

Uputstvo za promjenu PIN-a na Thales IDPrime tokenu

Datum: 01.12.2020.

Oznaka dokumenta: UPTPP01

Verzija: 1.0

Istorijat izmjena

Verzija	Datum	Broj promjena	Opis promjena
1.0			Inicijalna verzija dokumenta

Preispitivanje dokumenta

Datum sljedećeg zakazanog preispitivanja

Distribucija

Naziv	Naslov
Svi	

Odobrio

Ime	Pozicija	Potpis	Datum
Vuk Vujović	COO		

1. Sadržaj

1.	Sadržaj.....	3
2.	Svrha dokumenta.....	4
3.	Struktura Vaših sertifikata.....	4
4.	Promjena PIN-a.....	7
5.	Postavljanje PIN-a	11

2. Svrha dokumenta

Ovaj dokument isključivo služi za korisnike CoreSignFL, CoreSignOL i CoreStamp sertifikata, koji su preuzeli Thales IDPrime token, sa generisanim parom ključeva, od strane Registracionog tijela koji djeluje u okviru Coreit sertifikacionog tijela (Coreit CA), sa namjerom da promjene PIN njihovog tokena. Uputstvo u nastavku je namijenjeno za korisnike Windows operativnog sistema, ali je isto tako i primjenljivo za korisnike macOS.

3. Struktura Vaših sertifikata

Prilikom kupovine Vašeg sertifikata, Coreit CA u svojoj ponudi ima tri vrste paketa koje Vam nudi na tokenu a to su: **CoreSign FL**, **CoreSign OL** i **CoreStamp**.

CoreSign FL je paket koji sadrži dva sertifikata na tokenu. Jedan sertifikat služi za kvalifikovani potpis a drugi sertifikata za autentifikaciju fizičkog lica.

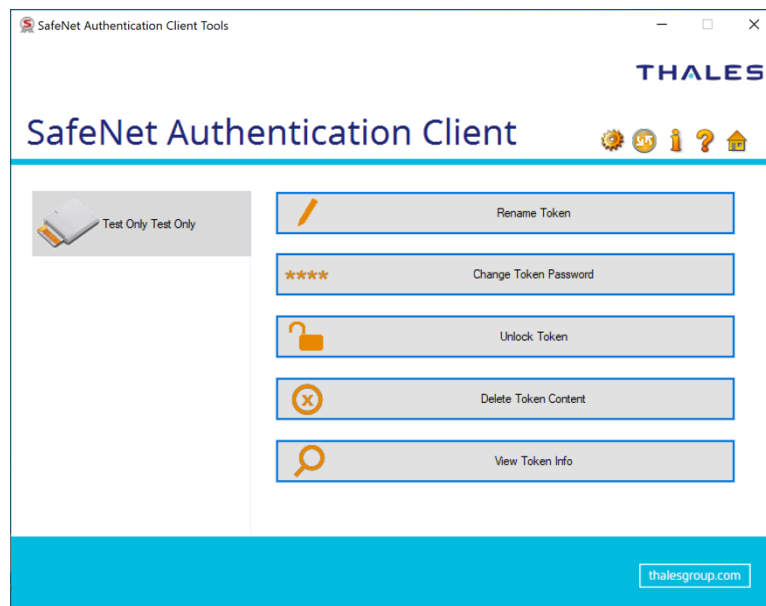
CoreSign OL je paket koji sadrži dva sertifikata na tokenu. Jedan sertifikat služi za kvalifikovani potpis a drugi sertifikata za autentifikaciju fizičkog lica u sklopu pravnog lica.

CoreStamp je paket koji sadrži jedan sertifikat na tokenu i on služi kao kvalifikovani pečat pravnog lica.

