

Manual pentru Instalarea Certificatului Digital Calificat DigiSign

Versiunea 3.0

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 7. Imaginile pot fi diferite în cazul altor versiuni de Windows, însă pașii sunt aceiași.

Atenție: În cazul în care ați **reînnoit** certificatul digital, iar aplicațiile sunt deja instalate pe calculator, vă rugăm **să reinstalați doar lanțul de încredere** de la punctul **2. a)** (pag. 2).

1. Asigurați-vă că sistemul dumneavoastră de operare este actualizat la zi și că nu aveți vreun program de tip antivirus/firewall ce ar putea bloca instalarea corespunzătoare a driver-ului dispozitivului USB eToken.

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

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!**

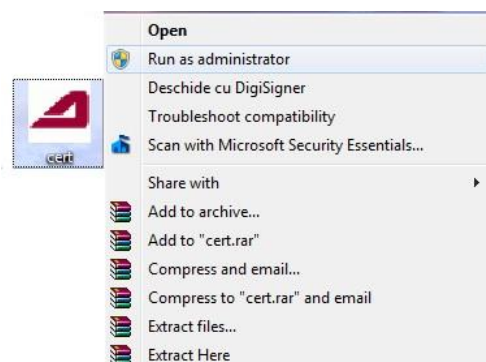


2. Instalarea aplicațiilor necesare utilizării dispozitivului eToken și a certificatului digital calificat.

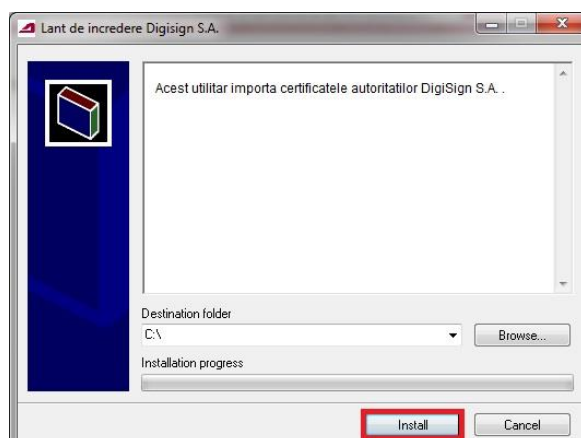
Pentru a putea folosi dispozitivul securizat Aladdin eToken pe care se află certificatul digital calificat (utilizat pentru crearea semnăturii electronice extinse), trebuie să instalați **lanțul de încredere DigiSign**, precum și **driverul DigiSign eToken PKI Client 8 al dispozitivului dvs eToken**.

a) **Instalarea lanțului de încredere DigiSign**

- Accesați <http://www.digisign.ro/uploads/cert.zip> și salvați lanțul de încredere în calculatorul dvs.
- 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**.
- Dacă folosiți sistemul de operare Windows 7 sau Windows 8, instalați lanțul de încredere prin *click-dreapta* pe executabilul **cert.exe** și *Run as Administrator*. Dacă folosiți sistemul de operare Windows XP, instalați lanțul de încredere prin *dublu-click* pe executabil.



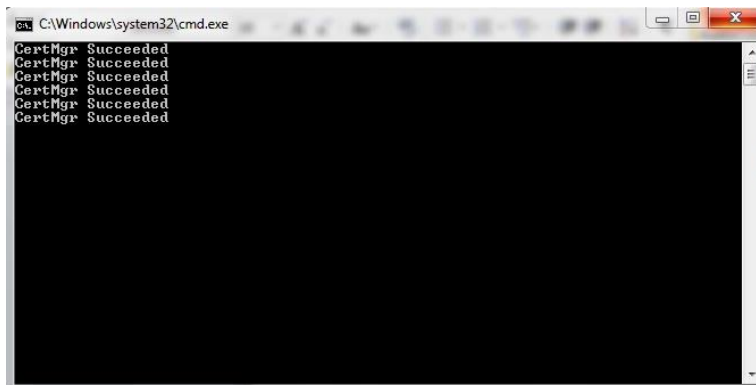
- Vi se va deschide utilitarul de importare a certificatelor **DigiSign**. Apăsați butonul **Install**.



