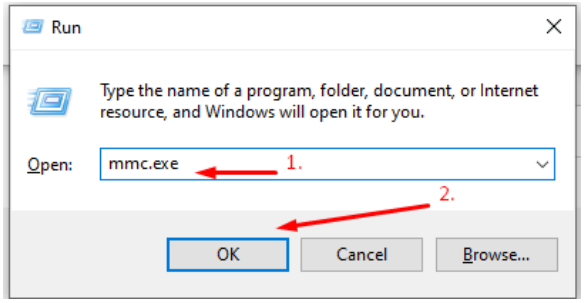
Nakon što ste se prijavili sa administratorskim privilegijama potrebno je provesti postupak naveden u narednih nekoliko koraka:

- Pokrenuti pomoćni program mmc.exe na slijedeći način: istovremenim pritiskom na Windows logo tipku (⊞) i tipku slova R otvorit će se Run prozor kao na slici 1.



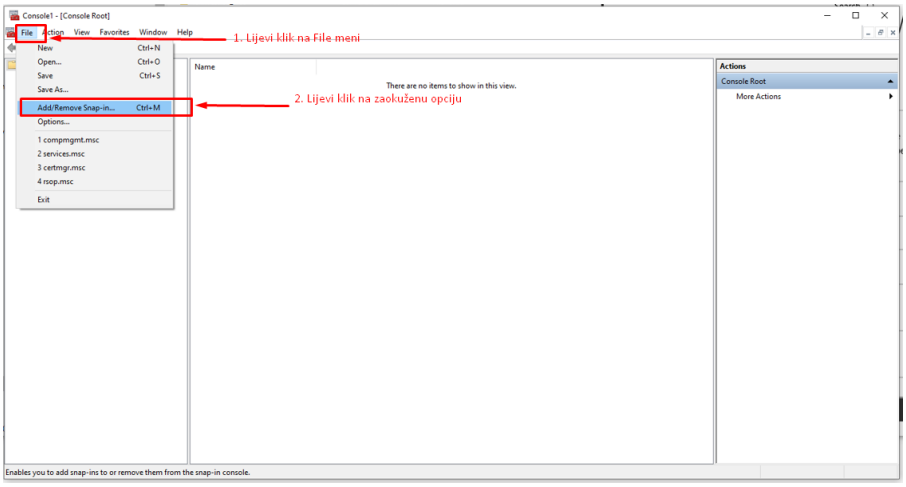
Slika 1 – otvaraje Run prozora

- U otvorenom prozoru, u dijelu naznačenom sa open, potrebno je unijeti **mmc.exe** i potvrditi klikom na OK dugme u prozoru – slika 2.



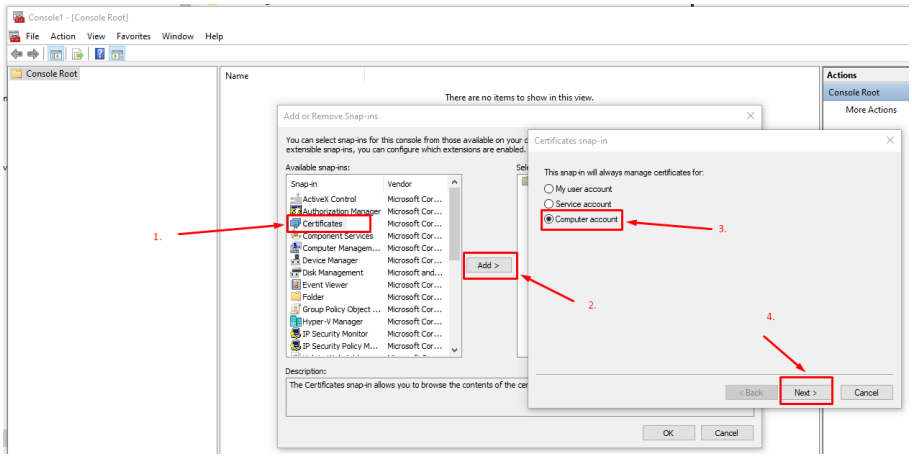
Slika 2 – pokretanje MMC konzole

MMC konzola omogućava pristupanje različitim funkcionalnostima. Za naše potrebe mi ćemo uz pomoć mmc konzole pristupiti funkcionalnostima potrebnim za upotrebu certifikata. Prvi korak je dodavanje i otvaranje odgovarajućeg Snap-ina – slika 3. Lijevim klikom miša na File meni otvara nam se niz opcija od kojih je potrebno odabrati opciju Add/Remove Snap-inn...



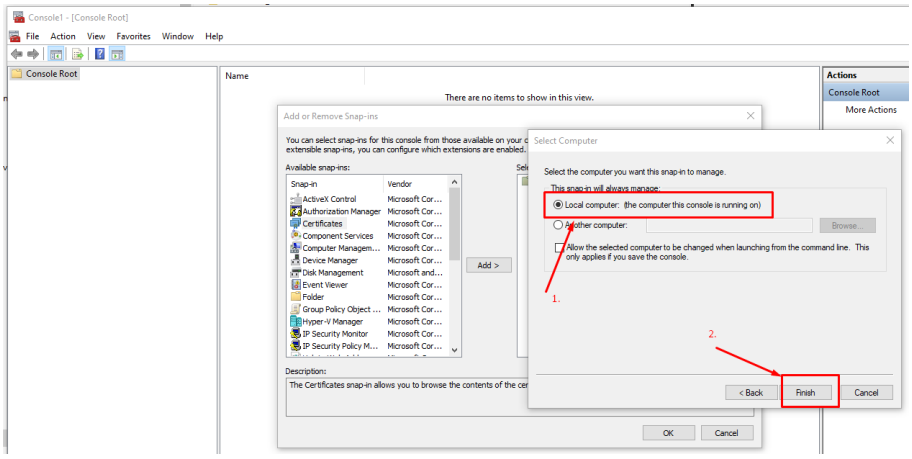
Slika 3 – otvaranje odgovarajućeg Snap-ina

Kao rezultat prethodne operacije otvara nam se novi prozor Add or Remove Snap-ins. Sa lijeve strane nalazi se lista dostupnih funkcionalnosti za koje je moguće izvršiti daljnja podešavanja. Potrebno je odabrati, u polju Available Snap-ins, segment označen kao **Certificates**, te kliknuti na dugme **Add** (u sredini), kako bi se izvršilo dodavanje opcije za pregled i upravljanje certifikatima, a koja nam je i potrebna. Klikom na dugme Add otvara se novi prozor gdje je potrebno odabrati segment na koji se primjenjuje sam Snap-in certifikata. Za naše potrebe biramo **Computer account**, odnosno primjenu na nivou računara. Klikom na opciju next u dnu prozora prelazimo na novi prozor. Svi navedeni koraci prikazani su na slici 4.



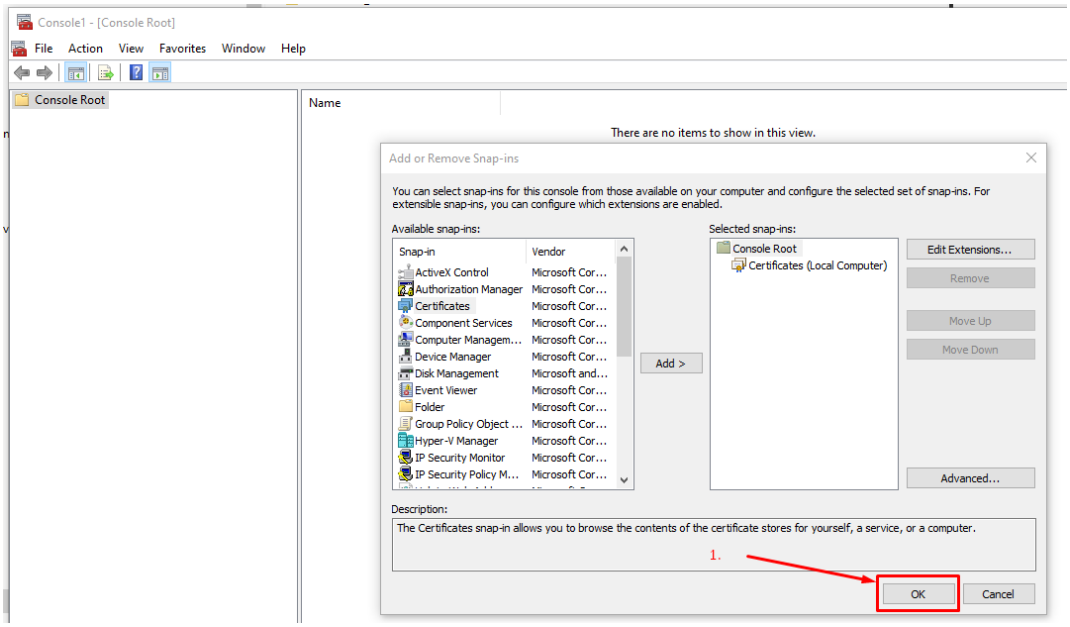
Slika 4 – dodavanje funkcionalnosti za certifikate u Snap-in

Klikom na next u prethodnom koraku dolazimo do novog prozora za odabir računara sa kojeg će se učitati postojeće postavke, a i na koji će se primjenjivati sve promjene. U našem slučaju portebno je izabrati opciju Local Computer, odnosno računar na kojem se i pokreće sama konzola. Nakon odabira ove opcije (koja je po početnim postavkama već i označena), klikom na dugme Finish završavamo odabir postavki, te se vraćamo na prozor sa početka dodavanja snap-inna – slika 5.



Slika 5 – odabir računara na kojem se izvršavaju promjene

Za otvaranje konzole potrebno je još potvrditi sve prethodno provedene korake klikom na dugme OK, čime se konzola otvara – slika 6.



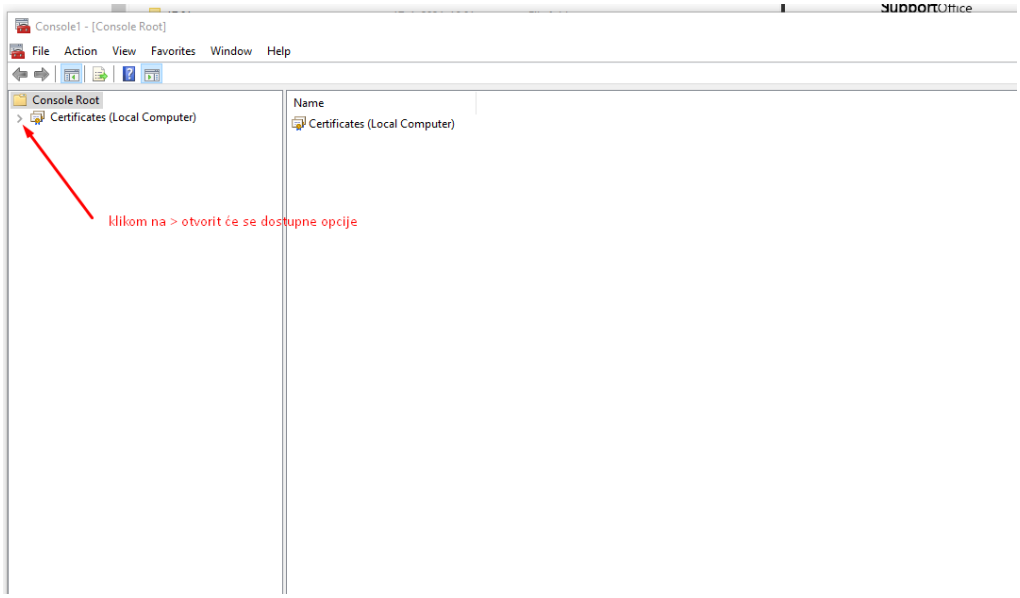
Slika 6 – potvrđivanje odabranih postavki i otvaranje konzole

1.3 Učitavanje CA certifikata

Certifikate CA servera Ovjerioca JP BH Pošta čine tri(3) certifikata, a koja smo prethodno dobavili, downloadovali sa web stranice JP BH Pošta d.o.o. Sarajevo, te ih pohranili na određenu lokaciju na lokalnom računaru. Certifikati koje je potrebno učitati u store – smještajno mjesto su RootCA i SubCA certifikati.

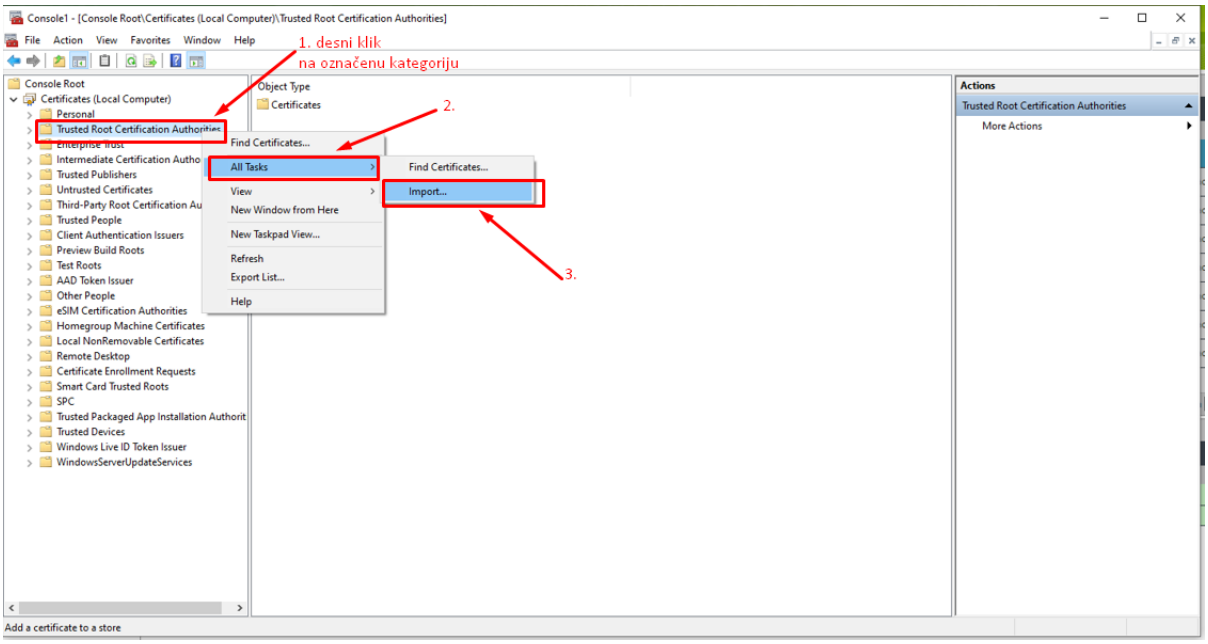
1.3.1 Učitavanje certifikata RootCA servera (naziv datoteke BHP-RootCA.der)

U otvorenoj MMC konzoli sada imamo, u okviru Console Root segmenta, prikazanu funkcionalnost koja je vezana za Certifikate. Učitavanje certifikata CA servera Ovjerioca JP BH Pošta izvršićemo pod odgovarajućim segmentima. Do tih segmenata dolazimo klikom na > a koji se nalazi ispred Certificates (Local Computer) opcije – slika 7.



