

Ghid de instalare a certificatului digital

Data: 17.05.10

Versiune: V13-17.05.2010

Se aplică pentru:

- Aladdin eToken Pro – PKI Client 5.1-SP1 x32 și x64 biți
- SafeNet iKey 2032 – SafeNet Borderless Security PK Client
- Oberthur Cosmo64 RSA v5.4 – AuthentIC Manager
- Internet Explorer și Mozilla Firefox
- Lanțul de încredere certSIGN
- clickSIGN

CUPRINS

| | |
|--|-----------|
| 1. IDENTIFICAREA DISPOZITIVULUI CRIPTOGRAFIC (OBLIGATORIU) | 4 |
| 1.1. ALADDIN eTOKEN PRO..... | 4 |
| 1.2. SAFE NET iKEY 2032..... | 4 |
| 1.3. OBERTHUR COSMO64..... | 5 |
| 2. INSTALAREA DISPOZITIVULUI CRIPTOGRAFIC (OBLIGATORIU) | 6 |
| 2.1. IDENTIFICAREA TIPULUI SISTEMULUI DE OPERARE..... | 6 |
| 2.2. INSTALAREA DISPOZITIVULUI CRIPTOGRAFIC ALADDIN eTOKEN PRO..... | 8 |
| 2.3. INSTALAREA DISPOZITIVULUI CRIPTOGRAFIC SAFE NET iKEY 2032 | 11 |
| 2.4. INSTALAREA DISPOZITIVULUI CRIPTOGRAFIC OBERTHUR | 12 |
| 3. ACCESAREA DISPOZITIVULUI ȘI SCHIMBAREA CODULUI PIN (RECOMANDAT).... | 19 |
| 3.1. SCHIMBAREA CODULUI PIN PENTRU DISPOZITIVUL CRIPTOGRAFIC ALADDIN eTOKEN PRO..... | 19 |
| 3.2. SCHIMBAREA CODULUI PIN PENTRU DISPOZITIVUL CRIPTOGRAFIC SAFE NET iKEY 2032 | 21 |
| 3.3. SCHIMBAREA CODULUI PIN PENTRU DISPOZITIVUL CRIPTOGRAFIC OBERTHUR | 22 |
| 4. INSTALAREA CERTIFICATULUI ÎN INTERNET EXPLORER (OPȚIONAL) | 24 |
| 5. INSTALAREA MODULULUI CRIPTOGRAFIC ÎN MOZILLA FIREFOX (OPȚIONAL) ... | 26 |
| 6. INSTALAREA CERTIFICATULUI ÎN MOZILLA FIREFOX (OPȚIONAL) | 28 |
| 7. INSTALAREA CERTIFICATULUI AUTORITĂȚII CERTSIGN ROOT CA ÎN MOZILLA FIREFOX (OPȚIONAL) | 31 |
| 8. INSTALAREA LANȚULUI DE ÎNCREDERE CERTSIGN (RECOMANDAT) | 32 |
| 9. UTILIZAREA CERTIFICATULUI DIGITAL (OBLIGATORIU) | 34 |
| 10. INSTALAREA APLICAȚIEI CLICKSIGN (OBLIGATORIU)..... | 35 |
| 11. DEFINIȚII ȘI ACRONIME | 40 |

Felicitări! Dacă vă aflați în această etapă, înseamnă că ați intrat în posesia unui certificat digital emis de certSIGN și doriți să beneficiați de toate avantajele utilizării lui.

Acest ghid se adresează tuturor posesorilor de certificate digitale emise de Autoritatea de Certificare a certSIGN și conține pașii ce trebuie urmați pentru o primă utilizare cu succes a certificatului digital achiziționat.

În cazul în care întâmpinați dificultăți privind instalarea acestuia sau orice altă problemă de ordin tehnic, departamentul nostru de suport vă stă la dispoziție:

- ✓ **Telefon:** 0311.509.111 sau 021.311.99.08
- ✓ **E-mail:** suport@certsign.ro.

1. Identificarea dispozitivului criptografic (obligatoriu)

1.1. Aladdin eToken Pro

În cazul în care dispozitivul dumneavoastră criptografic este identic cu cel din imaginea de mai jos, acest dispozitiv este un token **Aladdin eToken Pro** pentru care este necesară instalarea aplicației **PKI Client 5.1-SP1**. Pașii necesari instalării acestei aplicații se regăsesc la punctul 2.2.