Da bi ste promijenili PIN neophodno je da na svom računaru imate instaliranu **Safenet Authentication Client** aplikaciju. Uputstvo za instalaciju Safenet Authentication Client aplikacije možete preuzeti sa <https://ca.coreit.me/manual/COREUPTSAC01.pdf>

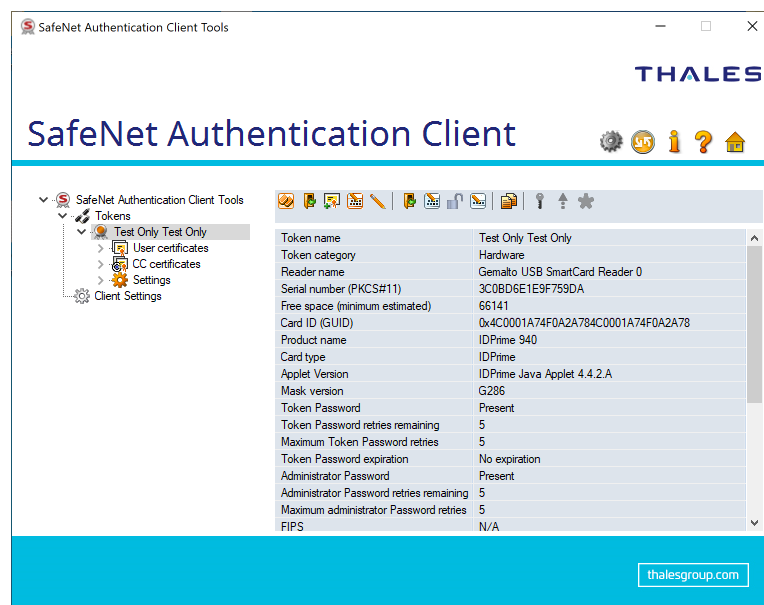
Ukoliko koristite **Safenet Minidriver** potrebno je da isti uklonite (deinstalirate) sa Vašeg računara kako bi ste mogli instalirati **Safenet Authentication Client**. **Ove dvije aplikacije ne mogu istovremeno biti prisutne na Windows operativnom sistemu.**

Nakon što povežete Vaš token sa računarom i otvorite **Safenet Authentication Client Tools** aplikaciju pojaviće Vam se prozor kao na slici 1.



Slika 1

Kliknite na ikonicu  kako bi ste pristupili **Advanced View** prozoru (Slika 2).



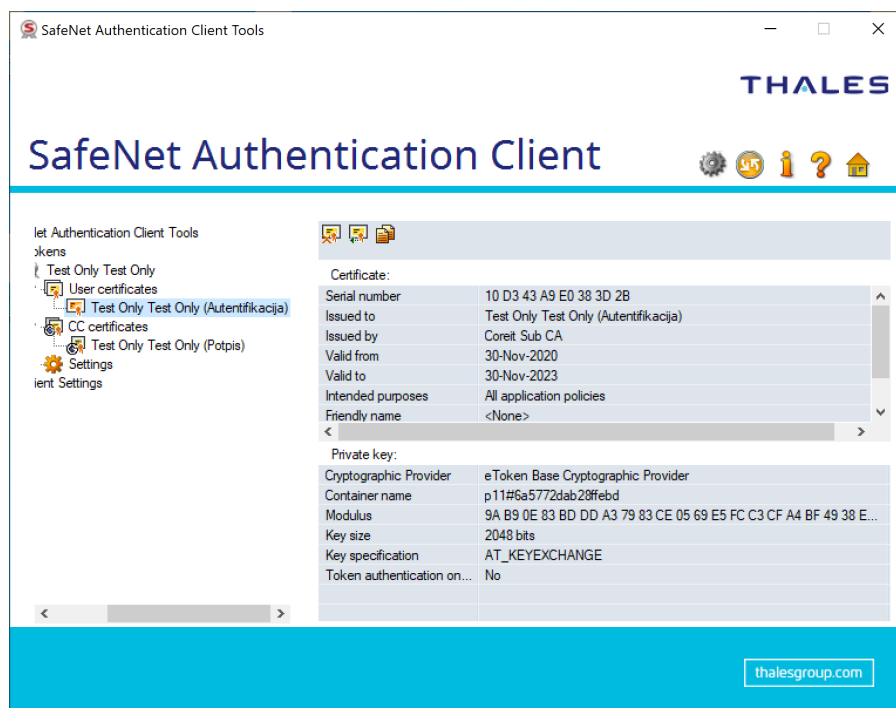
Slika 2

Sa lijeve strane prozora na slici 2 možete vidjeti prikaz Vašeg USB tokena kojeg ste povezali na računar. Naziv tokena će predstavljati Vaše ime i prezime (ime kompanije ukoliko je pečat u pitanju) i pritiskom na sami token (u našem slučaju na slici 2 pritiskom na  **Test Only Test Only**), na desnoj strani prikazaće Vam se sve informacija o njemu.