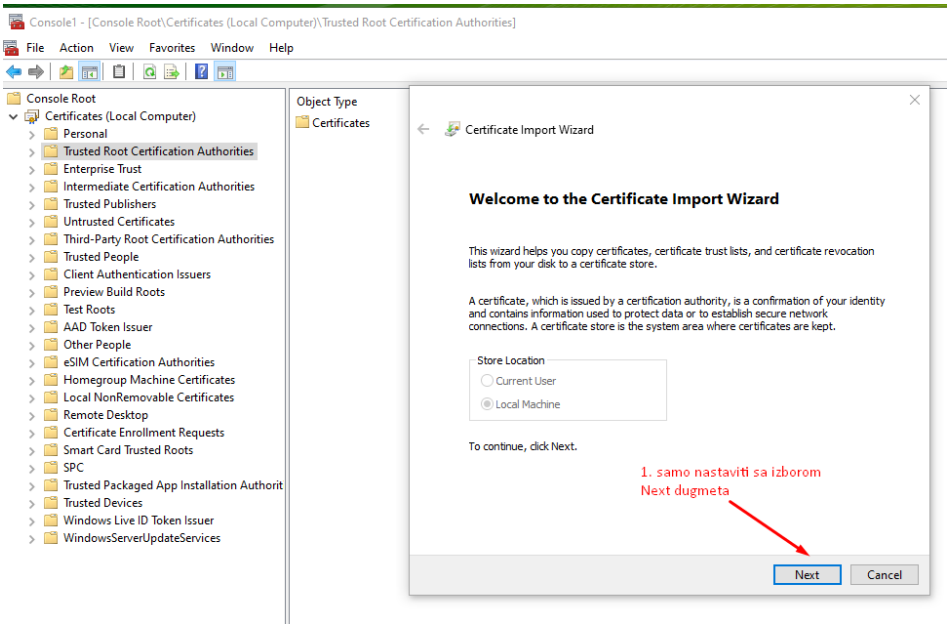
Slika 7 – otvaranje liste dostupnih opcija – smještajnih prostora certifikata

Izvršavanje prethodnog koraka pojavljuje nam se veći broj opcija, a koje u prinicipu predstavljaju mjesta, odnosno smještajni prostor, na kojem sam operativni sistem računara pohranjuje na računaru pristutne certifikate. Sada je potrebno da u odgovarajući Store - smještajni prostor dodamo i Certifikate Ovjerioca. Predmetne certifikate dodajemo u Trusted Root Certification Authorities segment i to desnim klikom na navedenu kategoriju u odabirom opcije All Tasks > Import... Navedeno je prikazano na slici 8.



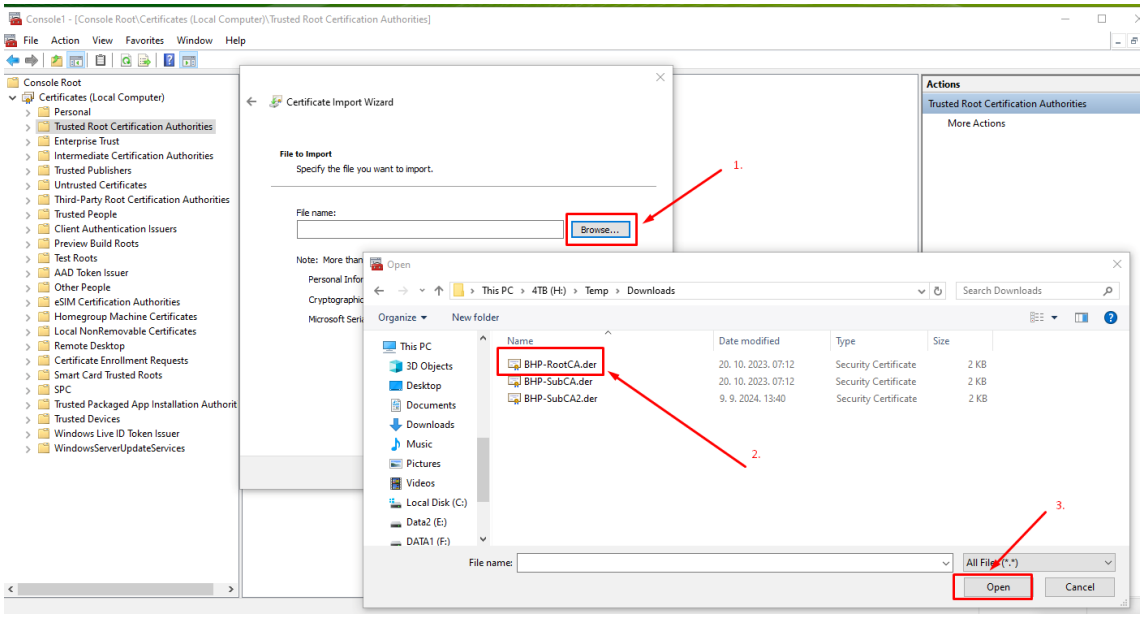
Slika 8 – dodavanje certifikata u odgovarajući store – smještajni prostor

Prethodno provedeno dovodi nas do novog prozora u kojem se provodi procedura za učitavanje potrebnih certifikata. Prozor za dobrodošlicu nudi osnovne informacije, te prikaz već prethodno odabrane opcije o storeu na koji se odnosi sama opcija učitavanja (da li na nivou korisnika ili lokalnog računara, a što smo birali u prethodnim koracima). Proces učitavanja ovdje samo nastavljamo klikom na Next – slika 9.



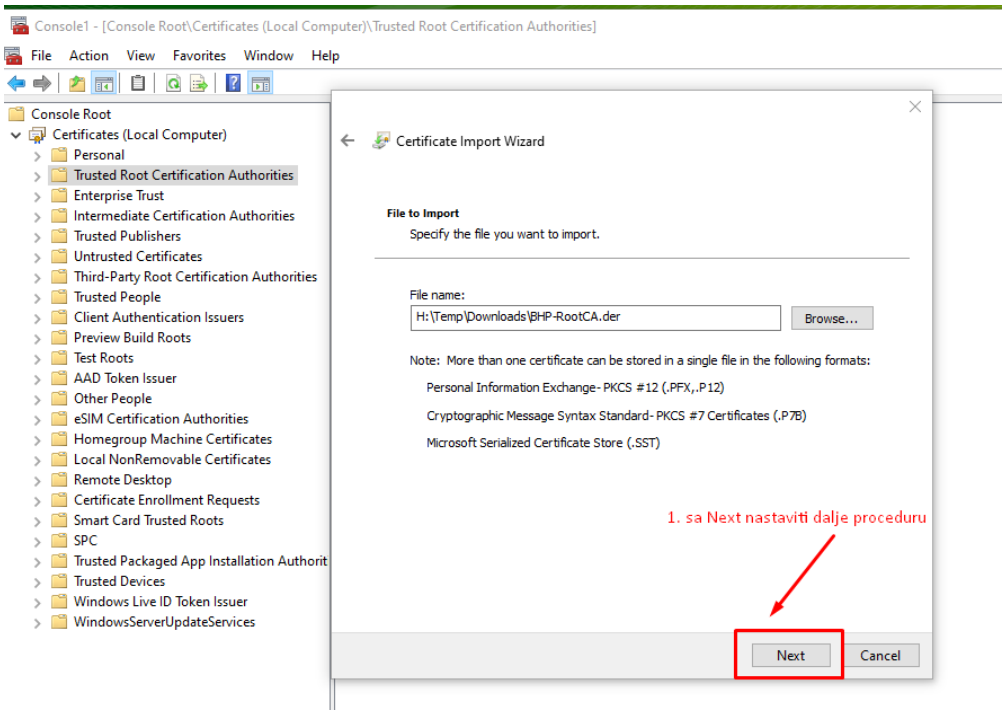
Slika 9 – nastavak procesa učitavanja certifikata u okviru Wizarda

U sljedećem koraku potrebno je odabrati certifikat koji je potrebno učitati. Odabir izvršavamo klikom na dugme Browse koje nam u novom prozoru omogućava da nađemo certifikat(e) koje želimo i da učitamo, sa putanje na kojoj nam se oni i nalaze. Nakon što odaberemo putanju na koju smo smjestili certifikate, odaberemo jedan od njih selektovanjem, te klikom na opciju Open, vraćamo se na opciju odabira filea, odnosno certifikata, za import – slika 10.



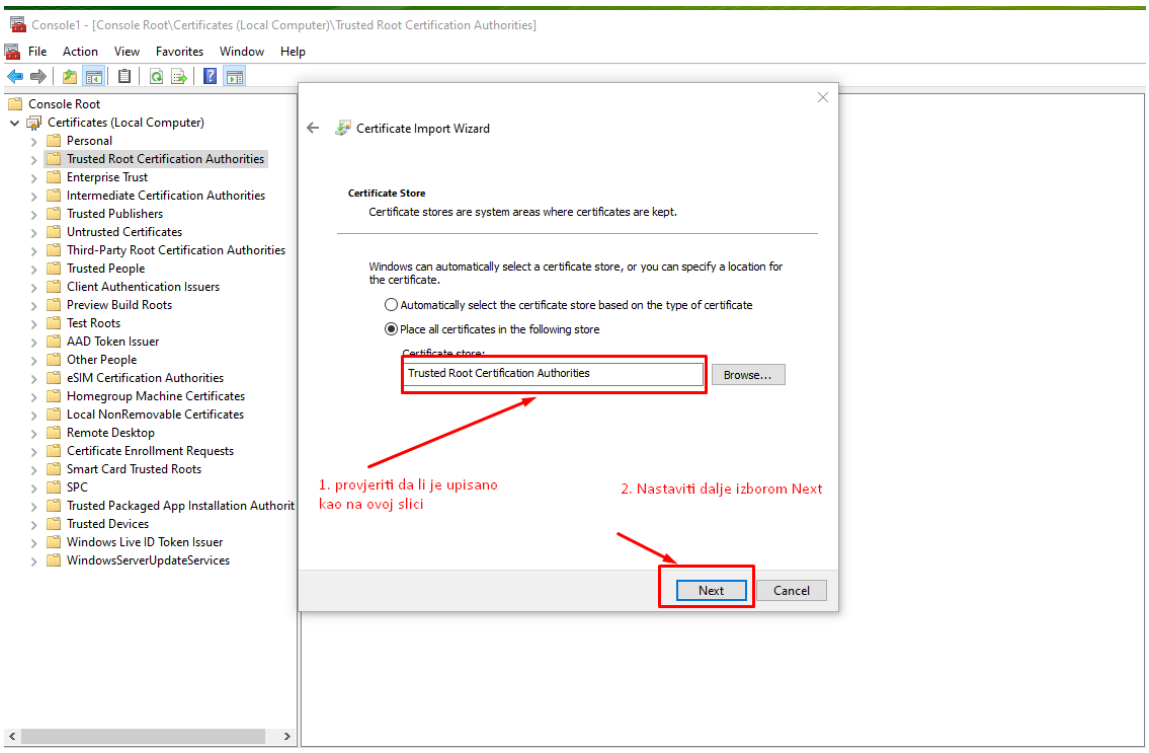
Slika 10 – odabir odgovarajućeg certifikata za učitavanje

U prozoru File to import možemo sada primijetiti i provjeriti da polje File name nije prazno (kao što je bilo prvobitno prije provođenja prethodnog koraka), već je u njemu upisano samo ime našeg certifikata, zajedno sa punom putanjom na kojem se isti nalazi. Klikom na opciju Next potvrđujemo odabir certifikata čije će se učitavanje izvršiti – slika 11.



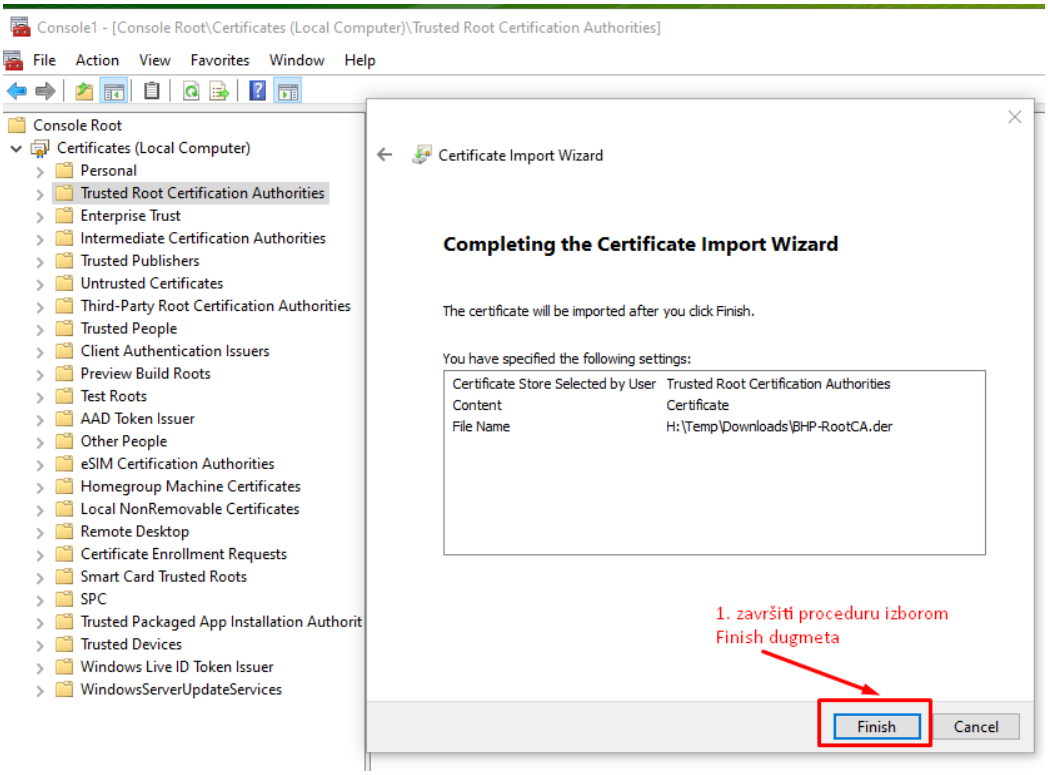
Slika 11 – potvrđivanje odabira odgovarajućeg certifikata, sa putanjom na kojoj se isti nalazi

U narednom koraku imamo ponuđenu opciju za odabir odgovarajućeg Storea, odnosno smještajnog prostora, gdje će operativni sistem pohranit naš certifikat kojeg učitajemo. Kako smo sam proces već pokrenuli sa odgovarajućeg storea u segmentu Certificate store trebalo bi da već stoji upisano „Trusted Root Certification Authorities“. Provjeriti da li je ovo u prikazano, te klikom na Next prelazimo na naredni korak – slika 12. Ukoliko pak nije odabrana ova odgovarajuća opcija, potrebno je ovdje izvršiti ovaj odabir klikom na dugme Browse, te odabirom prethodno navedenog storea.