Figura 1 Dispozitiv criptografic Aladdin eToken Pro

1.2. SafeNet iKey 2032

În cazul în care dispozitivul dumneavoastră criptografic este identic cu unul din dispozitivele din imaginea de mai jos, acest dispozitiv este un token **SafeNet iKey 2032** pentru care este necesară instalarea aplicației **SafeNet Borderless Security PK Client**. Pașii necesari instalării acestei aplicații se regăsesc la punctul 2.3.



Figura 2 Dispozitive criptografice SafeNet iKey 2032

1.3.Oberthur Cosmo64

În cazul în care dispozitivul dumneavoastră criptografic este identic cu cel din imaginea de mai jos, acest dispozitiv este un token **OberthurCosmo64** pentru care este necesară instalarea aplicației AuthentIC Manager. Pașii necesari instalării acestei aplicații precum și a driverelor se regăsesc la punctul 2.4



Figura 3 Dispozitiv criptografic Oberthur Cosmo64

2. Instalarea dispozitivului criptografic (obligatoriu)

Pentru a putea utiliza certificatul dumneavoastră trebuie să instalați dispozitivul criptografic pe care aveți generate atât cheile cât și certificatul. Driverul necesar dispozitivului sunt localizate pe CD-ul primit de la certSIGN.

Pentru instalarea driverelor vă rugăm să urmați pașii de mai jos

2.1. Identificarea tipului sistemului de operare

- Pentru a verifica tipul sistemului dumneavoastră de operare efectuați click pe **Start** și apoi click dreapta pe **My Computer** (Windows XP) sau pe **Computer** (Windows Vista). Efectuați click pe **Properties** și în fereastra **System Properties**, verificați informațiile din câmpul **System** (Windows XP), respectiv **System Type** (Windows Vista), întocmai ca în imaginile de mai jos.

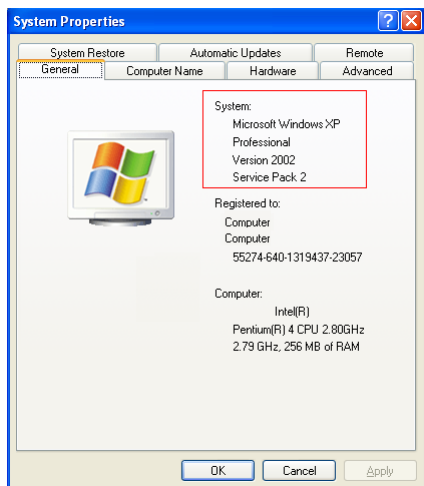



Figura 4 Microsoft Windows XP 32 biți Figura 5 Microsoft Windows XP 64 biți

View basic information about your computer

Windows edition

Windows Vista™ Ultimate
Copyright © 2007 Microsoft Corporation. All rights reserved.
Service Pack 1

System

Manufacturer: Lenovo
Model: Lenovo Computer
Rating:  1.0 Windows Experience Index
Processor: Intel(R) Pentium(R) 4 CPU 2.80GHz 2.79 GHz
Memory (RAM): 3.00 GB
System type: 32-bit Operating System

Computer name, domain, and workgroup settings

Computer name: Computer
Full computer name: Computer
Computer description:
Workgroup: WORKGROUP

Windows activation


Windows is activated
Product ID: 89733-OEM-7373332-73331 


Figura 6 Microsoft Windows Vista 32 biți

View basic information about your computer

Windows edition

Windows Vista™ Ultimate
Copyright © 2007 Microsoft Corporation. All rights reserved.
Service Pack 1

System

Manufacturer: Lenovo
Model: Lenovo Computer
Rating:  1.0 Windows Experience Index
Processor: Intel(R) Pentium(R) 4 CPU 2.80GHz 2.79 GHz
Memory (RAM): 3.00 GB
System type: 64-bit Operating System

Computer name, domain, and workgroup settings

Computer name: Computer
Full computer name: Computer
Computer description:
Workgroup: WORKGROUP