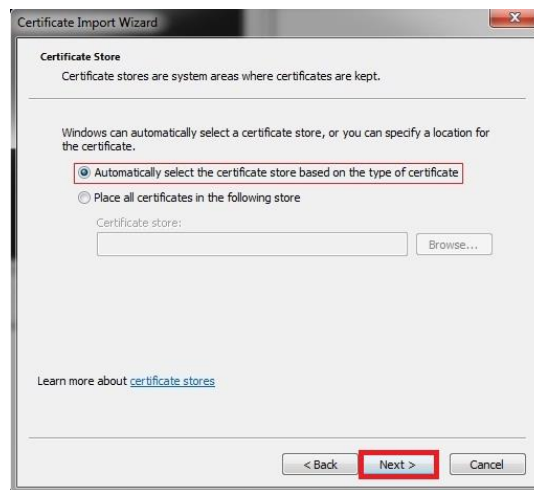
IMPORTANT: Asigurați-vă că lanțul de încredere se instalează corect!

Într-o fereastră asemănătoare cu cea prezentată în imaginea de mai jos, va fi afișat mesajul "CertMgr Succeeded" atunci când lanțul de încredere a fost instalat cu succes.

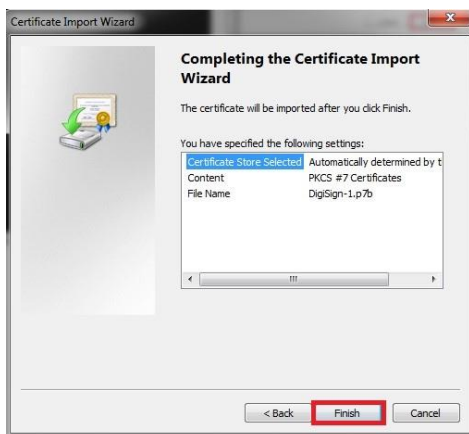
Dacă primiți mesajul **CertMgr Failed**, va trebui să dați *click-dreapta* pe fișierul **cert.exe** și să selectați opțiunea „Run as Administrator” (!) .



- În continuare, apăsați butonul **Next**, iar în următoarea fereastră, lăsați câmpul **Automatically...** bifat și alegeți butonul **Next**.



- Importarea certificatului a fost făcută cu succes, apăsați butonul **Finish**, iar apoi **OK**.



b) Instalarea driver-ului *DigiSign eToken PKI Client 8*

Compatibilitate: - Windows XP, Windows Vista, Windows 7, Windows 8;
- Windows Server 2003, Windows Server 2008, Windows Server 2012.

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

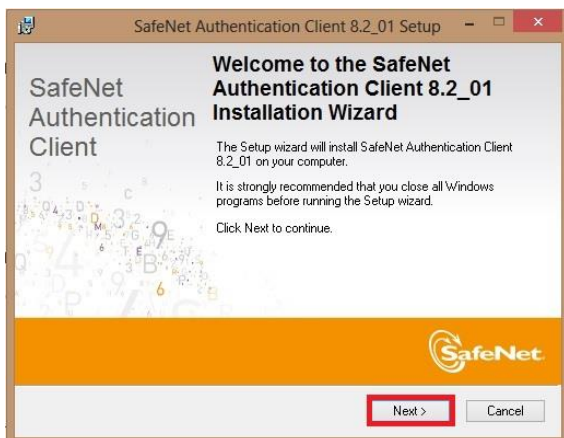
- ✓ 32 biti : http://www.digisign.ro/uploads/DigiSign_eToken_PKI_Client_x32.msi
- ✓ 64 biti : http://www.digisign.ro/uploads/DigiSign_eToken_PKI_Client_x64.msi