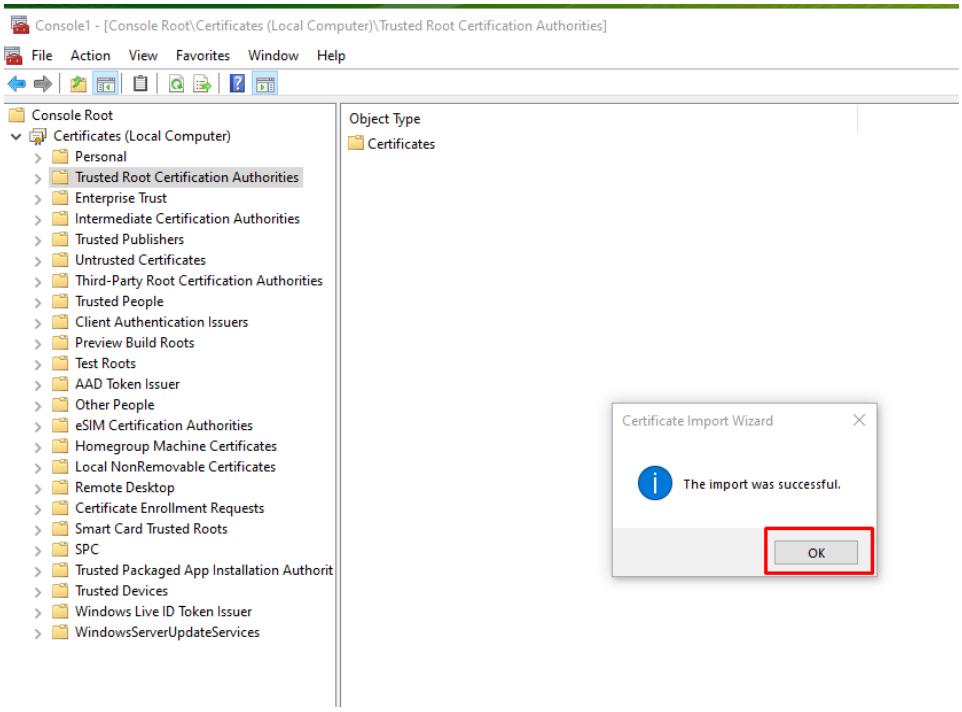
Slika 12 – provjera storea – smještajnog prostora certifikata

Okončanje postupka učitavanja certifikata završava se klikom na opciju Finish, na završnom prozoru. Na istom prozoru prikazane su i sve opcije koje smo odabrali, te koje možemo još jednom provjeriti ukoliko ima potrebe – slika 13.



Slika 13 – potvrđivanje opcija i završetak procedure za učitavanje certifikata

Po okončanju ovog postupka operativni sistem računara izvršava učitavanje odabranog certifikata. Ovisno o performansama računara proces može i potrajati neko kraće vrijeme, te po okončanju procesa učitavanja, ukoliko je isti uspješan, pojavljuje nam se automatski poruka koja nas i obavještava da je certifikat uspješno učitan – importovan. Poruka je prikazana na slici 14. Klikom na ok zatvaramo ovaj informativni prozor.

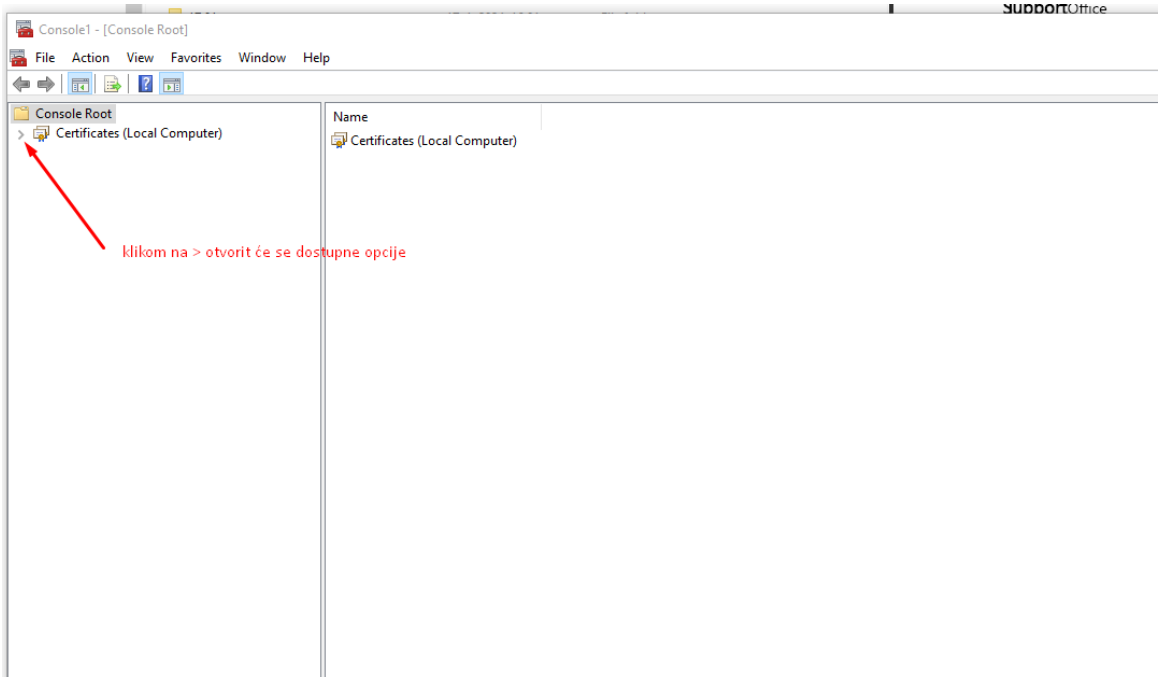


Slika 14 – poruka o uspješno izvršenom učitavanju certifikata

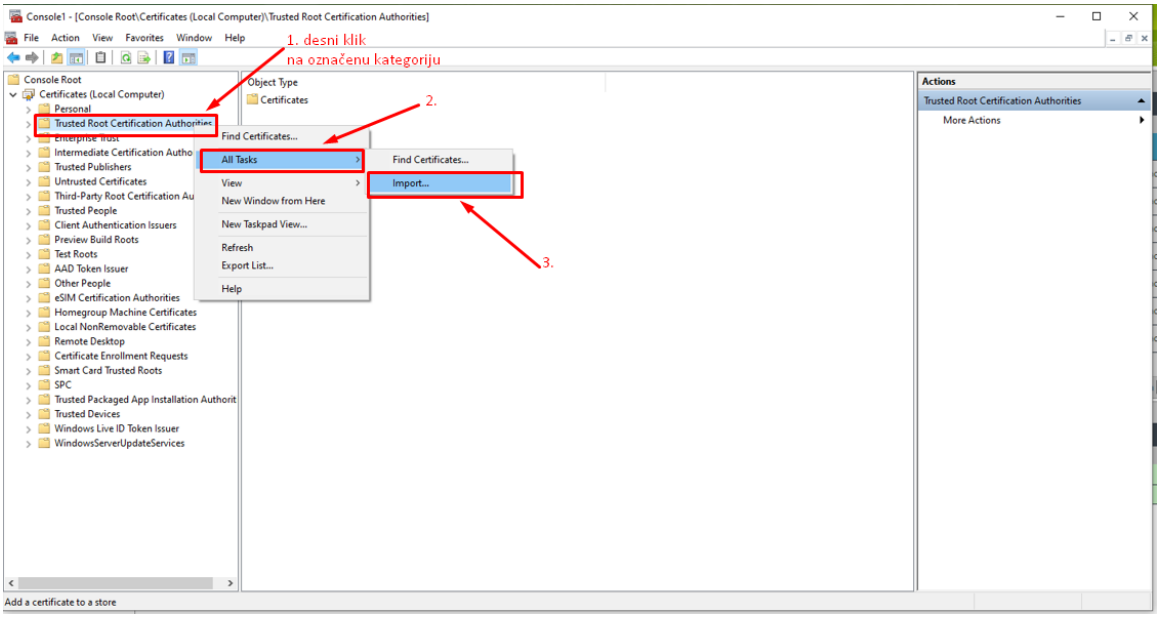
Praćenjem navedene procedure učitavanje certifikata trebalo bi se uspješno izvršiti. Ukoliko pak nismo dobili poruku da je certifikat uspještno učitan potrebno je dodatno ispitati uzrok, otkloniti eventualne probleme, te ponovo provesti proceduru, sve dok učitavanje ne bude uspješno. Potencijalni problemi mogu biti manjak administratorskih ovlasti, pogrešno odabran certifikat i slično. Ipak bez adekvatno učitanih certifikata Ovjerioca sistem neće raditi na potreban način.

1.3.2 Učitavanje certifikata SubCA servera (naziv datoteka BHP-SubCA.der i BHP-SubCA2.der)

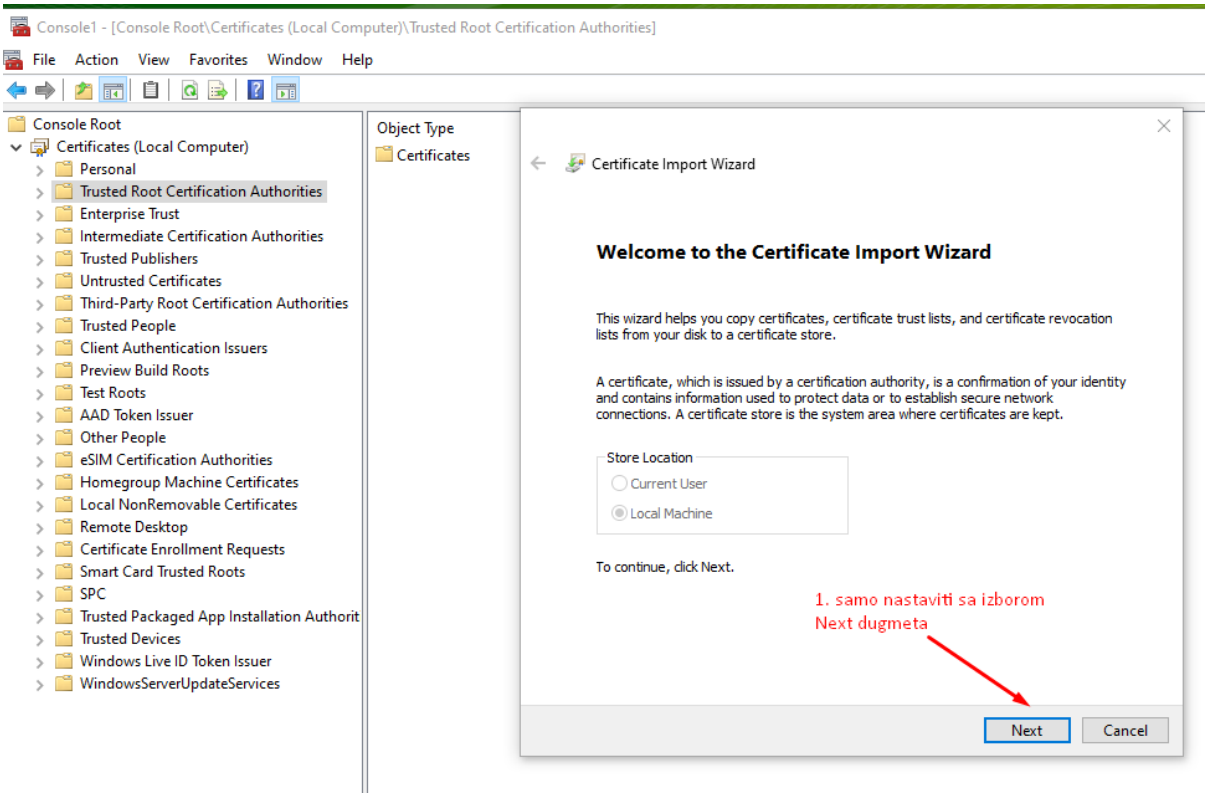
Učitavanje certifikata SubCA servera (dva certifikata) vrši se na isti način kao i prethodno detaljno opisano učitavanje certifikata RootCA servera. Jedina razlika se ogleda u tome što je dijelu u kojem se bira sam certifikat koji se učitava potrebno odabrati odgovarajući certifikat, kao što je rađeno i kod certifikata RootCA servera. Stoga je sam postupak dat samo na slikama 15 – 22, dok se za detaljne upute mogu koristiti opisi iz prethodnog segmenta. Kako u slučaju SubCA certifikata imamo dva certifikata ponavlja se identičan postupak dva puta, uz potrebu odabira dva različita certifikata. Na slici 18 prikazan je postupak sa BHP-SubCA.der certifikatom, dok je u drugom prolazu potrebno odabrati BHP-SubCA2.der certifikat. Također i ovdje se koristi MMC konzola za učitavanje certifikata.



