Korisničko uputstvo

Otključavanje zaključanog USB tokena sa kvalificiranom elektronskom potvrdom

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 pruža usluge izdavanja kvalificiranih elektronskih potvrda (KEP) 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 (tkz. middleware aplikacija)
3. PIN kod 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 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.

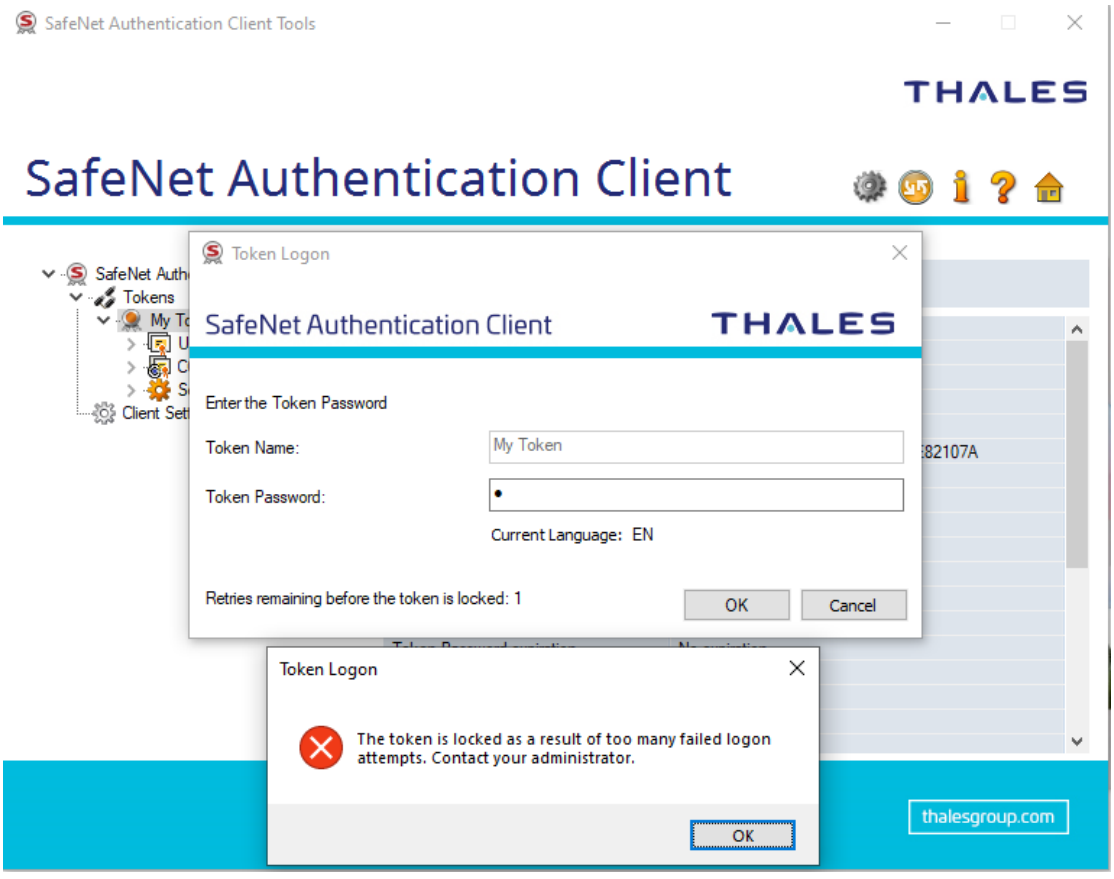
Prije nego što počnemo sa digitalnim potpisivanjem dokumenata, još jednom ističemo da je potrebno da su ispunjeni gore navedeni preduslovi za prepoznavanje i korištenje tokena sa digitalnim certifikatom koji već posjedujete. Zamolite svoj tim za tehničku podršku da provjeri postavke digitalnog potpisa na vašem računaru, ukoliko je to potrebno.