Ispod tokena se nalaze dva kontejnera u kome su smješteni sertifikati:

- **User Certificates** 
- **Common Criteria (CC) Certificates** 

Ukoliko koristite **CoreSign FL** i **CoreSign OL** sertifikate, sertifikat za autentifikaciju će biti smješten u **User Certificates** kontejneru, dok će sertifikat za kvalifikovani potpis biti smještene u **CC Certificates** kontejneru (Slika 3). Ukoliko koristite **CoreStamp** sertifikat, sertifikat za kvalifikovani pečat nalazi se u **CC Certificates** kontejneru.



Slika 3

4. Promjena PIN-a

Sertifikat za autentifikaciju i kvalifikovani potpis su zaštićeni lozinkama, i prilikom korišćenja jednog ili drugog sertifikata potrebno je unijeti validnu lozinku.

Prilikom korišćenja sertifikata za autentifikaciju od korisnika se traži da unese Token password.

Prilikom korišćenja sertifikata za kvalifikovani potpis od korisnika se traži da unese Digital Signature PIN.

Zbog lakšeg i jednostavnijeg korišćenja sertifikata na Vašem tokenu, **Token password** i **Digital Signature PIN** su IZJEDNAČENI i oni predstavljaju **PIN**, šestocifreni broj koji se nalazi u koverti koju dobijete prilikom preuzimanja tokena.

Iz tog razloga bilo da koristite sertifikat za autentifikaciju ili sertifikat za kvalifikovani potpis uvijek koristite **PIN (iz koverte)** kao validnu lozinku.

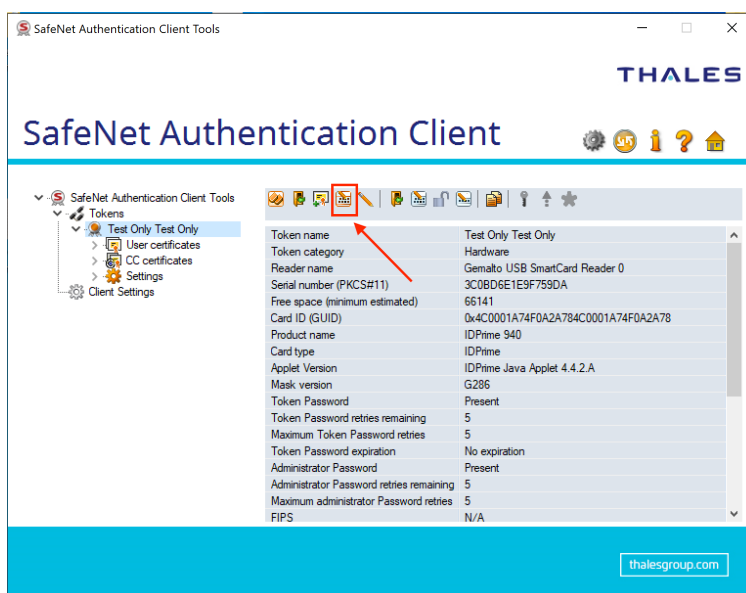
NAPOMENA: NE PREPORUČUJEMO PROMJENU PIN-a. Ukoliko ipak želite da promijenite Vaš PIN, preporučujemo Vam da ga zapišete i sačuvate na sigurnom mjestu.