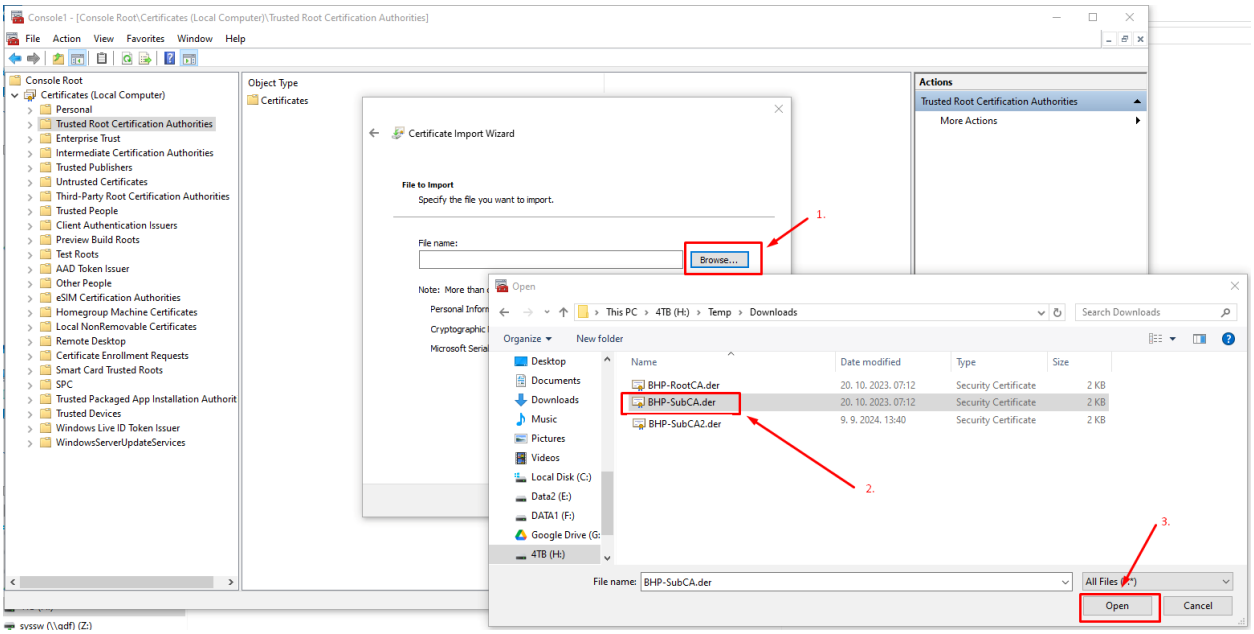
Slika 15 – otvaranje liste dostupnih opcija – smještajnih prostora certifikata



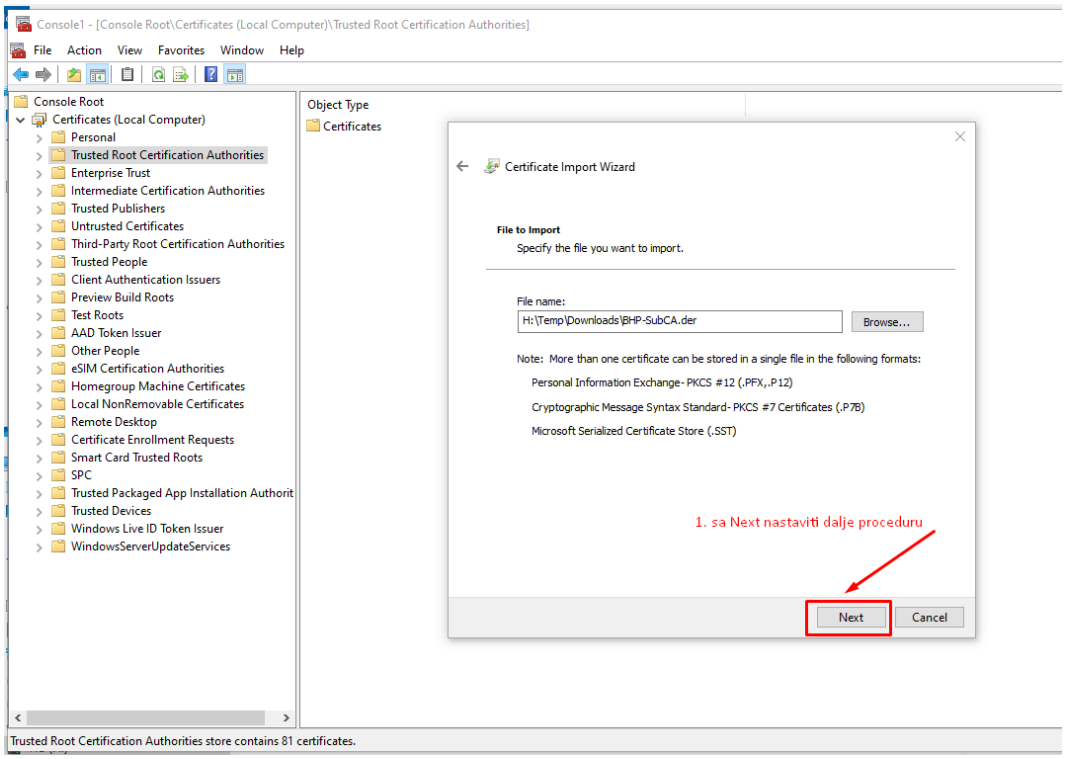
Slika 16 – dodavanje certifikata u odgovarajući store – smještajni prostor



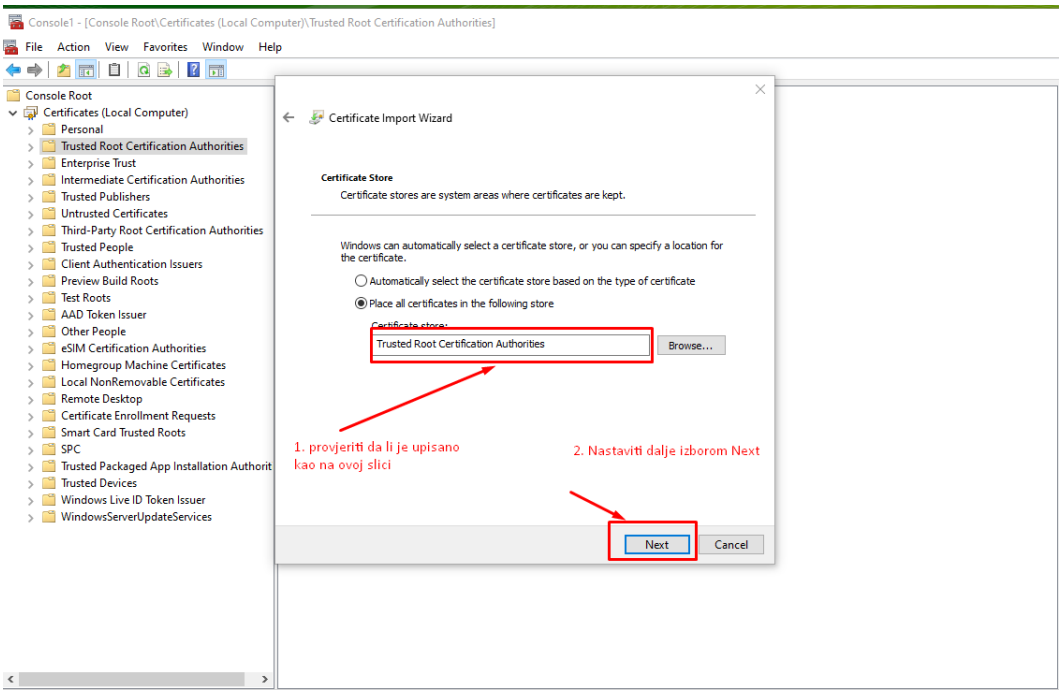
Slika 17 – nastavak procesa učitavanja certifikata u okviru Wizarda



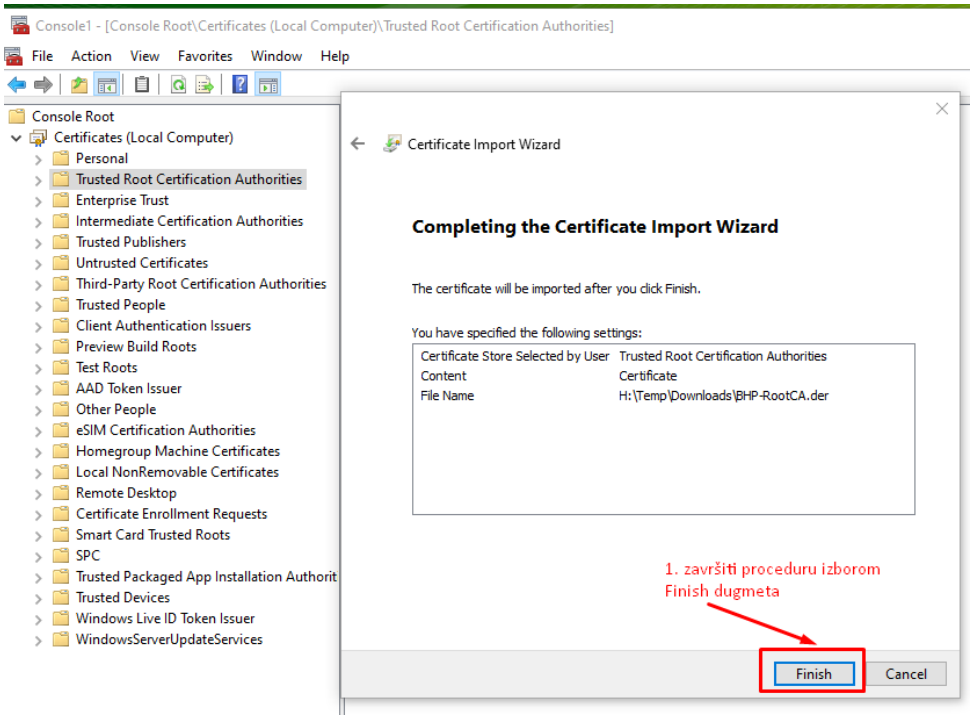
Slika 18 – odabir odgovarajućeg certifikata za učitavanje



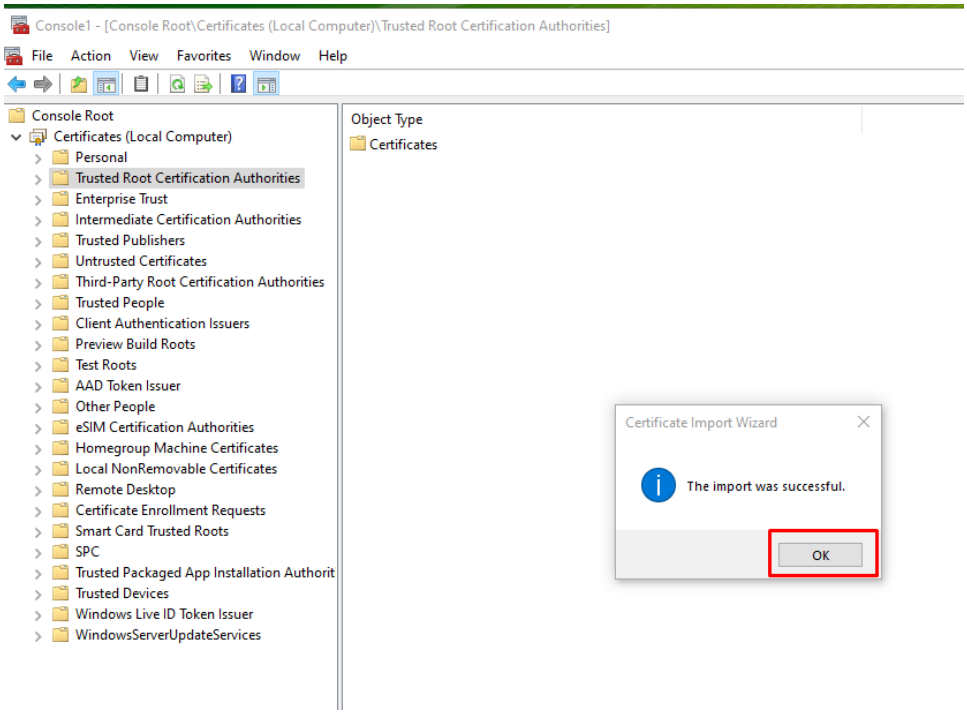
Slika 19 – potvrđivanje odabira odgovarajućeg certifikata, sa putanjom na kojoj se isti nalazi



Slika 20 – provjera storea – smještajnog prostora certifikata



Slika 21 – potvrđivanje opcija i završetak procedure za učitavanje certifikata



Slika 22 – poruka o uspješno izvršenom učitavanju certifikata

Nakon uspješnog učitavanja sva tri certfikata (certifikati CA servera) računar je podešen da vjeruje cerifikatima koje je izdao Ovjerioc JP BH Pošta, a što je neophodan korak za uspješno i odgovarajuće korištenje digitalnog certifikata izdanog od JP BH Pošta d.o.o. Međutim, za korištenje certifikata koji ste nabavili od JP BH Pošta d.o.o potrebno je instalirati i driver za USB token, na kojem se nalazi certifikat, kako bi računar uopšte prepoznao sam uređaj. Potrebni koraci za instalaciju driver-a dati u u nastavku.

2 Instalacija driver-a za token (tzv. middleware software)

Analogno kao kod dodavanja novog printera, web kamere ili sličnih eksternih uređaja, potrebno je da računar na koji se vežu uređaji sadrži i određene komade softvera – drivere, koji identificiraju sam uređaj te omogućavaju računaru komunikaciju i rad sa istim. Ukoliko ne postoje adekvatni driveri računar ne može da se poveže sa uređajem te se dobijaju poruke kao da isti nije prepoznat.

Za određene uređaje računar, odnosno operativni sistem, već ima potrebne drivere. Međutim, kako se ovdje radi o specifičnim uređajima potrebene drivere za prepoznavanje uređaja i komunikaciju računara sa istim potrebno je ručno instalirati. Radi se dakle o standardnoj i uobičajnenoj proceduri.

Datoteke koje su neophodne za instalaciju potrebnog drivera možete preuzeti sa linka https://www.posta.ba/e-potpis/preuzimanje_software-a. U zavisnosti od verzije operativnog sistema vašeg računara potrebno je odabrati i adekvatnu instalacijsku datoteku, 32-bit ili 64-bit verziju (za sve novije računare uglavnom se radi 64-bit verziji, dok 32-bit veerzija može biti na računarima koji su stari 10-tak i više godina).

Nakon što preuzmete potrebnu datoteku sa gore navedene web putanje potrebno je izvršiti instalaciju odgovarajućeg drivera, a koraci su dati u nastavku. Prethodno je potrebno se prijaviti kao administrator, odnosno da korisnički račun – account pod kojim se vrši instalacija ima administratorske privilegije na samom računaru.

