

Manual pentru Instalarea Certificatului Digital Calificat DigiSign

Versiunea 4.0

În vederea folosirii corespunzătoare a certificatului digital calificat emis de **DigiSign**, vă rugăm să urmați instrucțiunile din acest manual.

Nerespectarea acestor specificații sau utilizarea altor opțiuni din aplicație decât cele indicate în manual pot duce la întârzierea folosirii cu succes a certificatului digital sau la pierderea acestuia.

În continuare, vă este prezentat un exemplu de instalare a certificatului pe sistemul de operare Windows 10. Imaginile pot fi diferite în cazul altor versiuni de Windows, însă pașii sunt aceiași.

1. Asigurați-vă că sistemul dumneavoastră de operare este actualizat la zi

Folosiți funcția **Windows Update** sau urmați procedurile de pe site-ul Microsoft în vederea instalării ultimelor update-uri aferente sistemului dumneavoastră de operare.

Asigurați-vă că:

- **aveți drept de administrator pe sistemul pe care doriți să instalați certificatul digital**
- **ceasul, data și fusul orar de pe calculator sunt corect setate**
- **dispozitivul eToken **NU** este conectat în extensia USB a calculatorului pe durata procesului de instalare al aplicațiilor!**

2. Instalarea aplicațiilor necesare utilizării dispozitivului eToken și a certificatului digital calificat.

Pentru a putea folosi dispozitivul securizat SafeNet eToken pe care se află certificatul digital calificat (utilizat pentru crearea semnăturii electronice calificate), trebuie să instalați **lanțul de încredere DigiSign**, precum și **driverul SafeNet Authentication Client al dispozitivului dvs. eToken**.

a) **Instalarea lanțului de încredere DigiSign**

- Accesați <http://www.digisign.ro/uploads/cert.zip> și salvați lanțul de încredere în calculatorul dvs.

Pagina 1 din 9

- Deschideți arhiva **cert.zip** pe care ați descărcat-o și dezarhivați-o (click-dreapta -> *Extract Here* sau dublu-click -> *Extract To*). În acest moment, ați extras executabilul **cert.exe**.
- *Click-dreapta* pe executabilul **cert.exe** și *Run as Administrator*.



b) **Instalarea driver-ului eToken PKI Client**

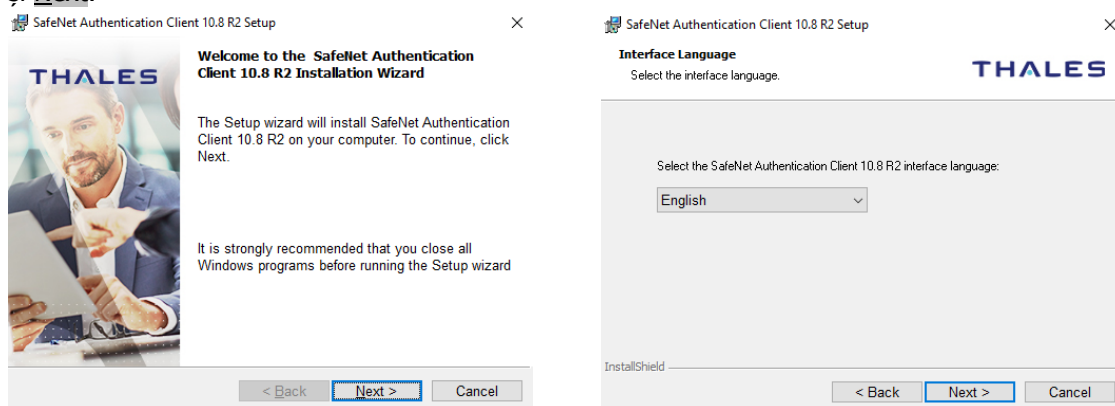
Compatibilitate: - Windows Vista, Windows 7, 8, 10, 11, Windows Server 2003, 2008, 2012, 2016, 2019.