Prilikom upotrebe USB tokena sa kvalificiranom elektronskom potrvdom potrebno je iz sigurnosnih razloga izvršiti autentikaciju upotrebe putem PIN koda. Svaki USB token je zaštićen PIN kodom koji treba da zna samo vlasnik USB tokena, te dijeljenje PIN koda je nepreporučljivo. Kao i u slučaju drugih sličnih uređaja, ponovo iz sigurnosnih razloga, uzastopan unos PIN kod-a ograničen je na 3 pokušaja. U slučaju pogrešnog unosa PIN koda, tri uzastopna puta, USB token se ključa i onemogućava dalju upotrebu. Ovim se spriječava neovlašteno korištenje eventualnim „probijanjem“ PIN koda, višestukim uzastopnim pokušajima unošenja sve dok se ne bi otkrio stvarni PIN kod. U slučaju zaključavanja tokena jedini način za ponovno otključavanje i ponovno korištenje jeste otključavanje USB tokena PUK kodom, odnosno administratorskom lozinkom, a koja je također jedinstveno dodijeljena USB tokenu, te koja se dobija zajedno sa PIN kodom. Ovo uputsvo je namjenjeno za prikaz koraka potrebnih za otključavanje USB tokena ovjerioca JP BH Pošta sa kvalificiranom elektronskom potvrdom (digitalnim certifikatom).

1 Otključavanje zaključanog tokena sa kvalificiranom elektronskom potvrdom

Prilikom svake upotrebe USB tokena sa kvalificiranom elektronskom potvrdom istu je potrebno autenticirati korištenjem odgovarajućeg PIN koda. Isti je poznat samo vlasniku uređaja, a prilkom same upotrebe KEP-a middleware aplikacija izbacuje prozor u koji je potrebno unijeti PIN kod, kako bi se odobrilo korištenje kvalificirane elektronske potvrde. Ovim se osigurava neporecivost, odnosno osigurava se da samo vlasnik uz upotrebu USB tokena i pozavajući PIN kod može izvršiti potpisivanje ili upotrebu kvalificirane elektronske potvrde.

Sigurnosni razlozi nalažu da se broj uzastopnih neuspješnih pokušaja unošenja PIN koda ograniči kako bi se spriječili razni načini, da se metodom uzaludnih pokušaja, odnosno unošenjem raznih PIN kodova u većem broju ponavljanja, eventualno dođe do dogovarajućeg PIN koda. U slučaju kvalificirane elektronske potvrde ovjerioca JP BH POŠTA taj broj je tri (3). Nakon unosa 3 (tri) neuspješna pokušaja, iz raznih razloga, USB token se ključa. Na ekranu se pojavljuje informacija da je USB token zaključan usljed većeg broja neuspjelih pokušaja prijave (Slika 1).