Windows activation


Windows is activated
Product ID: 89733-OEM-7373332-73331 

Figura 7 Microsoft Windows Vista 64 biți

2.2. Instalarea dispozitivului criptografic Aladdin eToken Pro

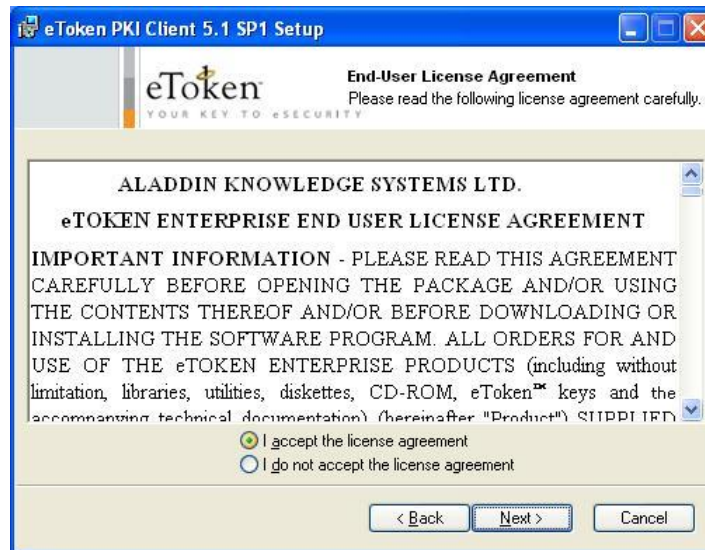
- În funcție de tipul sistemului dumneavoastră de operare: x32 biți sau x64 biți este necesară instalarea aplicației corespunzătoare: **PKIClient-x32-5.1-SP1.msi** pentru sistemul de operare pe 32 de biți, respectiv **PKIClient-x64-5.1-SP1.msi** pentru sistemul de operare pe 64 de biți.
- Accesați directorul de pe CD unde sunt localizate driverele: **<CDROM Drive>:\Aladdin**
- În funcție de sistemul dumneavoastră de operare efectuați dublu click pe **PKIClient-x32-5.1-SP1.msi** (pentru Windows XP/Windows Vista/Windows 7 pe 32 de biți) sau pe **PKIClient-x64-5.1-SP1.msi** (pentru Windows XP/Windows Vista/Windows 7 pe 64 de biți).
- În fereastra **eToken PKI Client 5.1 SP1 Setup**, efectuați click pe butonul **Next**, întocmai ca în imaginea de mai jos.



- În fereastra următoare efectuați click pe butonul **Next**.



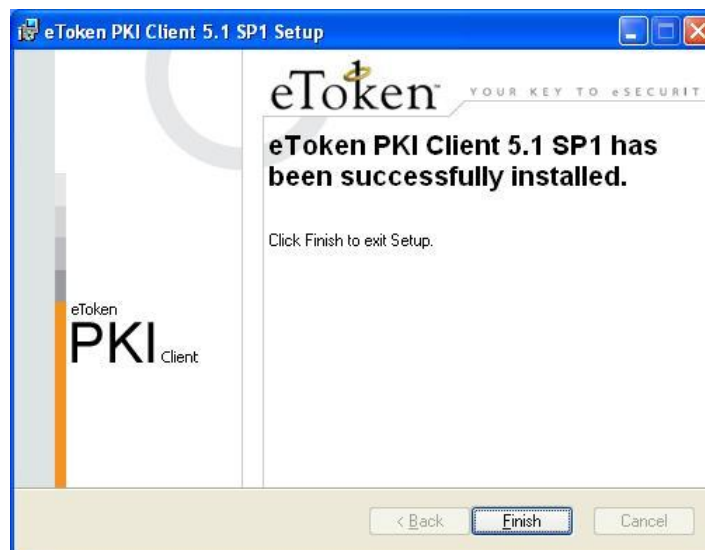
- În fereastra următoare selectați ***I accept the license agreement*** și efectuați click pe butonul **Next**.



- În fereastra următoare efectuați click pe butonul **Next**.



- În fereastra următoare finalizați instalarea efectuând click pe butonul **Finish**.