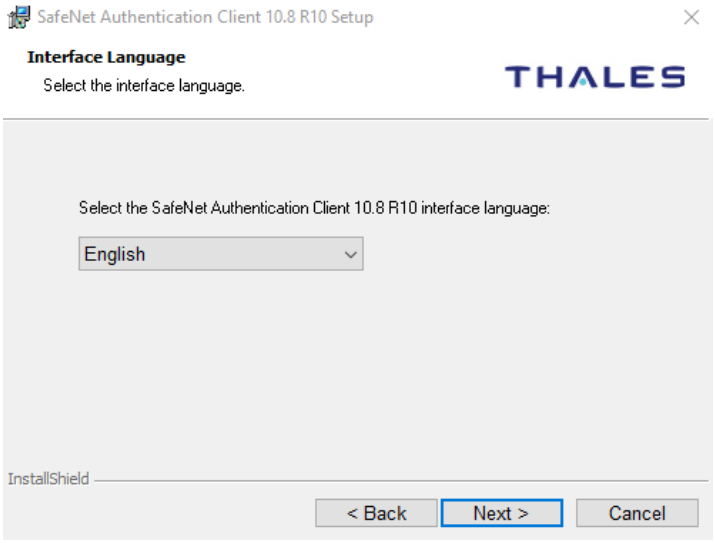
Također, poželjno je da se prije početka instalacije zatvore sve druge aplikacije. Pokretanje same instalacije može se uraditi na više načina, a jedan od njih je dvostruki/dupli klik na odgovarajuću datoteku:

- Dvostruki klik na odgovarajući datoteku (ovisno o sistemu):
  - SafeNetAuthenticationClient-x32-10.8-R6.msi (32-bit) ili
  - SafeNetAuthenticationClient-x64-10.8-R6.msi (64-bit)

Uspješnim pokretanjem instalacije, na prethodno opisan način, dolazimo do početnog ekrana - slika 23. Klikom na next počinjemo sa instalacijom.

Slika 23 – početni ekran dobrodošlice

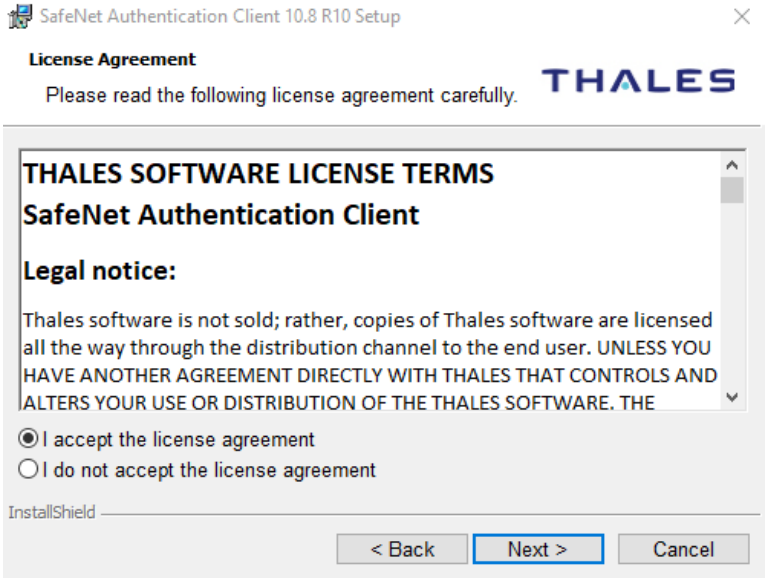
Prva opcija u postupku instalacije jeste odabir odgovarajućeg jezika instalacije – slika 24.



Slika 24 – odabir jezika instalacije

Bitno je ovdje napomenut da, u slučaju da je na računaru postojala neka verzija SafeNet software-a, Setup procedura će vam ponuditi da sačuvate postojeće postavke kroz opciju „**Use the existing configuration settings**“. Nije potrebno sačuvati stare postavke, mada odabir neće utjecati na rezultat instalacije.

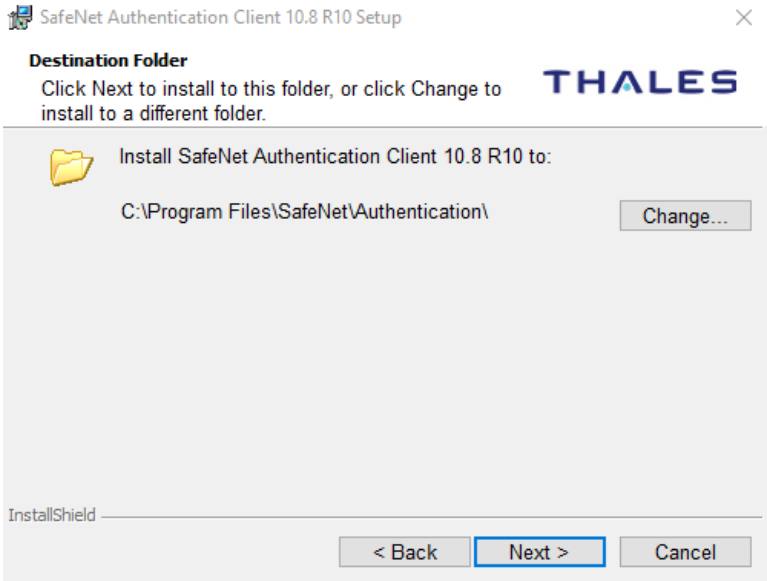
Nakon odabira jezika, instalaciju nastavljamo odabirom **Next** nakon čega će se prikazati prozor sa licencom za krajnjeg korisnika (**End-User License Agreement**) – slika 25.



Slika 25 – prozor sa prikazom licencnog ugovora

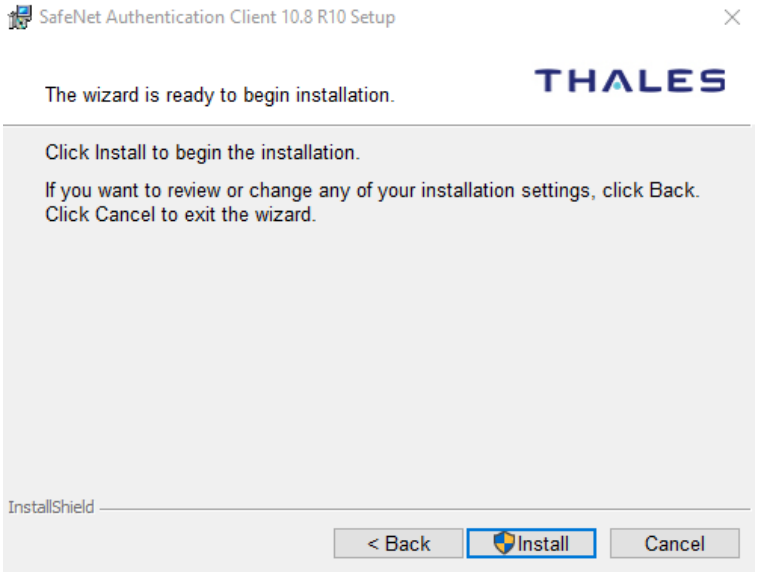
Nakon što se pročita sporazum o licenci, označiti prihvatanje licencnog sporazuma te klikom na **Next** nastaviti dalje sa instalacijom.

Naredni korak, na slici 26, prikazuje prozor za odabir destinacijskog foldera za instalaciju na lokalnom računaru. Moguće je promijeniti destinacijski folder koji je postavljen u osnovnoj instalaciji, ali je preporuka ostaviti ponuđenu putanju. Klikom na **Next** prihvatamo ponuđenu putanju i nastavljamo dalje sa procedurom.



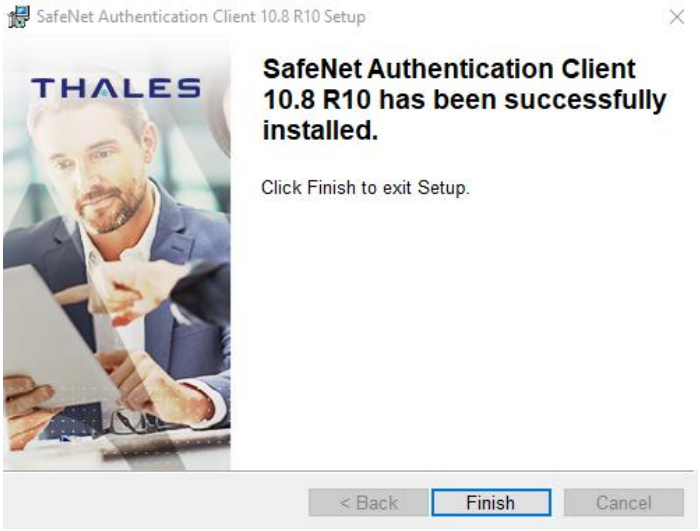
Slika 26 – odabir destinacijskog foldera za instalaciju

Sljedeći korak, slika 27, predstavlja informativni prozor, odnosno prozor upozorenja, u kojem nas sistem obavještava da je sve spremno za instalaciju, te da prelaskom na sljedeći korak sama instalacija se i pokreće. U ovom koraku imamo mogućnost davanja saglasnosti za instalaciju ili odustajanja od iste. Izborom opcije **Install** daje se saglasnost i pokreće instalacija software-a. Ikonica štita pored opcije Install sugeriše da su za instalaciju potrebne administratorske privilegije, odnosno prava, a kako je navedeno i na početku. Ovisno o sigurnosnim postavkama samog računara moguće je da se, prije nego instalacija krene, pojavi popup prozor samog operativnog sistema računara gdje se traži još jednom odobrenje za instalaciju. Potrebno je klikom na odgovarajuću opciju (uglavnom opcija Yes) odobriti instalaciju.



Slika 27 – pokretanje samog postupka instalacije

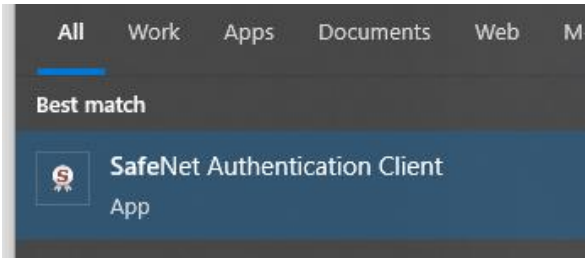
Nakon što je instalacija završena prikazat će se prozor sa porukom da je instalacija uspješno završena. Klikom na Finish zatvaramo prozor i okončavamo proceduru instalacije potrebnih drivera – slika 28.



Slika 28 – okončavanje postupka instalacije

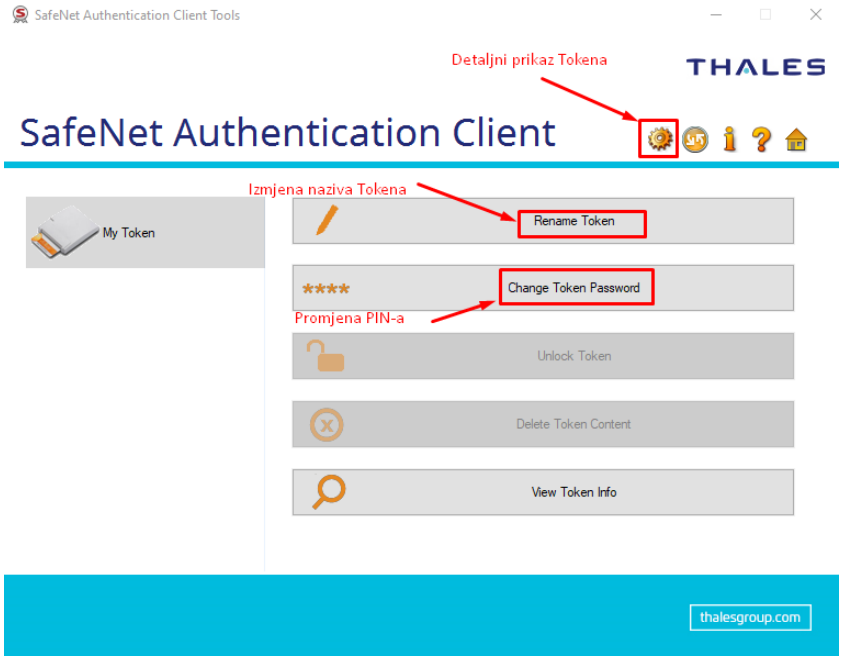
3 Pristup USB tokenu i osnovna konfiguracija

Nakon što je driver (tzv. middleware aplikacija) instaliran na računar, na samom računaru moguće je pronaći novoinstaliranu aplikaciju *„SafeNet Authentication Client Tools“.* Aplikaciju je moguće pronaći i pokrenuti kroz Start meni računara, kao na slici 29 (npr. u search polje se unese *safenet*), dok se ista može naći i u „system tray“.



Slika 29 – pokretanje SafeNet aplikacije

Pokretanjem aplikacije *„SafeNet Authentication Client Tools“* pokreće se aplikacija u osnovnom prozoru kao na slici 30.



Slika 30 – osnovni, početni prozor SafeNet aplikacije

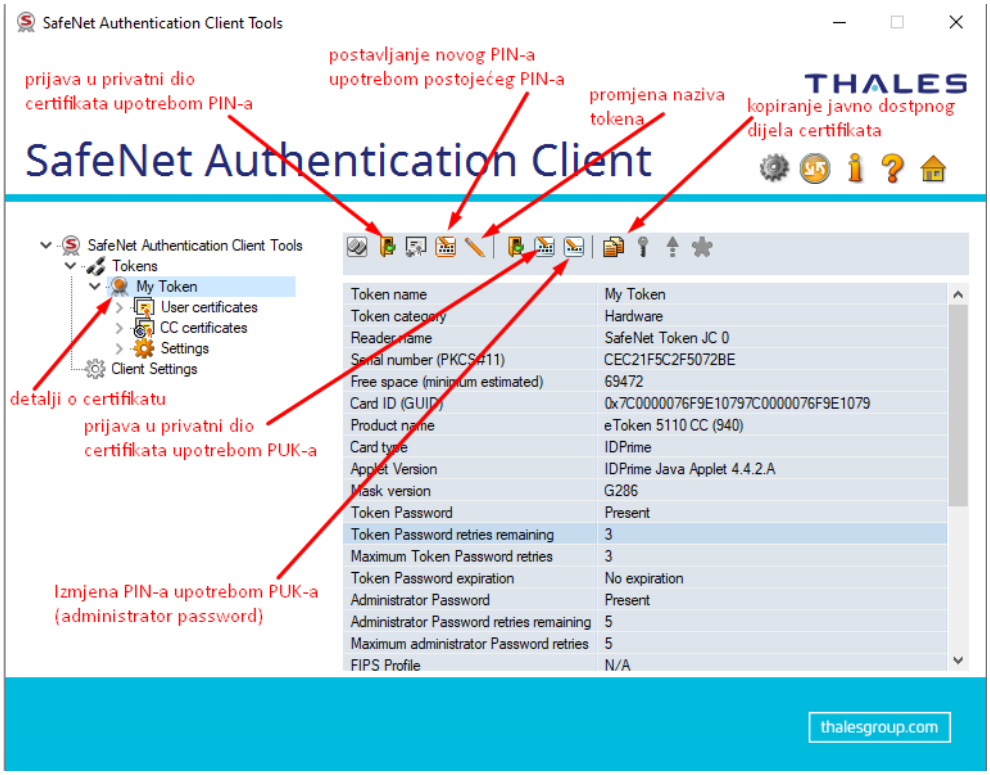
U okviru osnovnog, početnog prozora aplikacije postoji nekoliko opcija, a moguće je i preći u detaljniji prikaz Tokena sa dodatnim opcijama. Bitno je da naglasiti da se u okviru početnog prozora nalaze opcije za izmjenu PIN-a certifikata (u aplikaciji **Token Password** je zapravo PIN !) i po želji izmjeniti naziv Tokena – slika 30.