Vă rugăm să alegeți driverul în funcție de versiunea sistemului de operare folosit:

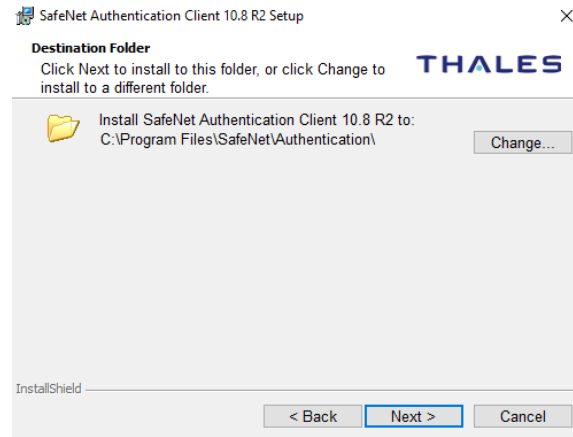
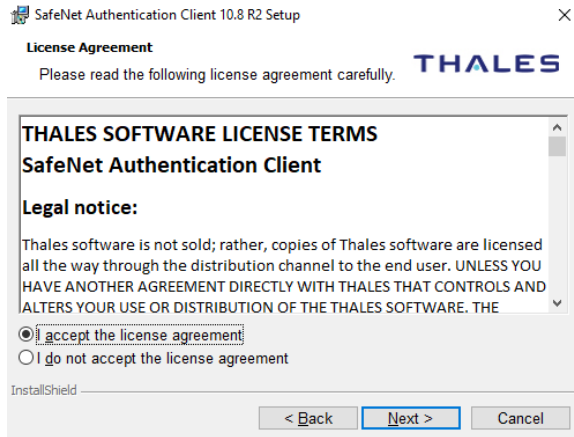
- ✓ 32 biti : http://www.digisign.ro/uploads/DigiSign_eToken_PKI_Client_x32.msi
- ✓ 64 biti : http://www.digisign.ro/uploads/DigiSign_eToken_PKI_Client_x64.msi

IMPORTANT: Înainte de a instala driver-ul, asigurați-vă că dispozitivul eToken NU este conectat în portul USB al calculatorului dvs.

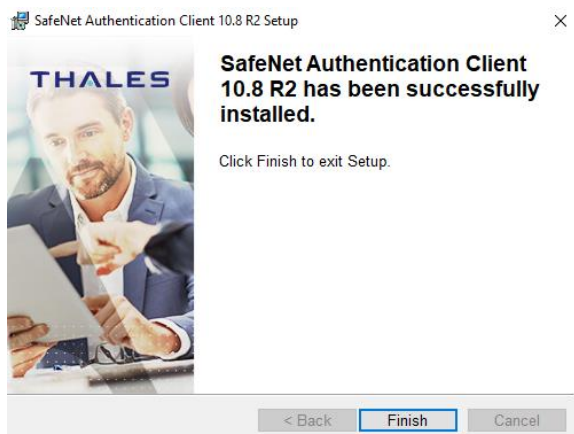
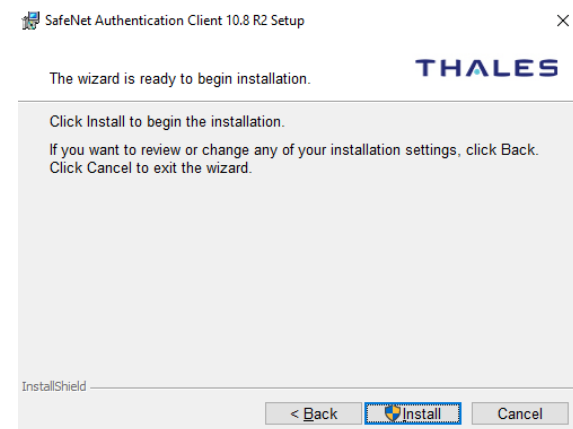
- Deschideți fișierul descărcat;
- În fereastra deschisă, apăsați butonul **Next** pentru a începe procesul instalării, selectați limba dorită și **Next**.