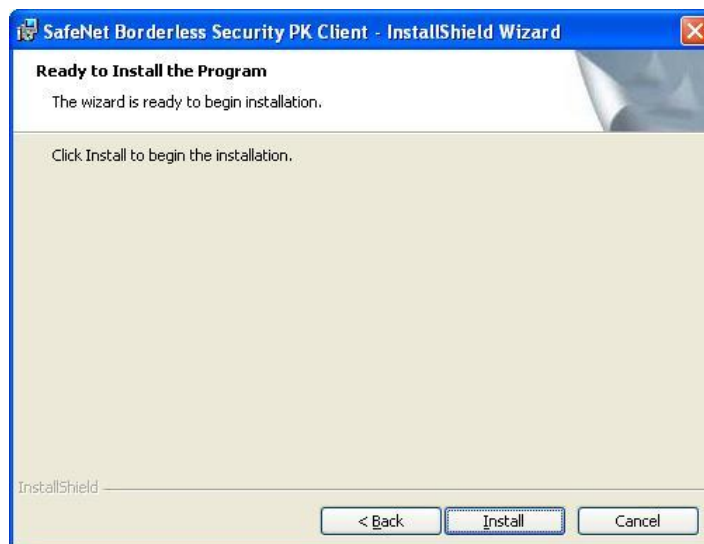


2.3. Instalarea dispozitivului criptografic SafeNet iKey 2032

- Accesați directorul de pe CD unde sunt localizate driverele: **<CDROM Drive>:\SafeNet\SafeNet72**
- Efectuați dublu click pe **Safenet72.msi**.
- În fereastra nou deschisă, **SafeNet Borderless Security PK Client** efectuați click pe butonul **Next**, întocmai ca în imaginea de mai jos.



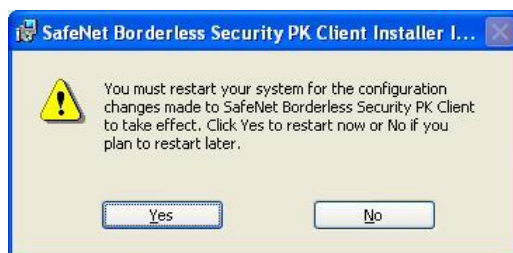
- În fereastra următoare, efectuați click pe butonul **Install**.



- În fereastra următoare finalizați instalarea efectuând click pe butonul **Finish**.



- Salvați fișierele aflate în lucru și închideți toate aplicațiile și ferestrele active, apoi efectuați click pe butonul **Yes** pentru a restarta sistemul.



2.4. Instalarea dispozitivului criptografic Oberthur

- Accesați directorul de pe CD unde sunt localizate driverele: **<CDROM Drive>:\Oberthur\driver_v.3.3.3**
- În funcție de versiunea sistemului dumneavoastră de operare accesați unul din subdirectoarele: **win2K3**, **winVISTA**, **winVISTA_x64** sau **winXP**.
- Executați dublu-click pe fișierul **Id-One Token Driver 3.3.3.msi**
- În fereastra care se deschide apăsați butonul **Next**



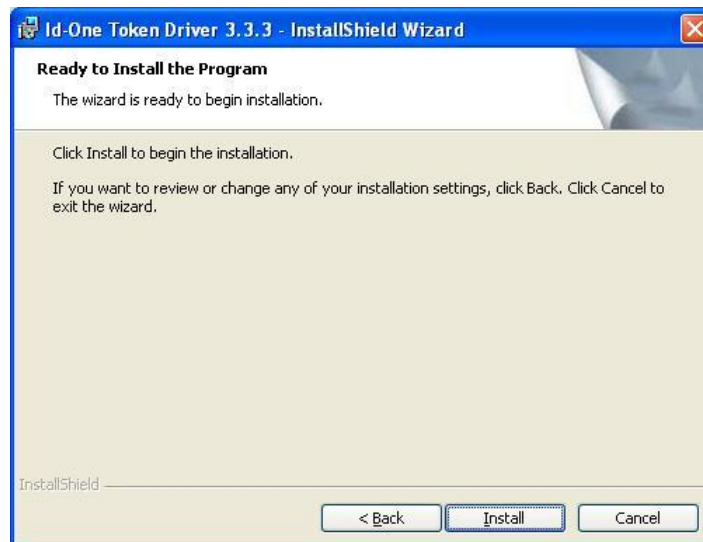
- În fereastra de mai jos selectați ***“I accept the terms in the license agreement”*** și apoi apăsați butonul **Next**



- În următoarea fereastră se afișează locația în care se va instala aplicația.
Pentru continuare apăsați butonul **Next**



- Pentru a începe instalarea executați click pe butonul **Install** în fereastra de mai jos.