Bitno je napomenuti da pojedine funkcionalnosti aplikacije su nedostupne ili su nefunkcionalne zbog načina na koji se USB Token upotrebljava na platformi Ovjerioca JP BH Pošta.

Klikom na ikonu  (zupčanik) otvorit će se prozor sa detaljnim prikazom Tokena, kao i dodatnim opcijama. Sama ikonica kojom se otvara dodatni prikaz je na slici 30, dok je na slici 31 prikaz izgleda ekrana i dodatnih opcija.

U detaljnom prikazu tokena kroz aplikaciju možete izvršiti slijedeće:

- pronaći detalje o vašem certifikatu
- kopirati javno dostupan dio certifikata
- pristupiti (logovati se) u privatni dio certifikata upotrebom PIN-a (Token Password)
- postaviti novi PIN kada znate stari PIN (Token Password)
- promjeniti naziv tokena
- pristupiti (logovati se) u privatni dio certifikata upotrebom PUK-a (u aplikaciji **Administrator Password** je zapravo **PUK** !)
- Izmjena Administrator Password-a (tj. PUK-a)
- postaviti novi PIN (Token Password) upotrebom Administrator Password-a (PUK) tj. postavljanje novog PIN kada ne znate postojeći PIN



Slika 31 – Detalji tokena i dodatne opcije

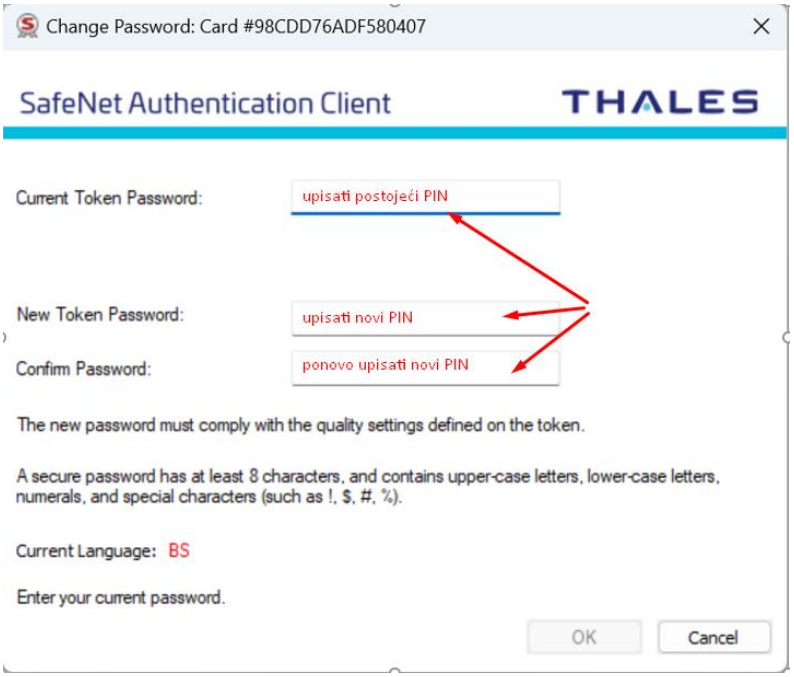
Kao i u prethodnom slučaju potrebno je napomenuti da pojedine funkcionalnosti aplikacije su nedostupne ili su nefunkcionalne zbog načina na koji se USB Token upotrebljava na platformi Ovjerioca JP BH Pošta.

3.1 Promjena PIN-a (Token password)

Promjena PIN-a certifikata, o okviru aplikacije SafeNet označena kao Token password, vrši se odabirom opcije za izmjenu Token poassword-a (PIN-a) (Change Token Password, slika 30), te se otvara forma za promjenu PIN-a (Token password), slika 32.

Za uspješnu promjenu PIN-a potrebno je prevashodno znati postojeći PIN, a zatim i zadovoljiti minimalne zahtjeve u pogledu kompleksnosti novog PIN-a. Unos novog PIN-a se ponavlja dva puta, te oba unosa moraju biti identična.

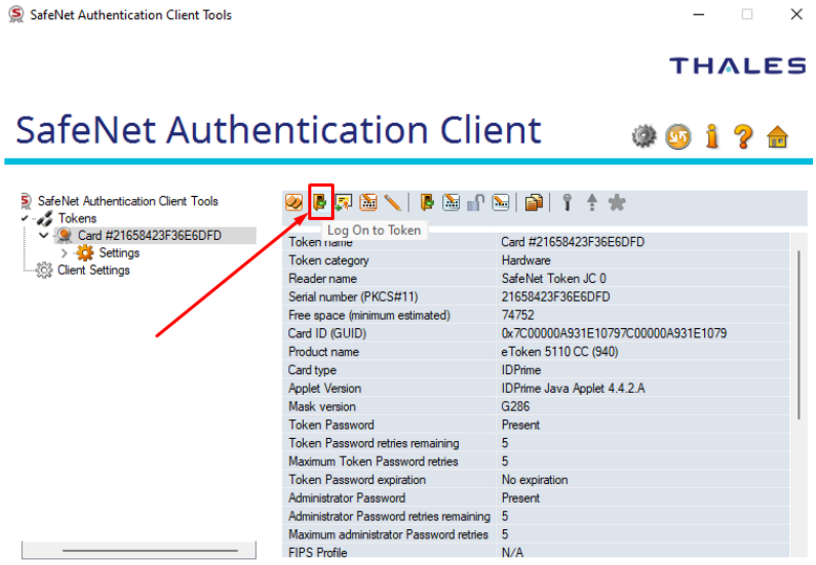
Konkretno, u postupku promjene postojeći PIN se unosi u polje „Current Token Password“, te dva puta novi Token Paswword (PIN), u polja „New Token Password“ i „Confirm Password“. Odabirom OK završen je postupak promjene Token password-a (PIN-a) – slika 32.



Slika 32 – promjena PIN-a certifikata

Bitno je napomenuti da se PIN (Token Password) mora sastojati od najmanje 6 brojeva.

Prijavom na USB Token moguće je verifikovati novi postavljeni PIN, i to odabirom **Log On to Token** opcije, kao na slici 33.

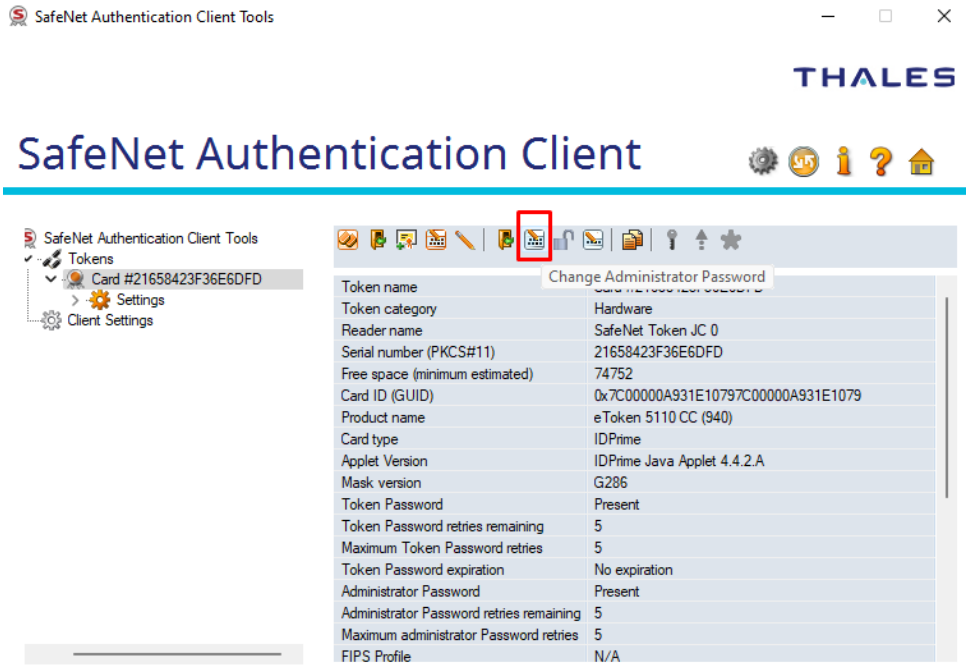


Slika 33 – prijava na USB token

3.2 Promjena USB Token Administratorske lozinke (PUK)

Za promjenu administratorske lozinke USB Tokena potrebno je pratiti sljedeće korake:

1. Pokrenuti **SafeNet Authentication Client Tools** aplikaciju.
2. Klikom na ikonu (zupčanik) otvorit će se prozor sa detaljnim prikazom Tokena.
3. Odabrati opciju **Change Administrator Password** – slika 34

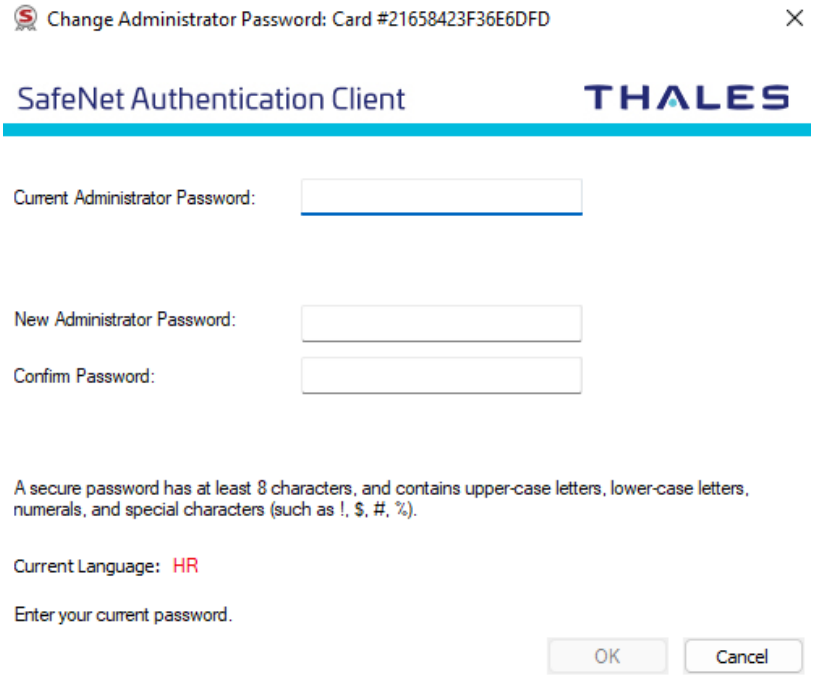


Slika 34 – Promjena administratorske lozinke USB Tokena (PUK)

Kao i u slučaju promjene PIN-a, u prozoru za unos trenutnog i novog Administrator password-a (PUK) – slika 35, potrebno je unijeti:

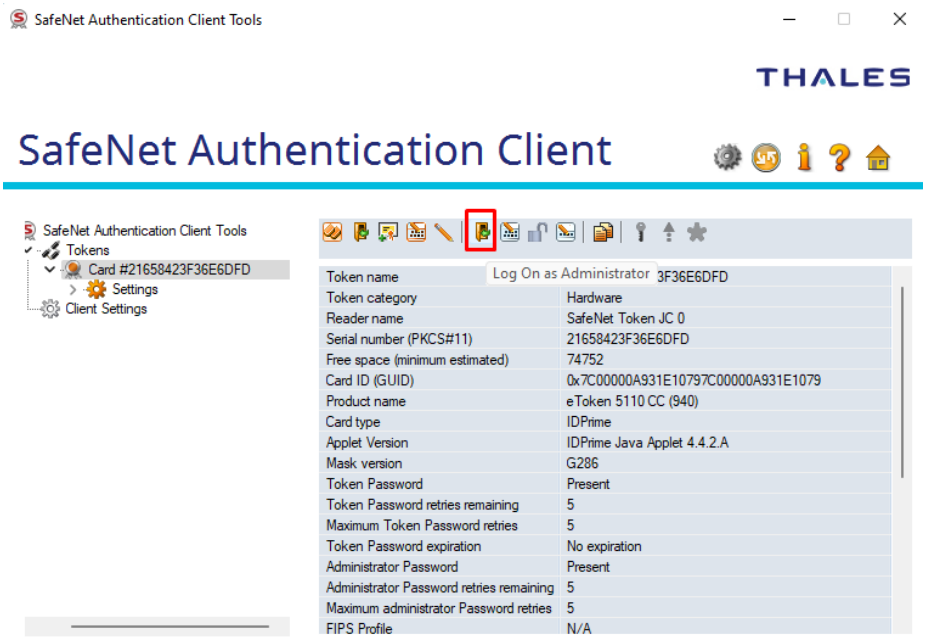
- U dijelu **Current Administrator Password** unijeti trenutni PUK
- U dijelu **New Administrator Password** i **Confirm Password** unijeti novi PUK.

Odabirom opcije **OK** potvrđujemo unos i završava se postupak promjene Administrator Password-a (PUK). Bitno je napomenti da administratorska lozinka USB tokena (PUK) mora da sadrži najmanje 16 karaktera, jedno veliko slovo, jedno malo slovo, minimalno jedan broj i specijalni karakter (npr. !, $, #, %)



Slika 35 – prozor za promjenu administratorske lozinke USB Toknena (PUK)

Prijavom na USB Token moguće je verifikovati novi postavljeni password (PUK), i to odabirom opcije **Log On as Administrator**, kao na slici 36.