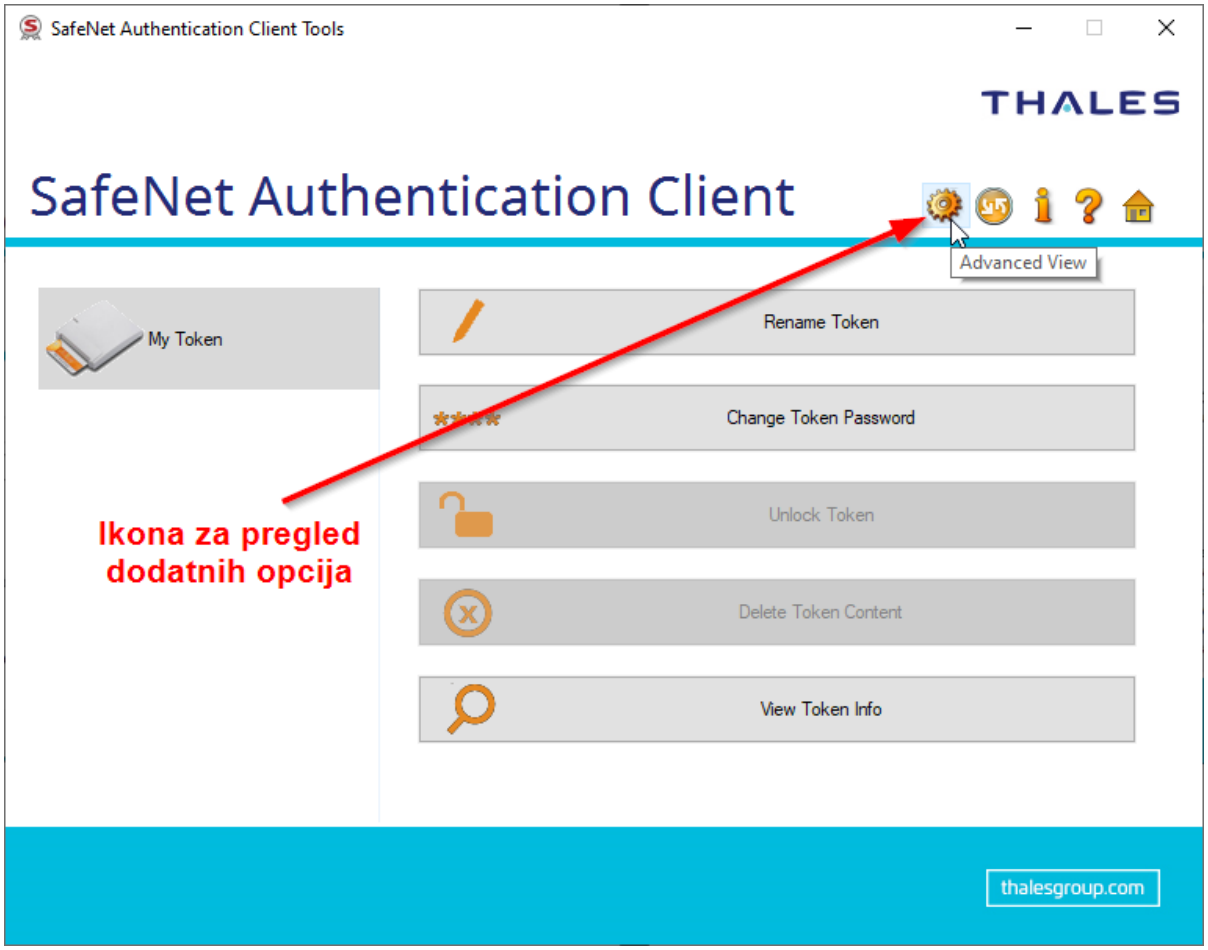


Slika 1 - Poruka u slučaju zaključanog USB tokena

USB token zaključan na navedni način nije dalje moguće koristiti sve dok se isti ne otključa. Za otključavanje USB tokena potreban je drugi kod – PUK kod. PUK kod je jedinstven za svaki token, a dobija se prilikom podnošenja zahtjeva za KEP-om, odnosno kod izdavanja iste. PUK kod se dobija na isti način kako i PIN kod. Ovdje ističemo da je preporučljivo ove kodove (PIN i PUK) sigurno pohraniti i na neki digitalni način, a ne samo čuvati na papiru na kojem su dobijeni. Sve iz razloga što papir prirodno gubi svojstva tokom vremena, pa se može destiti da PUK kod postane nečitljiv.

Uz poznavanje PUK koda za otključavanje zaključanog USB tokena koristi se pripadajuća middleware aplikacija *Thales Safenet* (koja je dostupna na web stranici JP BH Pošta d.o.o. i koja se i koristi za samu upotrebu USB tokena). Koraci za otključavanje su sljedeći:

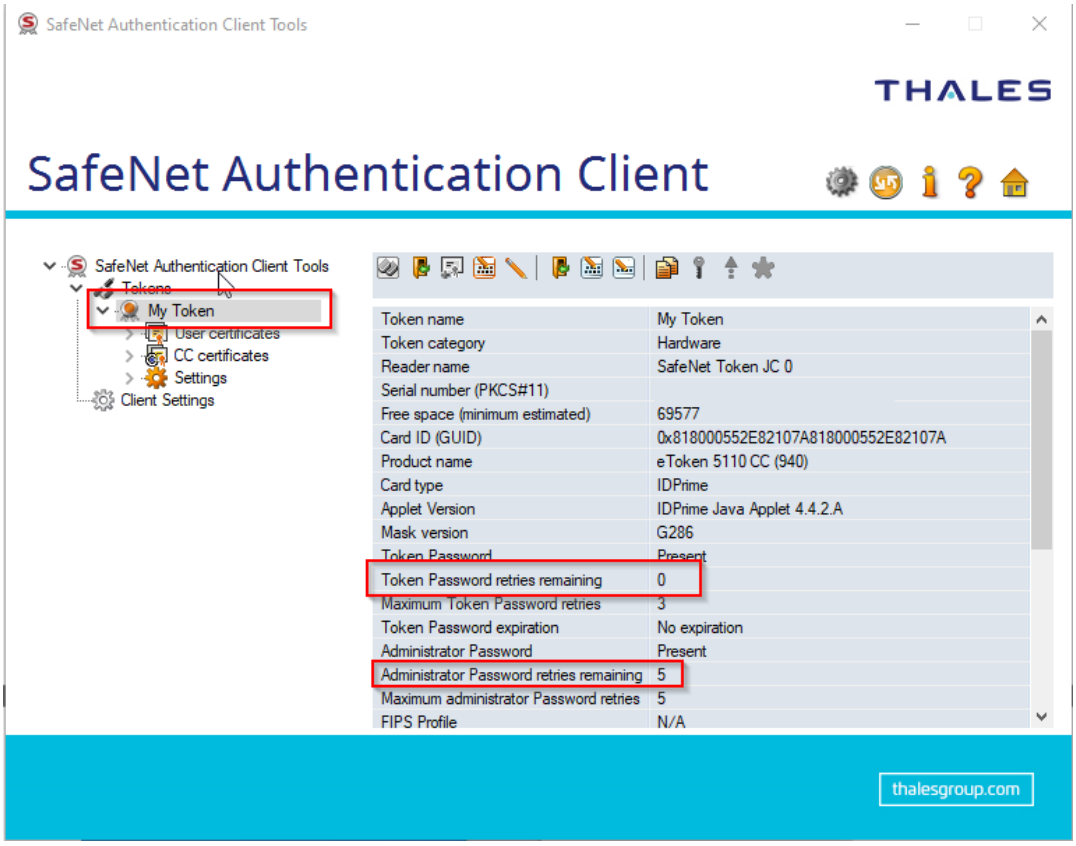
1. Otvoriti *SafeNet Authentication Client* aplikaciju, sa USB tokenom uključenim u računar. Klikom na opciju za *Dodatni pregled/Advanced View* ( ) dolazimo do prikaza dodatnih opcija koje će nam omogućiti otključavanje zaključanog tokena (Slika 2).