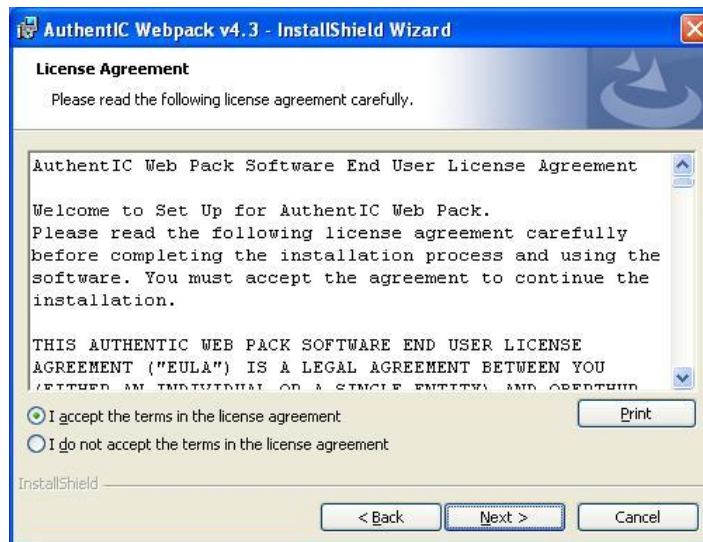
- Pentru finalizare instalării apăsați butonul **Finish**.



- În continuare vom parcurge procedura de instalare a aplicației de administrare pentru dispozitivul Oberthur. Accesați directorul de pe CD:
<CDROM Drive>:\Oberthur\AuthentIC Web Pack v4.3
- Executați dublu-click pe fișierul **AuthentIC Webpack v4.3**
- În fereastra care se deschide apăsați butonul **Next**.



- În următoarea fereastră selectați *“I accept the terms in the license agreement”* și apoi apăsați butonul **Next**.



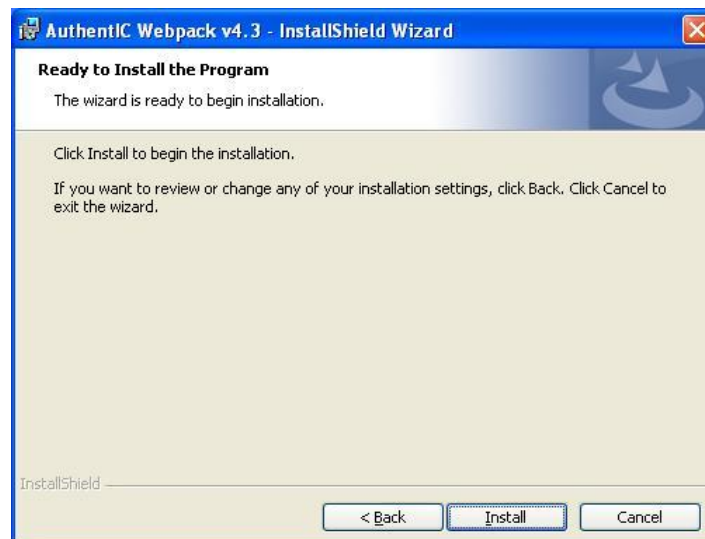
- În următoarea fereastră se afișează locația în care se va instala aplicația.
Pentru continuare apăsați butonul **Next**



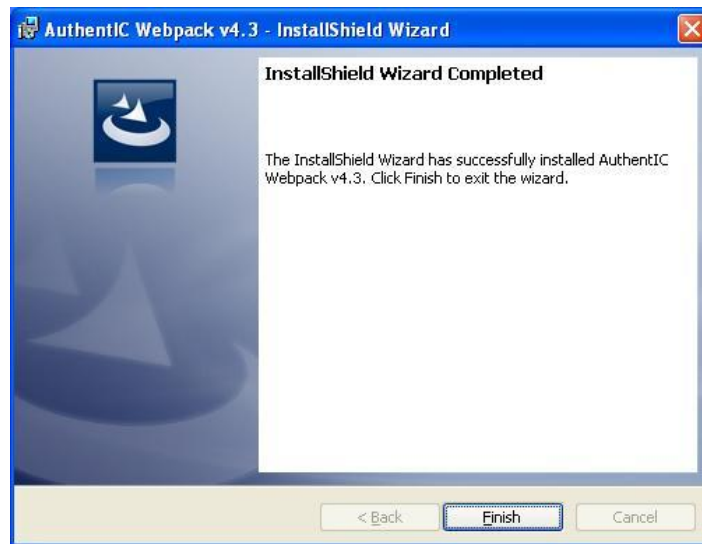
- În fereastra următoare lăsați opțiunea implicită **Complete**



- În următoarea fereastră apăsați butonul **Install** pentru a începe instalarea.