- Bifați câmpul **•I accept the license agreement**, apăsați butonul **Next**, iar în următoarea fereastră selectați iar butonul **Next**.



- Apăsați butoanele **Next**, **Install** și apoi **Finish**.



3. Verificarea instalării corespunzătoare a aplicațiilor

a) Verificarea instalării corespunzătoare a lanțului de încredere **DigiSign**

Alegeți **una** dintre variantele de mai jos pentru a verifica instalarea cu succes a lanțului de încredere **DigiSign**. Dacă observați că certificatele de mai jos **nu se regăsesc** în aplicațiile de pe calculatorul utilizat, va trebui să repetați procesul de instalare al lanțului de încredere prezentat la punctul 2. a) (pag.1) al acestui document.

1. Folosind browserul **Microsoft Edge**

- Deschideți browserul Microsoft Edge. Din meniul Settings selectați → Privacy, Search, and services → Security → Manage Certificates → Intermediate Certification Authorities.

În lista respectivă ar trebui să apară certificatul *DigiSign Qualified CA Class 3 2017*, dacă instalarea lanțului de încredere a fost făcută corespunzător.

- Deschideți browserul Microsoft Edge. Din meniul Settings selectați → Privacy, Search, and services → Security → Manage Certificates → Trusted Root Certification Authorities

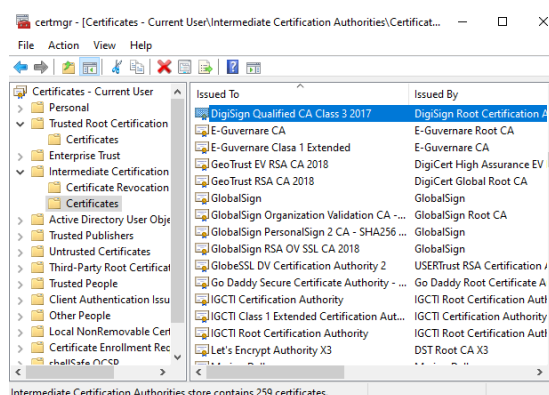
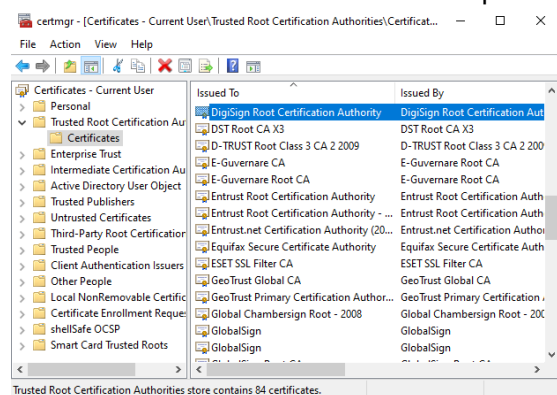
În lista respectivă ar trebui să apară certificatul *DigiSign Root Certification Authority*, dacă instalarea lanțului de încredere a fost făcută corespunzător.

2. Folosind utilitarul **Certificate Manager**

Din meniul **Start** al **Windows**-ului alegeți opțiunea **Run**. Tastați **certmgr.msc** și apăsați butonul **OK**.