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

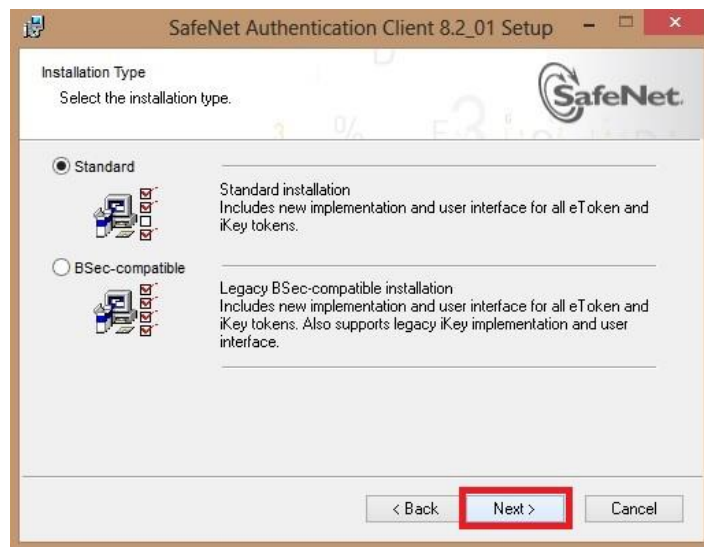
- Selectați fișierul descărcat; în cazul în care folosiți sistemul de operare Windows 7 sau Windows 8, prin *click-dreapta* apăsați butonul **Run as administrator**, iar în cazul în care folosiți Windows XP, apăsați *dublu-click*. Apăsați butonul **Run**.



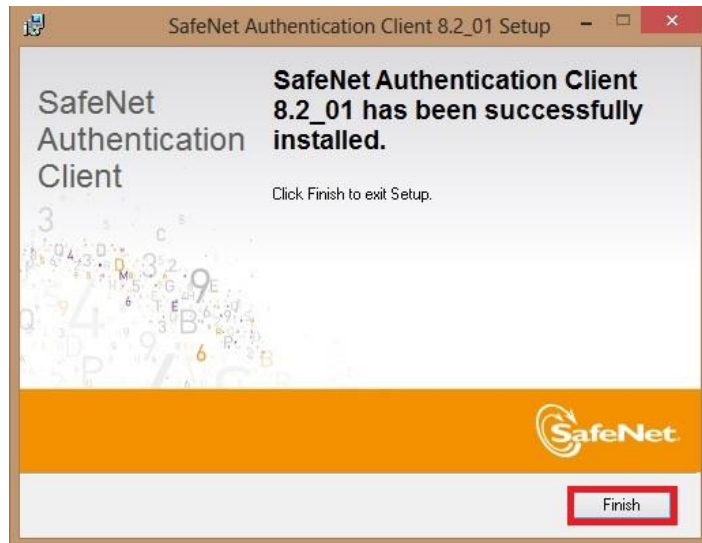
- În fereastra deschisă, apăsați butonul **Next** pentru a începe procesul instalării, selectați limba dorită și **Next**.



- Bifați câmpul **I accept the license agreement**, apăsați butonul **Next**, iar în următoarea fereastră lăsați bifat tipul **Standard** și continuați alegând butonul **Next**.



- Apăsați butonul **Next** și **Finish** pentru a finaliza instalarea driver-ului.



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.2) al acestui document.

1. Folosind browserul **Internet Explorer**

Deschideți browserul Internet Explorer. Din meniul Tools selectați → Internet Options → Content → Certificates → Intermediate Certification Authorities

În lista respectivă ar trebui să apară certificatul: *DigiSign Qualified Public CA* și *DigiSign Qualified Root CA v2* dacă instalarea lanțului de încredere a fost făcută corespunzător.

Deschideți browserul Internet Explorer. Din meniul Tools selectați → Internet Options → Content → Certificates → Trusted Root Certification Authorities