Slika 36 – Prijava kao administrator, može poslužiti kao provjera novog PUK-a

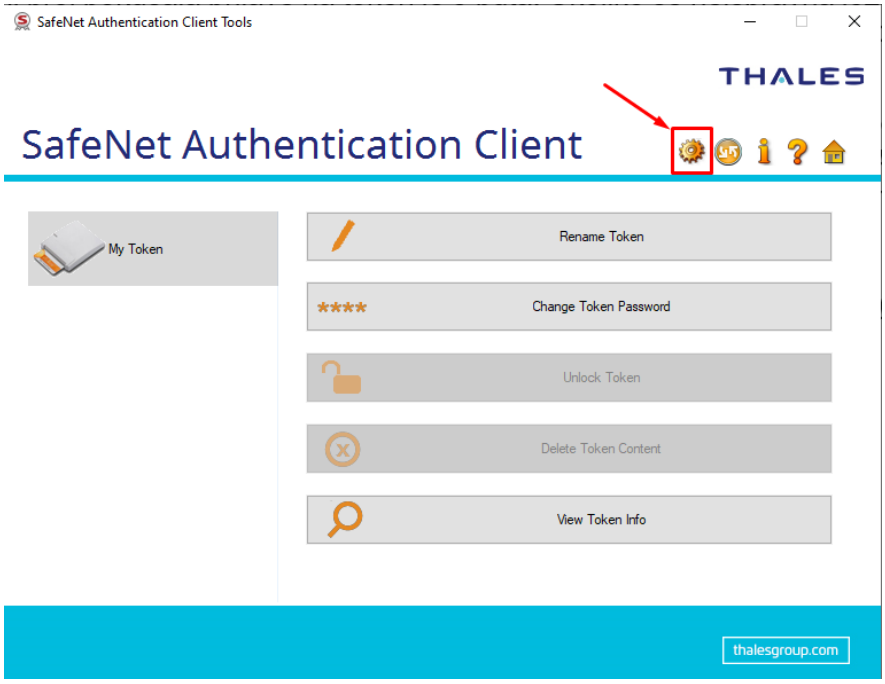
3.3 Deblokada USB Tokena u slučaju zaboravljenog PIN-a

Kako bi se sigurnosno zaštitio USB Token, te spriječile potencijalne zloupotrebe, kao i kod drugih sličnih sistema, ograničen je i maksimalni broj pokušaja prijave na USB token. U slučaju USB Tokena koji izdaje Ovjerilac JP BH Popšta maksimalni broj neispravnih uzastopnih pokušaja prijave je 3 puta. Ukoliko se neispravna lozinka - PIN unese 3 puta uzastopno, dolazi do zaključavanja USB Tokena.

U tom slučaju USB Token je potrebno otključati, a za otključavanje USB tokena potrebno je poznavanje Administratorske lozinke USB Tokena tj. PUK-a.

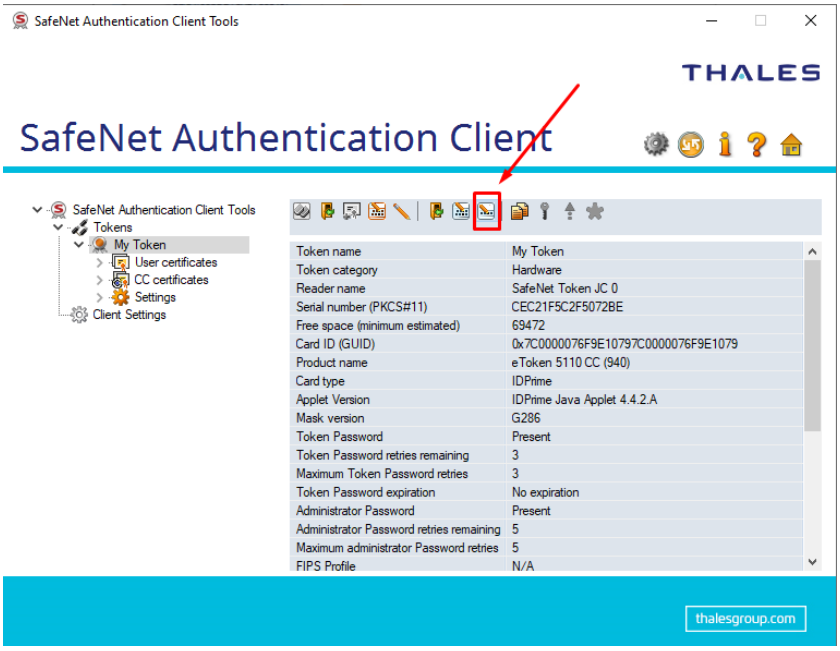
Otključavanje USB tokena vrši se kroz narednih nekoliko koraka:

1) Ubaciti USB token u korisnički računar i otvoriti *SafeNet Authentication Client* aplikaciju.
2) Odabrati ***Advanced View*** opciju – slika 37.



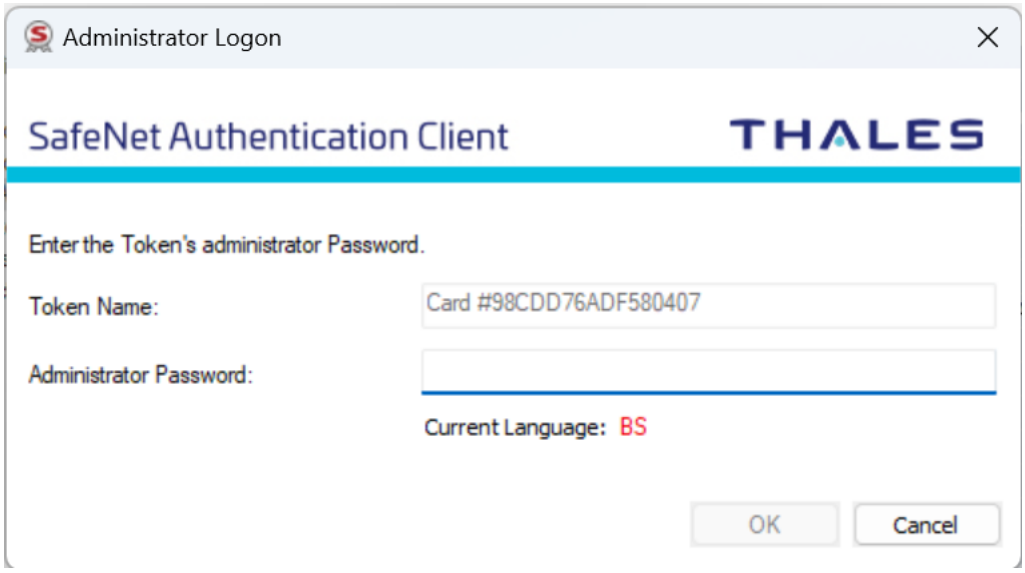
Slika 37 – Odabir opcije koja omogućava dodatne postavke

3) Odabrati ***Set Token Password***, označeno na slici 38.



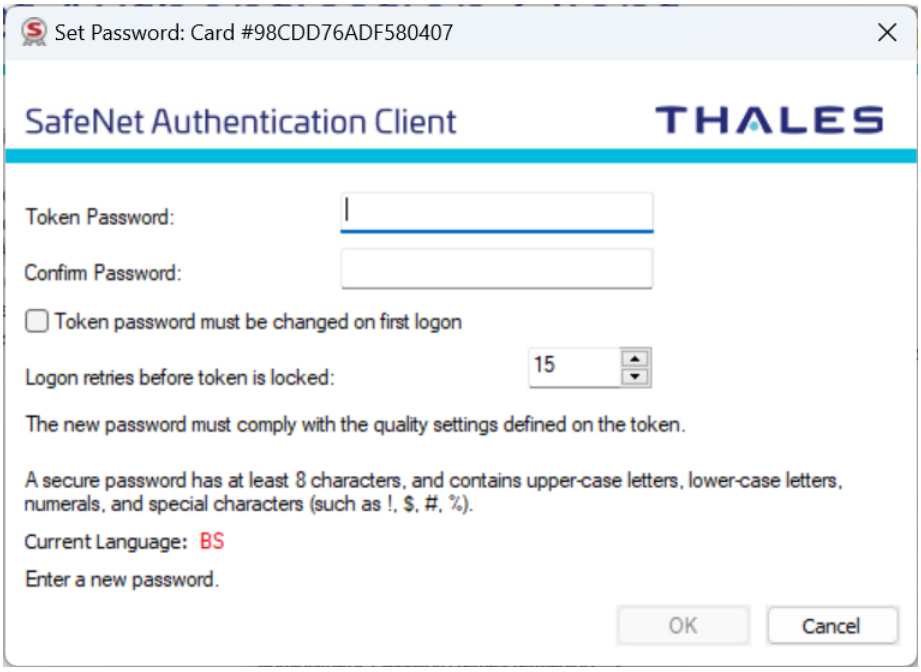
Slika 38 – Opcija za promjenu Token lozinke tj. PIN-a

4) Nakon ovoga sistem će tražiti unos Administratorske lozinke kako bi opcija promjene bila omogućena. Unijeti Administratorsku lozinku u dijelu **Administrator Password** i potvrditi unos na **OK**, slika 39.



Slika 39 – unos administratorske lozinke (PUK) radi dostupnosti opcija

5) Unosom ispravnog Administrator password, prikazuje se prozor za unos novog Token password-a (PIN-a). Potrebno je unijeti novi password dva puta (**Token Password & Confirm Password**) i potvrditi unos na **OK**, slika 40.



Slika 40 – unos nove lozinke USB Tokena (PIN)

Veoma je važno istaknuti i naglasiti da je potrebno posebno voditi računa prilikom unosa Administratorske tj. PUK lozinke. U slučaju zaključavanja Administrator password-a (PUK), USB Token postaje trajno zaključan. USB Token se trajno zaključava pogrešnim neispravnim uzasatopnim unosom od 5 puta.

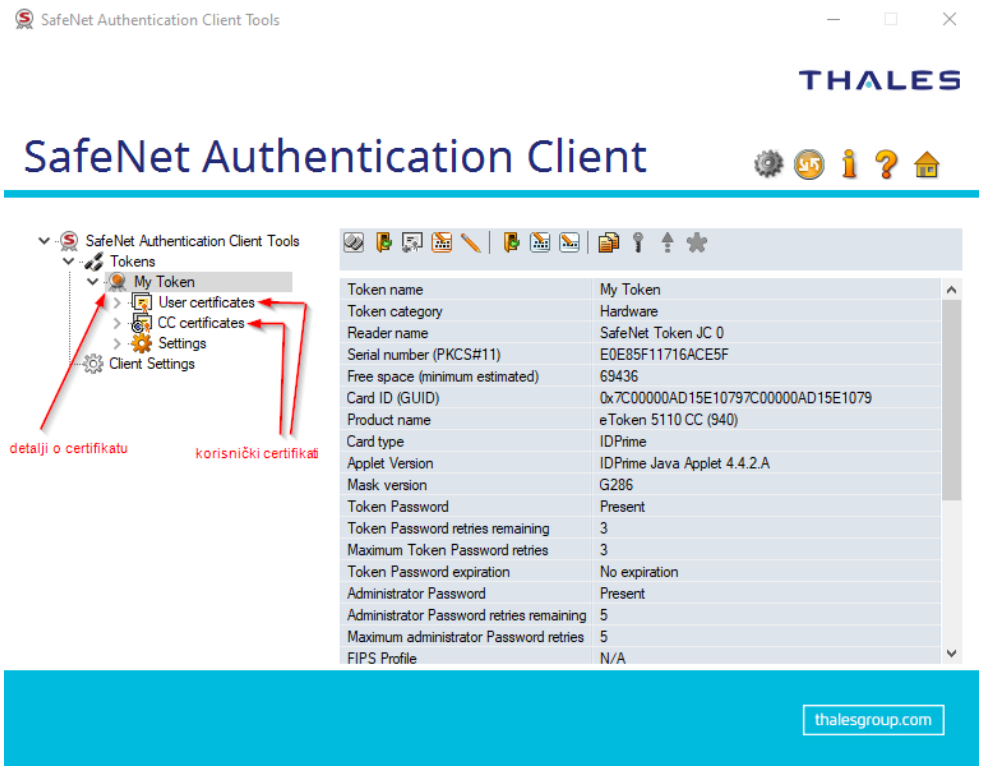
Otključavanje USB Tokena na ovaj način nije moguće i kao rješenje potrebno je ponovo podnijeti zahtjev za izdavanje novog digitalnog certifikata, te izdavanje novog USB Tokena.

4 Kopiranje/izvoz (export) javno dostupnog dijela certifikata

U zavisnosti od aplikativnih rješenja i načina rada institucija, kompanija ili ostalih pravnih subjekata, koji prihvataju i rade sa kvalificiranim elektronskim potrvdama (digitalnim certifikatima), može se doći u situaciju da je potrebno tim stranama dostaviti javni dio certifikata. Ovo je recimo slučaj sa aplikacijom Uprave za indirektno oporezivanje, a koja radi i sa kvalificiranim elektronskim potrvdama (digitalnim certifikatima) Ovjerioca JP BH Pošta.