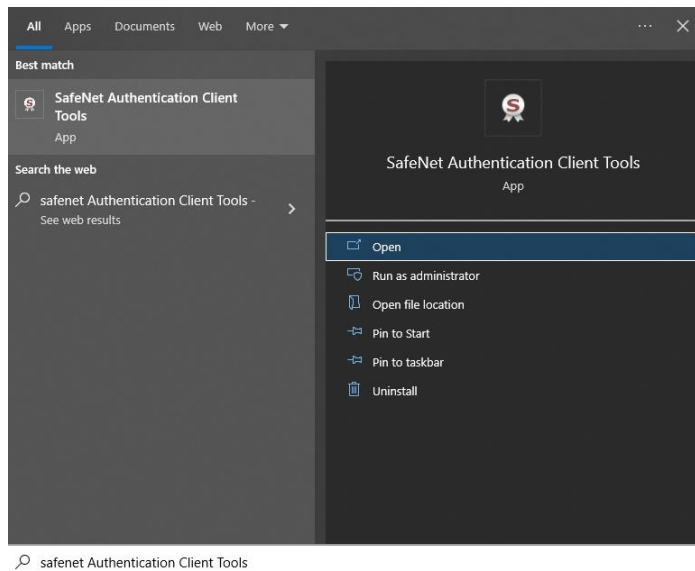
- Selectați Certificates–Current User → Trusted Root Certification Authorities → Certificates. În lista din dreapta ar trebui să apară certificatul *DigiSign Root Certification Authority*, dacă instalarea lanțului de încredere a fost făcută corespunzător.

- Certificates–Current User → Intermediate Certification Authorities → Certificates. În lista din dreapta ar trebui să apară certificatul *DigiSign Qualified CA Class 3 2017*, dacă instalarea lanțului de încredere a fost făcută corespunzător.

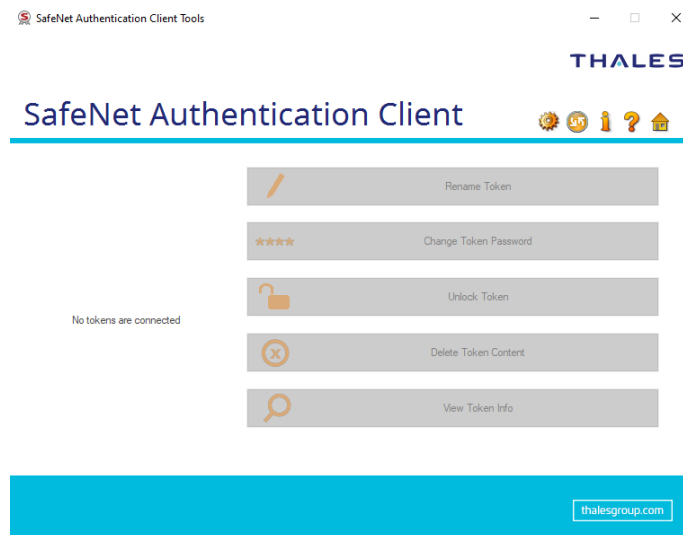


b) Verificarea instalării corespunzătoare a driver-ului pentru dispozitivul **eToken**

- ✓ Din meniul **Start**, cautați **SafeNet Authentication Tools**.



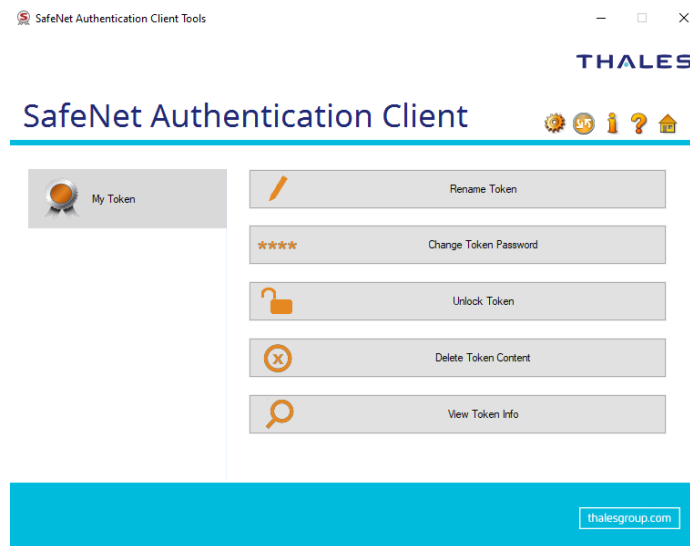
- ✓ Dacă utilitarul a fost instalat cu succes, vi se va afișa fereastra din imaginea următoare:



În acest moment, lanțul de încredere DigiSign și driverul sunt corect instalate !