Slika 2 - Uključivanje dodatnih opcija

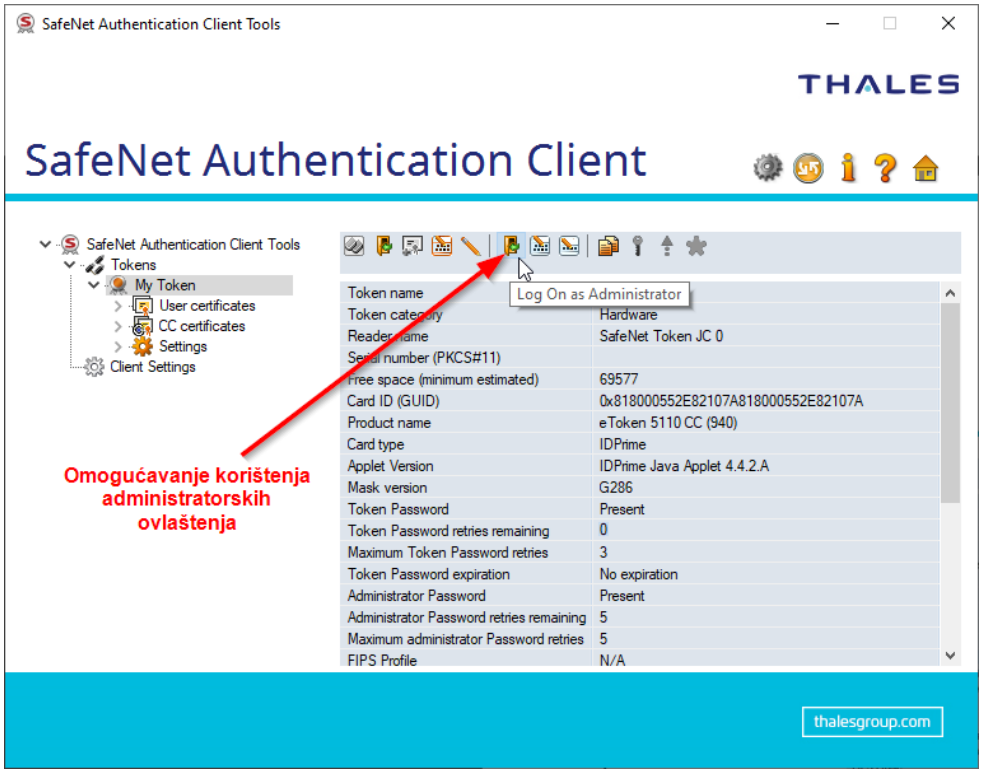
2. Ulaskom u dio sa dodatnim opcijama dobijamo priliku kako za pregled informacija o samom USB Tokenu, tako i za podešavanje određenih postavki. Sa lijeve strane prikazane su informacije o USB Tokenu i certifikatima koji se nalaze na istom. Klikom na pojedine stavke sa lijeve strane na desnoj dobijamo dodatne informacije koje se tiču tih stavki. Kako se u našem slučaju radi o USB tokenu u globalu ostajemo na kratici *My Token* (što je početna vrijednost, dok se prikazuje ime tokena ukoliko smo izvršili imenovanje).

   Bitno je primijetiti dvije vrijednosti sa desne strane a to su: *Broj preostalih pokušaja unosa lozinke tokena/Token Password retries remaining* što odgovara PIN kodu, te *Broj preostalih pokušaja unosa lozinke adminstratora/Administrator Password retries remaining* što odgovara PUK kodu. U slučaju zaključanog tokena prva vrijednost biti će 0 (nula) što daje još jednu indikaciju da je USB token zaključan. Ono što je izuzetno bitno da se ne iskoriste uzaludno svi dostupni pokušaji unošenja PUK koda, jer ukoliko se to desi USB token se trajno ključa i više je neupotrebljiv (Slika 3).



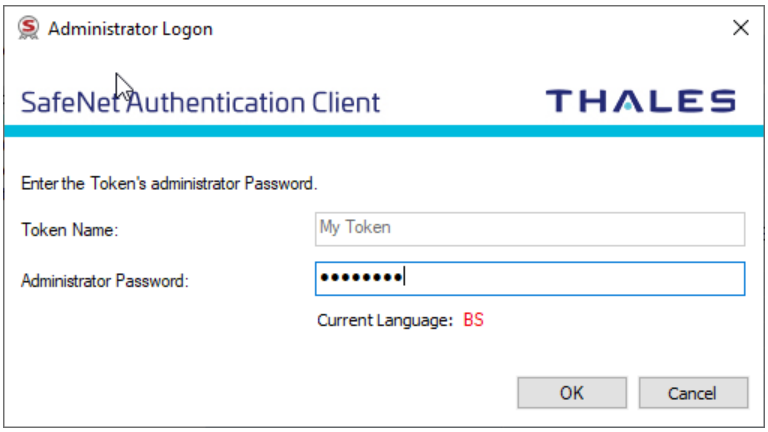
Slika 3 - Pregled dodatnih informacija o USB tokenu, sa naglaskom na broj preostalih pokušaja unošenja PIN i PUK koda

3. Klikom na ikonicu *Prijavi se kao administrator/Log on as Administrator* otključavamo dodatne opcije pomoću kojih možemo podešavati određene postavke USB tokena, u našem slučaju naročito važnu opciju postavljanja PIN koda (Slika 4)