S obzirom da **Token password** i **Digital Signature PIN** predstavljaju izjednačene vrijednosti koje su prikazane kao **PIN (iz koverte)**, da bi ste promijenili PIN potrebno je da promijenite i Token password i Digital signature PIN kroz Safenet Authentication Client. **Radi jednostavnijeg korišćenja Vaših sertifikata Token password i Digital signature PIN TREBAJU DA BUDU ISTI.**

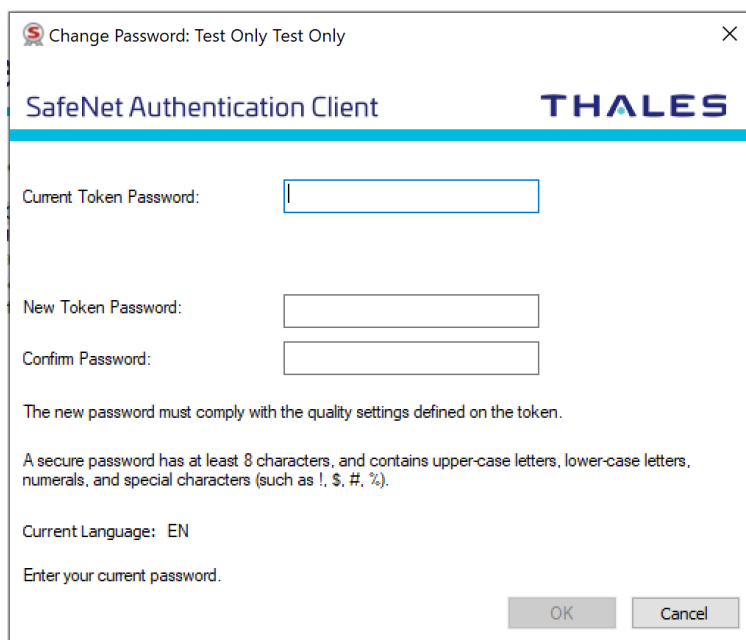
Da promijenite **Token Password**, otvorite Safenet Authentication Client aplikaciju i pritisnite **Advanced View** ikonicu. Na lijevoj strani prozora kliknite na Vaš token, a zatim pritisnite ikonicu  **Change Password** koja se nalazi na desnoj strani prozora aplikacije (Slika 4).

Unutar polja **Current Token Password** unesite **PIN sa koverte**, a unutar **New Token Password** i **Confirm Password** polja unesite broj koji želite da vam predstavlja novi **PIN** (Slika 5). Obratite pažnju da dužina novog **PIN-a** ne smije da bude manja od **6 (šest)** cifara.

Pritiniste **OK**, nakon čega treba da Vam iskoči novi prozor sa potvrdom da je Token Password uspješno promijenjen.