4. Utilizarea corespunzătoare a driver-ului pentru dispozitivul eToken

- Introduceți dispozitivul eToken în extensia USB a calculatorului.
- Din meniul **Start**, cautați **SafeNet Authentication Tools**.
- Pe ecran se va afișa **Panoul de comandă** al dispozitivului eToken:



a) **Rename Token (funcția de redenumire a dispozitivului eToken)**

Această funcție este opțională și permite utilizatorului să schimbe numele dispozitivului (pentru personalizare). Numele inițial al dispozitivului dvs este *My Token*.

b) **Change Password (funcția de schimbare a parolei dispozitivului eToken)**

Această funcție este recomandată și permite utilizatorului să schimbe parola dispozitivului.

Dacă optați pentru schimbarea parolei inițiale, vă rugăm să luați în considerație faptul că driver-ul nu păstrează un istoric al parolelor. Prin urmare, odată schimbată parola inițială, noua parolă devine responsabilitatea dvs.

IMPORTANT (!):

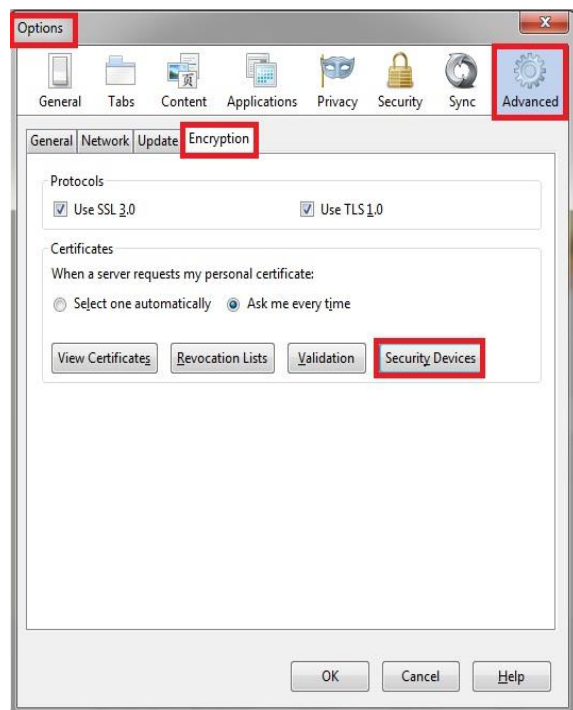
- **În cazul în care parola este introdusă greșit de mai mult de 15 ori consecutiv, dispozitivul se va bloca.**

5. Activarea/dezactivarea modului eToken în browser-ul Mozilla Firefox

Activarea modului eToken în browser-ul Mozilla Firefox este **strict opțională** și recomandată doar în cazul în care doriți să vă logați pe anumite portale cu acest browser sau să completați formularul de reînnoire online a certificatului digital calificat care poate fi accesat la adresa www.digisign.ro.

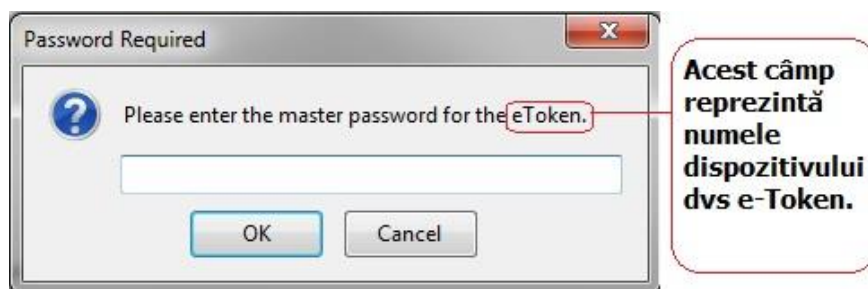
1. Activarea modului eToken

- Deschideți browser-ul Mozilla Firefox, accesați: *Options* → *Advanced* → *Encryption* → *Security Devices*
- În noua fereastră deschisă, apăsați butonul *Load*, selectați din calculatorul dvs prin butonul *Browse* fișierul *eTPKCS11.dll* (gasit în directorul *Windows* → *system32*).
- Apăsați butonul **OK**, iar modulul eToken se va activa în browser.