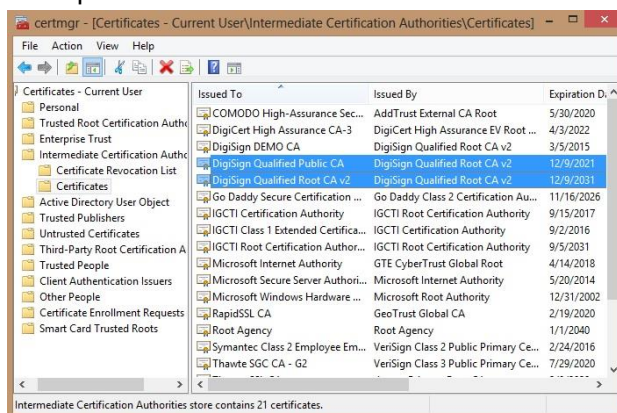
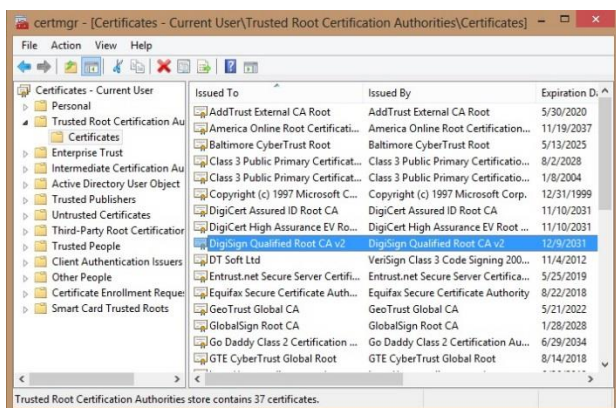
În lista respectivă ar trebui să apară certificatul: *DigiSign Qualified Root CA v2* dacă instalarea lanțului de încredere a fost făcută corespunzător.

2. Folosind utilitarul **Certificate Manager**

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

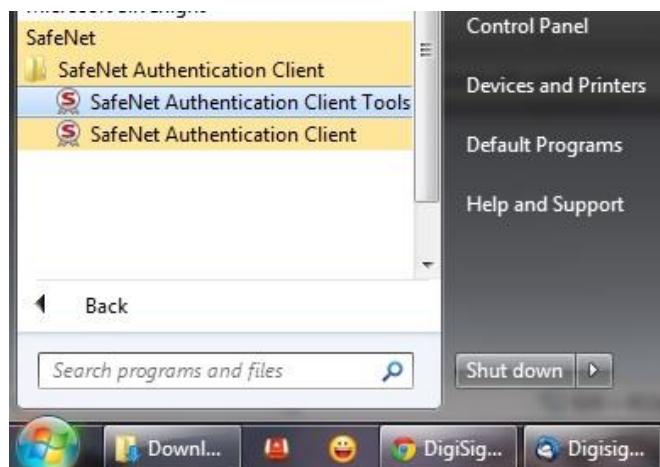
Selectați Certificates–Current User → Trusted Root Certification Authorities → Certificates. În lista din dreapta ar trebui să apară un certificat DigiSign: *DigiSign Qualified Root CA v2* dacă instalarea lanțului de încredere a fost făcută corespunzător.

Certificates–Current User → Intermediate Certification Authorities → Certificates. În lista din dreapta ar trebui să apară un certificat DigiSign: *DigiSign Qualified Public CA* și *DigiSign Qualified Root CA v2* dacă instalarea lanțului de încredere a fost făcută corespunzător.



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

- ✓ Din meniul **Start**, alegeți **All Programs** → **SafeNet** → **SafeNet Authentication Client** → **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**, alegeți **All Programs** → **SafeNet** → **SafeNet Authentication Client** → **SafeNet Authentication Tools**.
- Pe ecran se va afișa **Panoul de comandă** al utilitarului Aladdin eToken:



a) **Rename eToken (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*.

- Apăsați butonul .
- În fereastra care se va deschide, introduceți parola dispozitivului dvs și apăsați **OK**.



- În câmpul **New token name**, introduceți denumirea personalizată dorită și apăsați **OK**.



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. **NU EXISTĂ** posibilitatea de deblocare a acestuia.

- Apăsați butonul



- În fereastra deschisă, scrieți parola actuală în primul câmp, iar în următoarele doua câmpuri scrieți parola nouă și apăsați butonul **OK**.