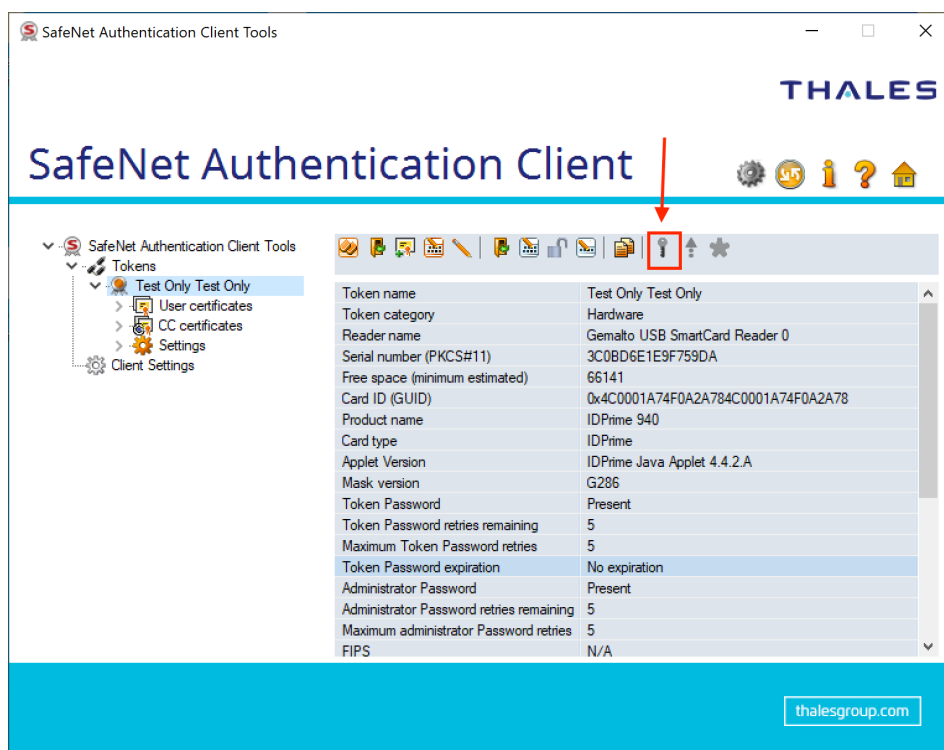


Slika 4



Slika 5

Za promjenu **Digital Signature PIN-a** pratite veoma sličnu procedure, s tim što ovdje treba da pritisnete na ikonicu  **Change Digital Signature PIN** (Slika 6).

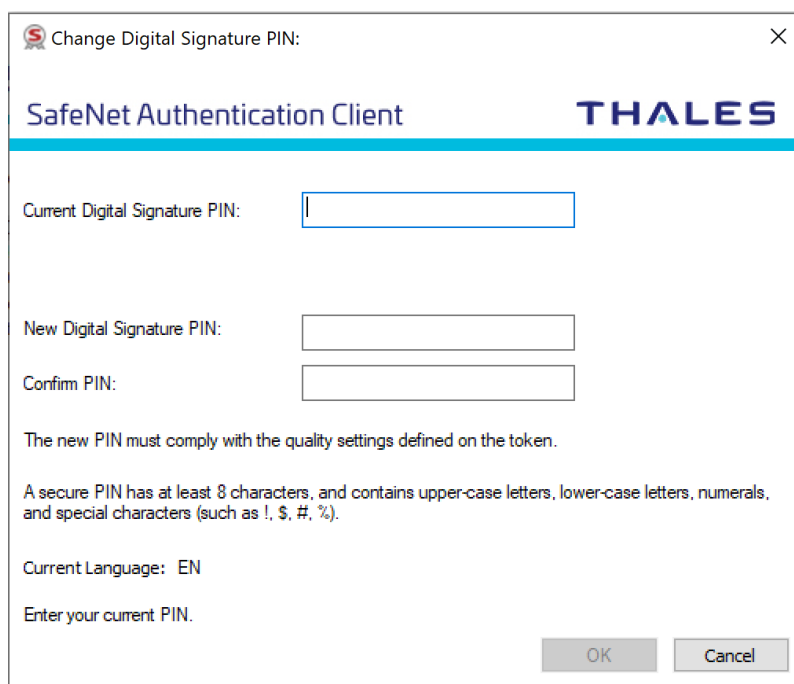


Slika 6

Unutar polja **Current Digital Signature PIN** unesite **PIN sa koverte** dok unutar **New Digital Signature PIN** i **Confirm PIN** polja unesite broj koji želite da vam predstavlja novi **PIN** (Slika 7). Obratite pažnju da dužina novog **PIN-a** ne smije da bude manja od **6 (šest)** cifara.

NAPOMENA: VEOMA JE VAŽNO ISTAĆI DA TOKEN PASSWORD BUDE ISTI KAO DIGITAL SIGNATURE PIN IZ RAZLOGA JEDNOSTAVNIJEG KORIŠĆENJA VAŠIH SERTIFIKATA.

PROMJENA PIN-A NIJE PREPORUČENA ALI UKOLIKO IPAK ŽELITE DA GA PROMJENITE, PAŽLJIVO PRATITE UPUTSTVA.



Slika 7

NAPOMENA: Ukoliko prilikom korišćenja sertifikata za autentifikaciju pogriješite unos PIN-a više od 5 (pet) puta, dok za sertifikat za kvalifikovani potpis pogriješite unos PIN-a više od 3 (tri) puta, token će se zaključati i Vaše sertifikate više nije moguće koristiti. Da bi ste uspješno otključali token potrebno je da postavite novi PIN. Procedura za postavljanje novog PIN-a je opisana u narednoj sekciji.