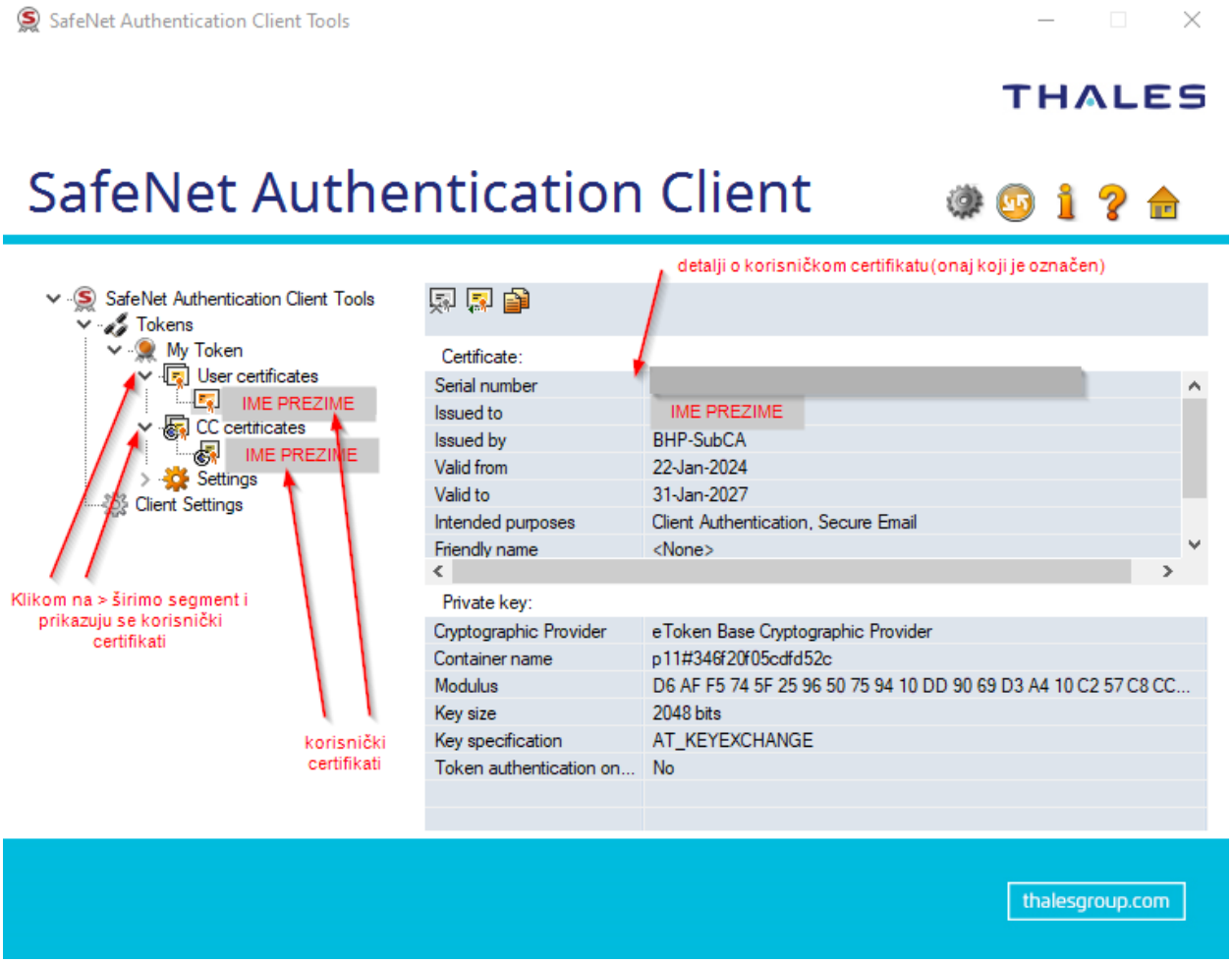
U ovakvim slučajevima potrebno je, kroz dostupnu SafeNet aplikaciju, izvršiti kopiranje, odnosno export (izvoz) javno dostupnog dijela certifikata na lokalni računar, radi daljeg proslijeđivanja drugoj strani (putem e-maila ili na neki drugi način, kako je već to definisano načinom rada te strane). Bitno je naglasiti da je ovo kopiranje javnog dijela certifikata dozvoljena operacija i da ni na koji način ne narušava integritet, sigurnost, niti kompromituje na neki način izdati digitalni certifikat. Upravo zato jer se radi samo o javno dostupnom dijelu certifikata.

Sam postupak kopiranja, odnosno exporta/izvoza opisan je u narednih nekoliko koraka. Potrebno je pristupiti SafeNet aplikaciji i to segmentu sa dodatnim opcijama (vidi stranu 22-24 ovog uputstva). U dijelu My Token imamo sve informacije o samom tokenu. Detalji o korisničkim certifikatima su u segmentima označenim sa User certificates i CC certificates. Navedeno je prikazano na slici 41.



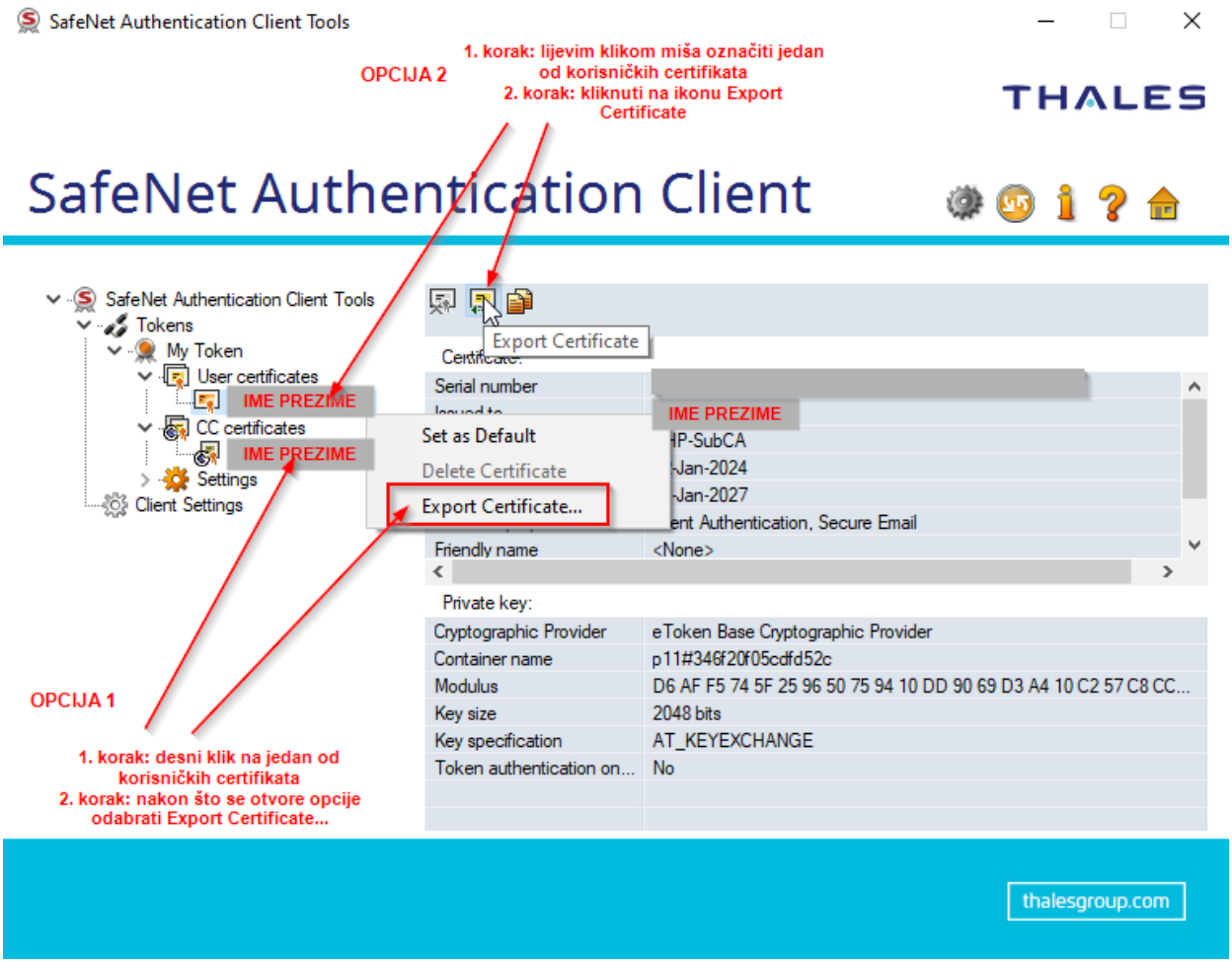
Slika 41 – pristup detaljima o tokenu i korisničkim certifikatima

Da bi došli do podataka o korisničkim certifikatima, te imali opciju za kopiranje, odnosno export/izvoz javnog dijela certifikata potrebno je da klikom na ikonu „**>**“ ispred gore navedenih polja otvorimo iste, te dobijemo prikaz korisničkih certifikata. Certifikate je lako prepoznati jer su izdati na ime i prezime korisnika, odnosno vlasnika certifikata. Klikom i označavanjem certifikata u prostoru sa oznakom *Certificate:* (na desnoj strani) dobijamo prikazane detalje o istom. Navedeno je prikazano na slici 42.



Slika 42 – korisnički certifikati i detalji o istima

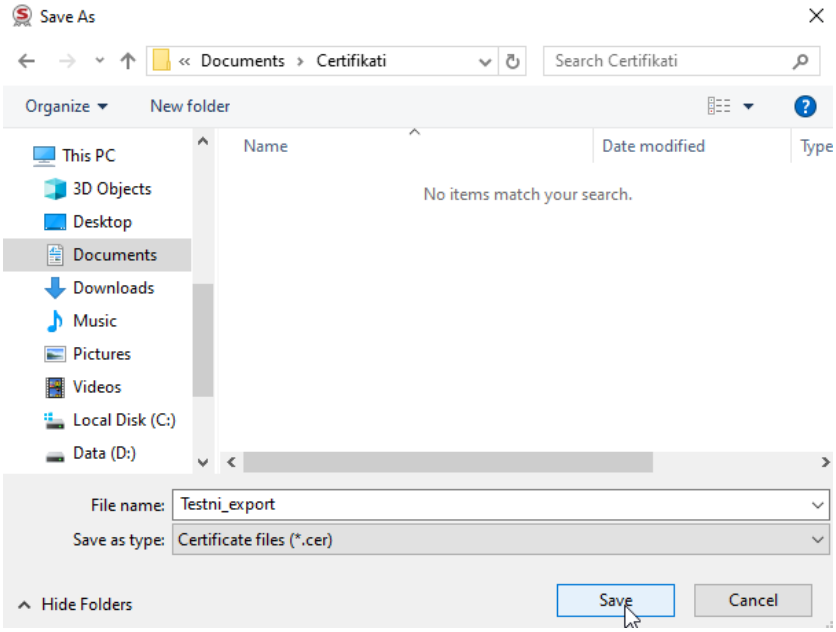
Sam postupak kopiranja, odnosno exporta/izvoza certifikata sada možemo izvršiti na dva načina. Jedan od njih je desnim klikom miša na jedan od korisničkih certifikata, te nakon pojavljivanja dodatnih opcija odabirom opcije *Export Certificate...* Na slici 43 navedeno je prikzano pod oznakom 1. Drugi način je označavanje jednog korisničkog certifikata lijevim klikom miša, te odabirom opcije Export Certificate klikom na ikonicu iznad detalja o korisničkom certifikatu. Na slici 43 ovaj postupak je označen oznakom 2.



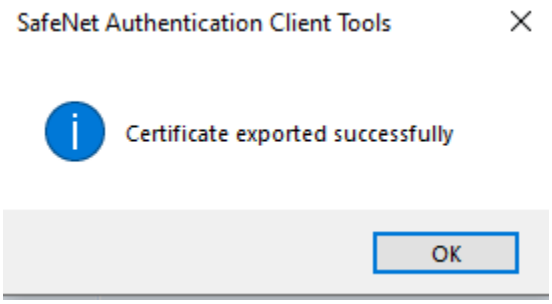
Slika 43 - pokretanje kopiranja (export/izvoz) korisničkog certifikata

Nakon pokretanja opcije za kopiranje, odnosno export/izvoz certifikata dobijamo prozor u kojem je potrebno odabrati putanju (folder) u koji želimo spasiti izvezeni javni dio korisničkog certifikata – slika 44. Osim same putanje na lokalnom računaru potrebno je i da damo ime file-u u polje *File name:*. Tip certifikata koji će se spasiti na lokalnom računaru je već predefinisan i može biti samo .cer tip file-a.

Ukoliko je procedura uspješno okončana pojavljuje se prozor sa informacijama da je certifikat uspješno kopiran, odnosno exportovan/izvezen. Klikom na ok primamo k znanju tu informaciju i završavamo postupak – slika 45.

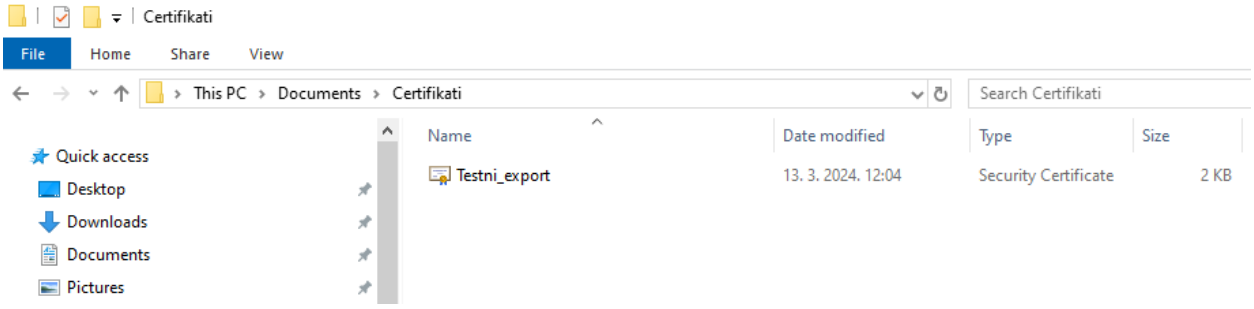


Slika 44 - odabir putanje i imena certifikata na lokalnom računaru



Slika 45 - Prozor sa potvrdom o uspješnom kopiranju (exportu) certifikata

Provjeru da su certifikati uspješno kopirani, odnosno exportovani/izvezeni možemo izvršiti odlaskom na putanju koju smo unijeli u prethodnoj proceduri, kao lokaciju na računaru za smještaj izvezenog certifikata. Trebali bi imati prikazane izvezene certifikate kao na slici 46. Pregledom datuma kreiranja file-a na prikazu možemo provjeriti i potvrditi da se radi o exportu koji smo upravo i izvršili.



Slika 46 - Provjera izvezenih certifikata na file sistemo lokalnog računara

Potrebno je napomenuti da se može izvršiti kopiranje, odnosno export/izvoz samo jednog korisničkog certifikata istovremeno. Ukoliko je potrebno exportovati, u našem slučaju, oba certifikata (a što je vezano za način rada i sistem treće strane, tj one koja prihvata digitalni certifikat), potrebno je navedenu proceduru provesti za svaki korisnički certifikat pojedinačno – slike 43 – 46. U konačnici na file sistemu lokalnog računara imaćemo 2 odvojena file-a, te je iste potrebno poslati, odnosno dostaviti, na način kako je već propisan od treće strane. Jedan od načina, a možda i najčešći, jeste dostavljanje putem e-maila. Kako se radi o .cer tipu file-a, a da bi izbjegli eventualni problemi pri slanju i primanju takvog tipa file-a, preporučuje se da se svi certifikati sa lokalnog računara zapakuju u zip, rar ili neku drugu arhivu, te zatim šalju kao jedan arhivski file.