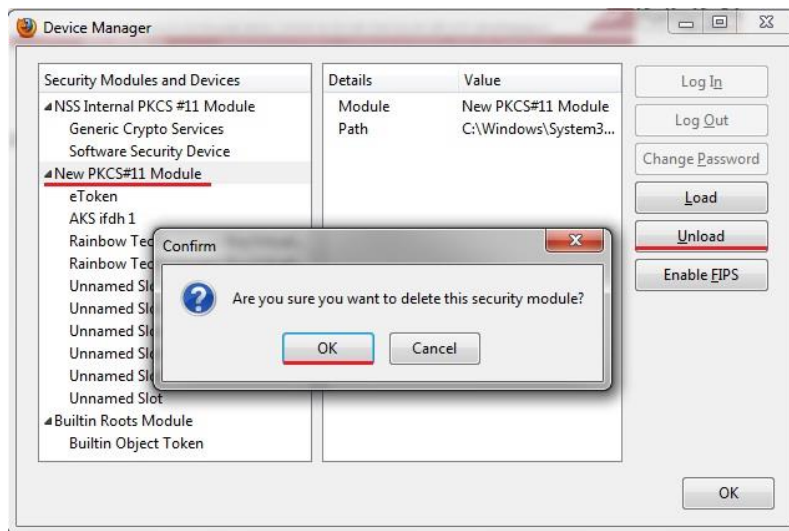
IMPORTANT:

Dacă aveți introdus în calculator dispozitivul dvs eToken și deschideți browser-ul Mozilla Firefox, iar acesta vă afișează o fereastră de tipul celei de mai jos, va trebui să introduceți parola dispozitivului dvs eToken.



2. Dezactivarea modulului eToken

- Deconectați dispozitivul dvs eToken din calculator
- Deschideți browser-ul Mozilla Firefox, accesați meniul:
Options → *Advanced* → *Encryption* → *Security Devices*
- În noua fereastră deschisă, selectați câmpul: · numele dispozitivul dvs eToken
sau
· "New PKCS#11 Module"
- Apăsați butonul **Unload** și apăsați butonul **OK**.



În acest moment, modulul eToken din browser-ul Mozilla Firefox este dezactivat.

DigiSign S.A. eliberează certificate digitale calificate în conformitate cu Regulamentul eIDAS 910/2014. Aceste certificate calificate pot fi utilizate în mai multe sisteme (de exemplu: **ANAF, CNVM, ONRC, CSSPP, AEGRM, CSA-CEDAM, SEAP**), unde DigiSign S.A. nu este operator și nu are posibilitatea de a vă acorda consultanță/sprrijin pentru utilizarea facilităților acestor sisteme care aparțin unor instituții ale statului. Pentru a beneficia de accesul în aceste sisteme, precum și modalitatea de utilizare a certificatului digital calificat obținut în cadrul acestora, vă rugăm să contactați administratorii respectivelor sisteme.

Link-uri utile:

- [Instalare si configurare Semnătură Electronică pentru Microsoft Office 2016](#)
- [Instalare și configurare Semnătură Electronică pentru Microsoft Outlook 2016](#)
- [Instalare și configurare Semnătură Electronică pentru Mozilla Thunderbird](#)
- [Instrucțiuni completare fisier de confirmare](#)
- [Instrucțiuni depunere declarații online ANAF](#)
- [Download Adobe Acrobat Reader](#)

Tutoriale video:

- [Instalarea certificatului digital - tutorial video](#)
- [Reinnoirea certificatului digital la ANAF - tutorial video](#)

Actualizări:

Nr. Crt.	Versiunea în vigoare	Data
1	3.0	16.10.2014
2	3.1	21.07.2017
3	3.2	07.04.2021
4	4.0	26.07.2022