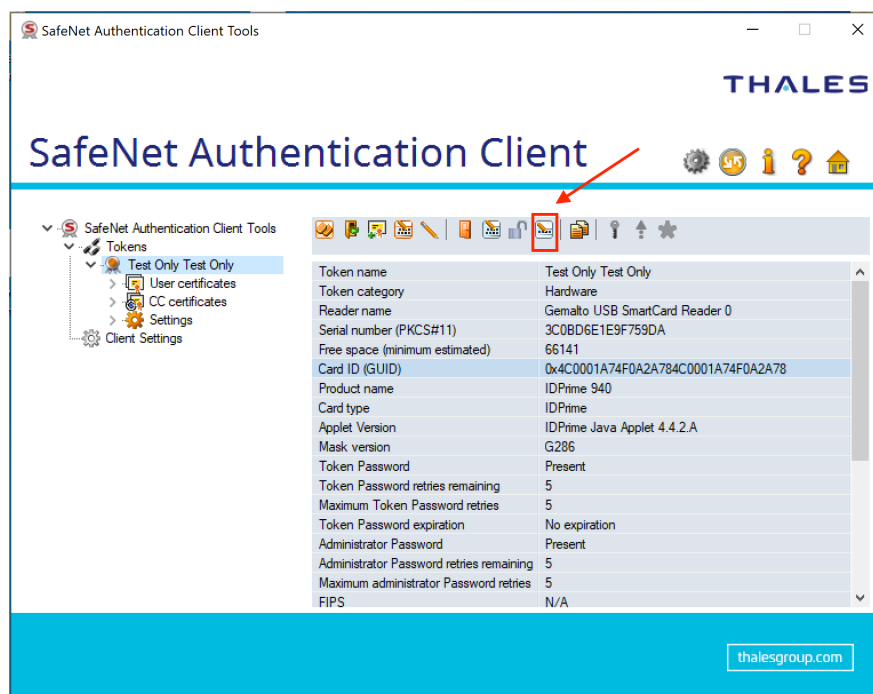
5. Postavljanje PIN-a

Ukoliko ste zaboravili PIN koji ste prethodno postavili ili ste zaključali Vaš token unoseći pogrešan PIN, novi PIN možete postaviti korišćenje **PUK-a** koji ste dobili u koverti prilikom preuzimanja tokena.

Kao što je naglašeno, prilikom promjene **PIN-a (iz koverta)**, potrebno je promijeniti Token Password i Digital Signature PIN i te dvije vrijednosti trebaju da budu iste, jer će one predstavljati Vaš novi **PIN** koji ćete koristiti kao validnu lozinku za oba sertifikata.

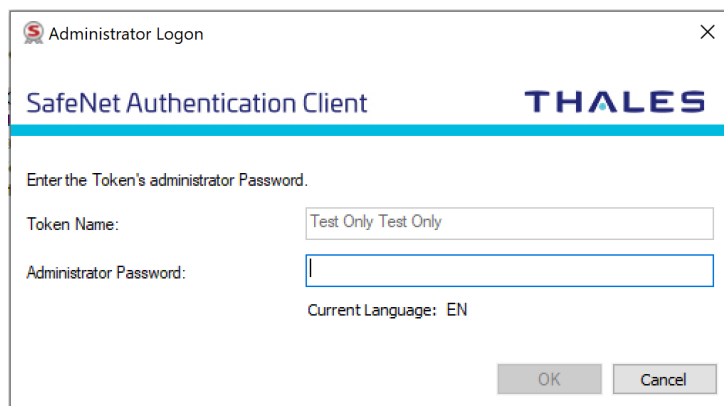
Za postavljanje PIN-a uz pomoć **PUK-a (iz koverta)** važi ista stvar. Potrebno je postaviti i Token password i Digital signature PIN.

Za postavljanje **Token Password-a** u Advanced View prozoru Safenet Authentication Client aplikacije pritisnite na ikonicu  **Set Token Password** (Slika 8).