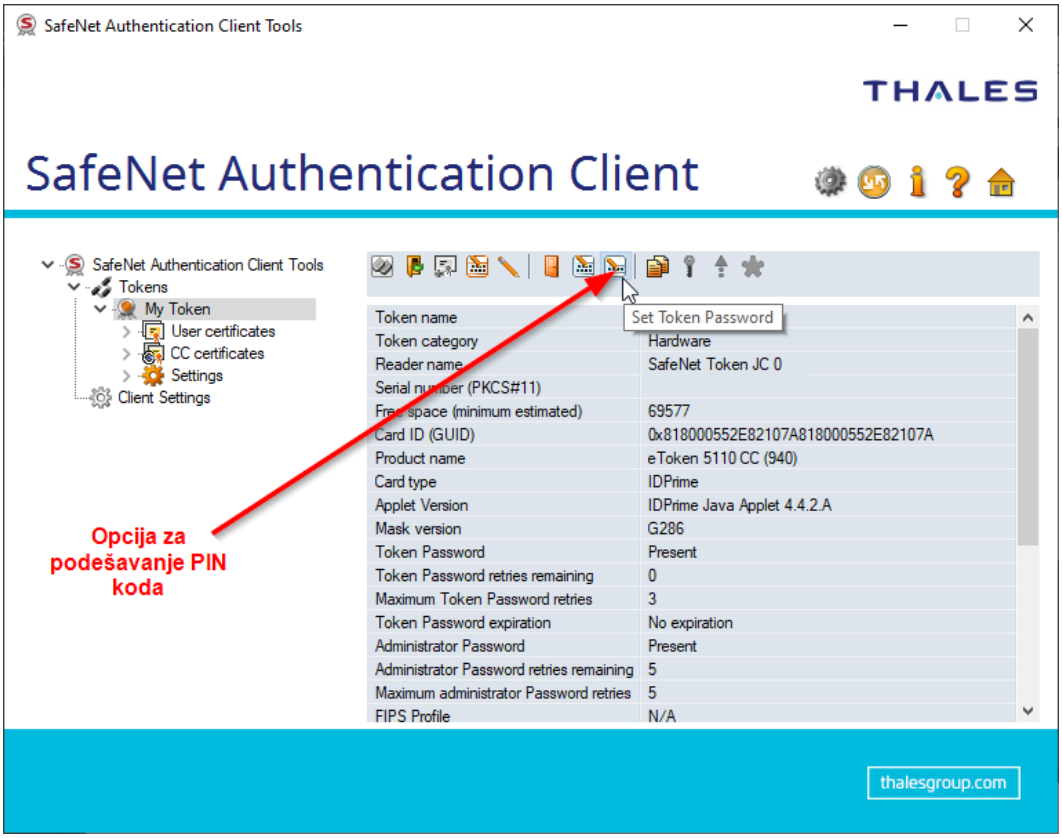
Slika 4 - Prijava kao administrator i otključavanje dodatnih ovlaštenja

4. Klikom na ikonicu iz prethodnog koraka otvara nam se prozor za unos administratorske šifre, odnosno PUK koda. U ovom koraku je izuzetno bitno da ne unesemo pogrešnu vrijednost više od dozvoljenog broja pokušaja, kako USB token ne bi postao trajno zaključan (Slika 5)



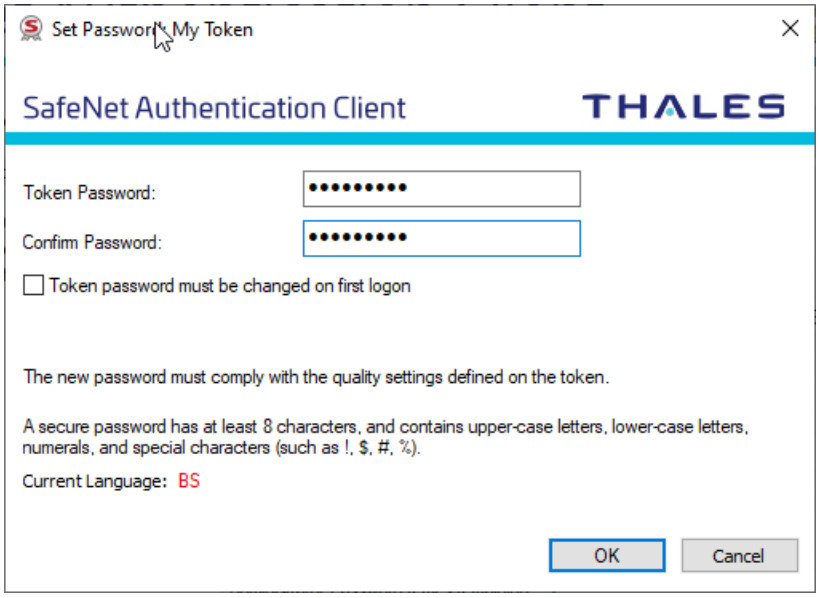
Slika 5 - Prozor za unos PUK koda i pristup administratorskim ovlaštenjima