În acest moment, parola a fost schimbată cu succes, iar driverul este configurat corect; nu mai sunt necesare alte operații în aplicație și certificatul poate fi utilizat

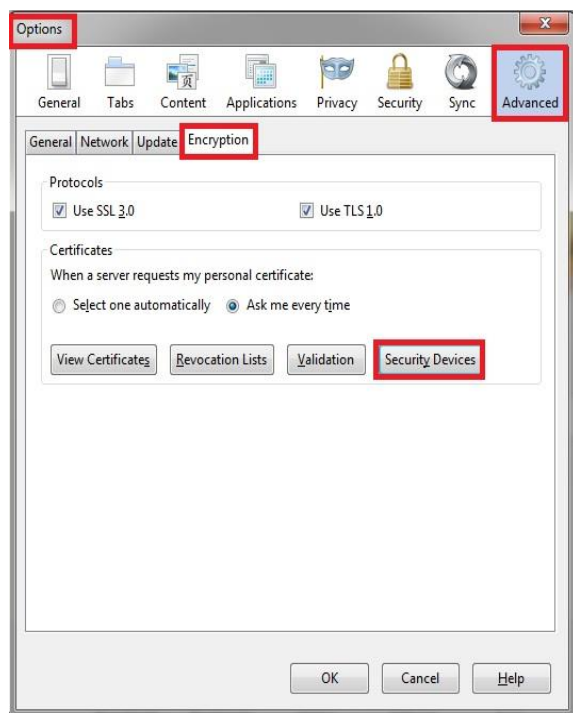


5. Activarea/dezactivarea modului eToken în browser-ul Mozilla Firefox

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 portal.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.



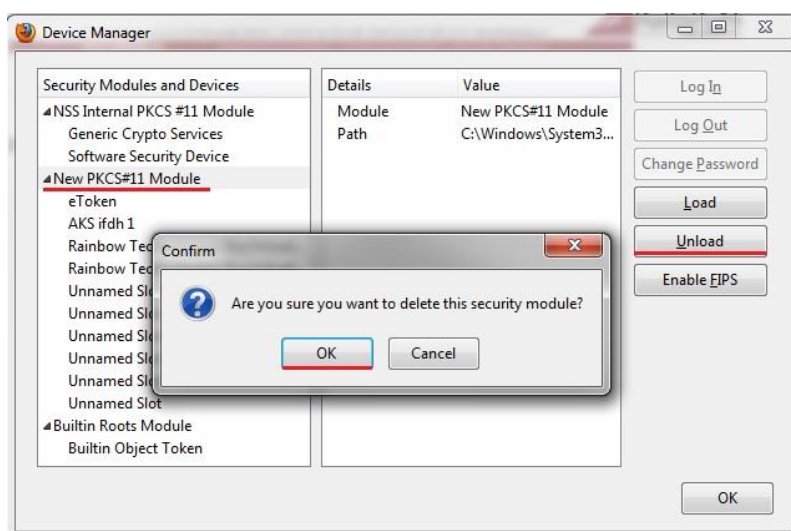
IMPORTANT:

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 modului 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 dispozitivului 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.



S.C. DigiSign S.A. eliberează certificate digitale calificate conform Legii nr. 455/2001 privind semnătura electronică. Aceste certificate calificate pot fi utilizate în mai multe sisteme (de exemplu: **ANAF, CNVM, ONRC, CSSPP, AEGRM, CSA-CEDAM, SEAP**), unde S.C. DigiSign S.A. nu este operator și nu are posibilitatea de a vă acorda consultanță/sprijin 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 și configurare Semnătură Electronică pentru Microsoft Office 2007](#)
- [Instalare și configurare Semnătură Electronică pentru Microsoft Outlook 2007](#)
- [Instalare și configurare Semnătură Electronică pentru Mozilla Thunderbird 3.0.1](#)
- [Instalare și configurare Semnătură Electronică pentru Outlook Express 6](#)
- [Instrucțiuni completare fișier de confirmare](#)
- [Instrucțiuni depunere declarații on-line ANAF](#)
- [Download Adobe Acrobat Reader 8.2](#)

Tutoriale video:

- [Înălarea certificatului digital - tutorial video](#)
- [Înregistrarea certificatului digital la ANAF - tutorial video](#)

Actualizări:

Nr. Crt.	Versiunea în vigoare	Data
1	3.0	16.10.2014