Slika 8

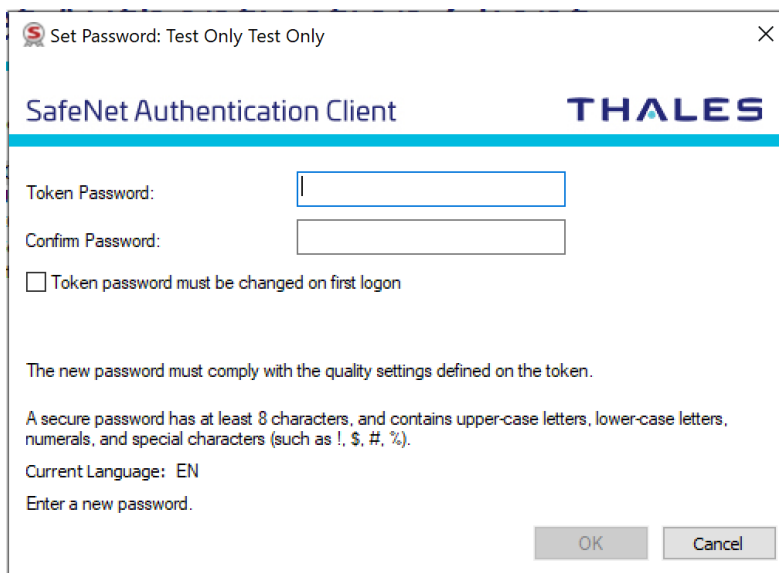
Na sledećem prozoru u polje **Administrator Password** unesite **PUK (iz koverte)** i pritisnite **OK** (Slika 9).



The dialog box is titled "Administrator Logon" and features the "SafeNet Authentication Client" and "THALES" logos. It contains a label "Enter the Token's administrator Password." followed by a "Token Name:" field with the text "Test Only Test Only". Below this is the "Administrator Password:" field, which is currently empty. To the right of the password field, it says "Current Language: EN". At the bottom right, there are "OK" and "Cancel" buttons.

Slika 9

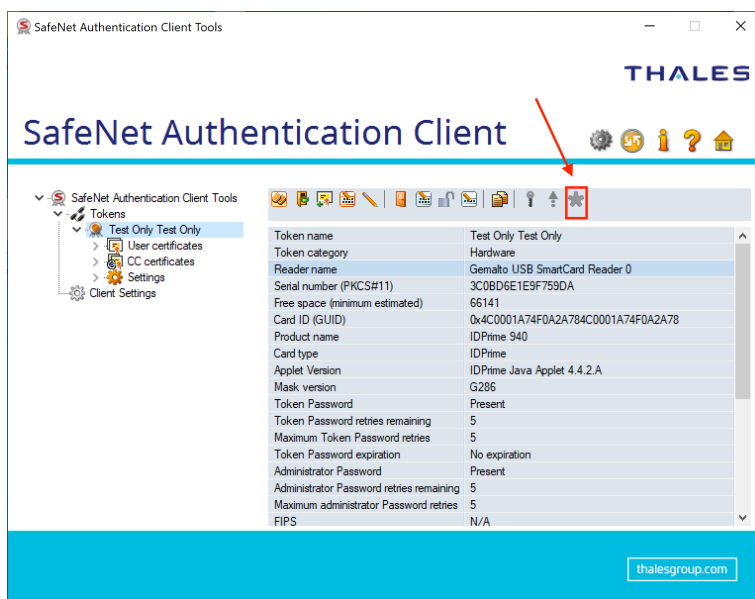
Nakon toga u poljima **Token Password** i **Confirm Password** unesite novi **PIN** koji želite da postavite (Slika 10). Obratite pažnju da dužina novog **PIN-a** ne smije da bude manja od **6 (šest)** cifara. Pritisnite **OK** i dobićete poruku da je password uspješno promjenjen.



The dialog box is titled "Set Password: Test Only Test Only" and features the "SafeNet Authentication Client" and "THALES" logos. It contains two password fields: "Token Password:" and "Confirm Password:". Below these fields is a checkbox labeled "Token password must be changed on first logon". A paragraph of text states: "The new password must comply with the quality settings defined on the token. A secure password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, \$, #, %).". Below this text, it says "Current Language: EN" and "Enter a new password.". At the bottom right, there are "OK" and "Cancel" buttons.