5. Uspješnom prijavom kao administrator možemo nastaviti sa promjenom, odnosno podešavanjem novog PIN koda, čime će se izvršiti i otključavanje USB tokena. U tu svrhu potrebno je da klikom odaberemo opciju *Podešavanje lozinke tokena/Set Token Password* (Slika 6).



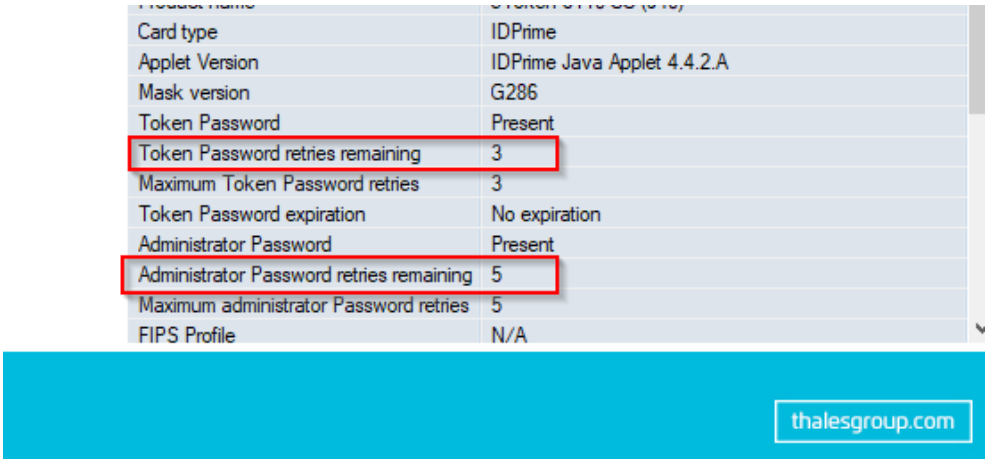
Slika 6 - Opcija za podešavanje PIN koda

6. Klikom na navedenu opciju otvara nam se prozor za unos nove lozinke tokena, odnosno novog PIN koda. Kao i obično u sličnim situacijama promjene lozinki potrebne je unijeti dva puta istu vrijednost. Također imamo i opciju za iniciranje ponovne promjene PIN koda prilikom prve upotrebe, odnosno prvog logona na USB token. Ovu opciju možemo uključiti klikom na odgovarajuću kućicu (checkbox), koji se nalazi ispred same ove opcije. Potvrdu unosa vršimo klikom na OK (Slika 7).



Slika 7 – Unos i podešavanje novog PIN koda

7. Ispravnim provođenjem navedenih koraka uspješno smo izvršili promjenu PIN koda, te ujedno izvršili otključavanje zaključanog USB tokena. Istu proceduru osim za zaključavanje možemo koristiti i za samu promjenu PIN koda. Dodatnu provjeru uspješno izvršene procedure otključavanja možemo izvršiti i provjerom parametara o dostupnom broju unosa PIN-a i PUK-a, iz koraka 2 (Slika 3). Parametri bi se trebali vratiti na početne vrijednosti. U tom slučaju USB token je otključan i možemo nastaviti sa upotrebom (Slika 8).



Slika 8 - Provjera preostalog broja pokušaja unosa PIN-a i PUK-a