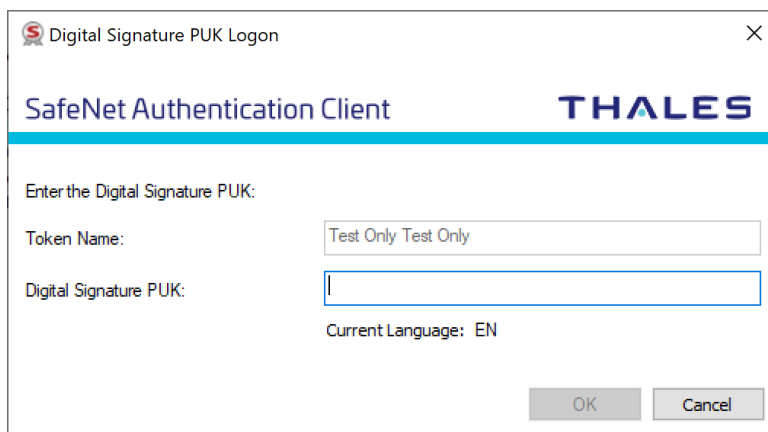
Slika 10

Za postavljanje Digital Signature PIN-a potrebno je kliknuti na ikonicu  **Set Digital Signature PIN** (Slika 11).



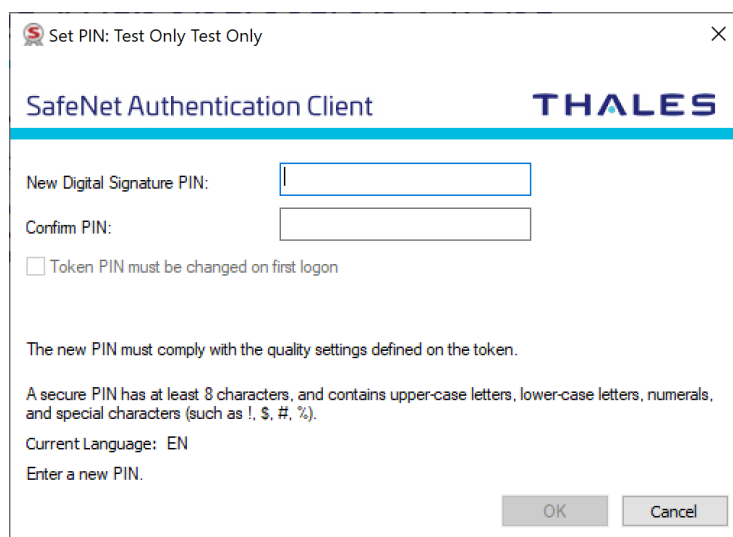
Slika 11

Na sličan način se otvara prozor, gdje u polju **Digital Signature PUK** unosite PUK iz koverte koju ste dobili prilikom preuzimanja tokena (Slika 12).



Slika 12

Nakon toga, u novom prozoru, unutar polja **New Digital Signature PIN** i **Confirm PIN** unesite novi **PIN** koji želite da postavite (Slika 13). Obratite pažnju da dužina novog **PIN-a** ne smije da bude manja od **6 (šest)** cifara. Pritisnite **OK** i dobićete poruku da je password uspješno promjenjen.



Slika 13

NAPOMENA: NIJE PREPORUČENO MIJENJATI PUK KOJI DOBIJETE U KOVERTI. UKOLIKO PROMJENITE PUK I ISTI ZABORAVITE, NIJE MOGUĆE OTKLJUČATI TOKEN U SLUČAJU DA GA ZAKLJUČATE POGREŠNIM UNOSOM PIN-A.

MJENJANJE PIN-A I PUK-A JE U POTPUNOSTI VAŠA ODGOVORNOST!!! UKOLIKO ZAKLJUČATE TOKEN I ISTI STE U NEMOGUĆNOSTI DA OTKLJUČATE, POTREBNO JE POKRENUTI PROCEDURU ZA RE-IZDAVANJE SERTIFIKATA PO VAŽEĆIM CIJENAMA.

Zato je **VEOMA VAŽNO** naglasiti da i ukoliko promijenite PIN i PUK, iste i zapišete i čuvate na sigurnom mjestu kako bi ste spriječili zloupotrebu vaših lozinki.