- Pentru a finaliza instalarea apăsați butonul **Finish** în următoarea fereastră.



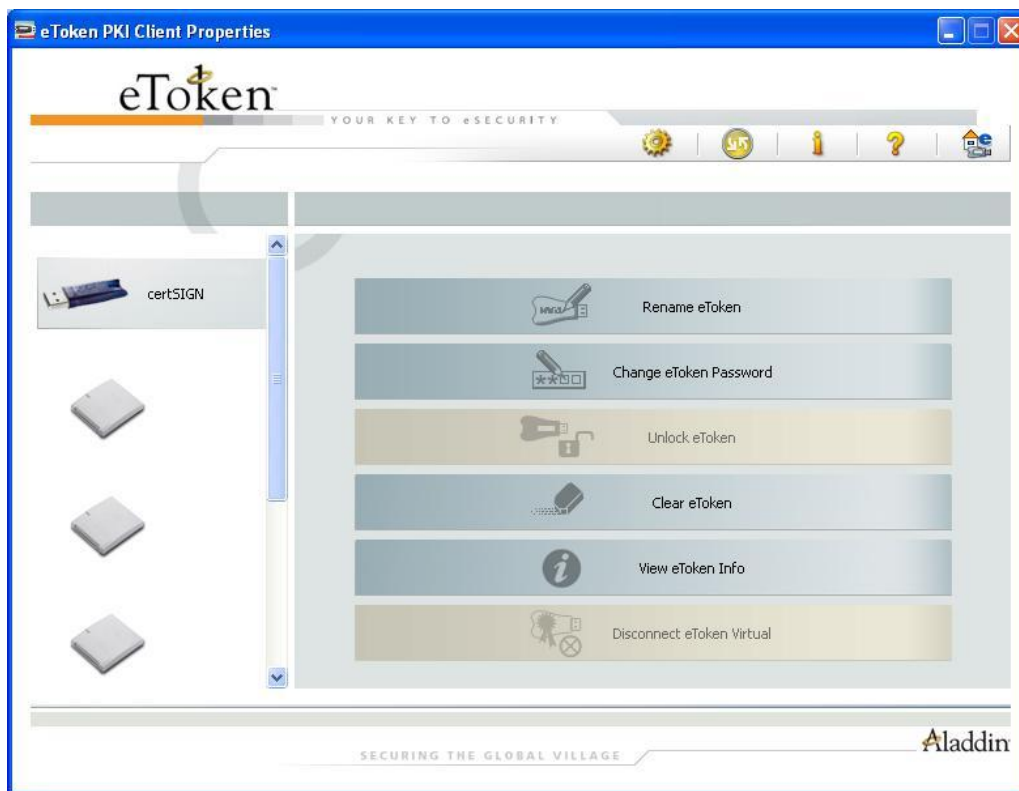
3. Accesarea dispozitivului și schimbarea codului PIN (recomandat)

Pentru a accesa dispozitivul dumneavoastră criptografic aveți nevoie de un cod PIN. Acest cod PIN este tipărit pe scrisoarea primită de la certSIGN în plic, în câmpul numit **Codul PIN aferent dispozitivului dumneavoastră criptografic**.

Se recomandă schimbarea acestui cod PIN imediat ce intrați în posesia dispozitivului.

3.1. Schimbarea codului PIN pentru dispozitivul criptografic Aladdin eToken Pro

- Conectați dispozitivul criptografic Aladdin eToken Pro la portul USB.
- Efectuați click pe **Start, All Programs, eToken, eToken PKI Client** și apoi pe **eToken Properties**.
- În fereastra **eToken PKI Client Properties** efectuați click pe butonul **Change eToken Password**.



- În fereastra **Change Password** introduceți parola curentă a dispozitivului (cea din scrisoarea primită de la certSIGN, din câmpul numit **Codul PIN aferent dispozitivului dumneavoastră criptografic**), în câmpul **Current eToken Password** și apoi introduceți noua parolă, ce trebuie să îndeplinească cerințele unei parole complexe (minim 6 caractere, litere mari și litere mici, cifre și caractere speciale) în câmpul **New eToken Password**. În câmpul **Confirm New eToken Password** introduceți din nou această nouă parolă și apoi efectuați click pe butonul **OK**.



ATENȚIE!

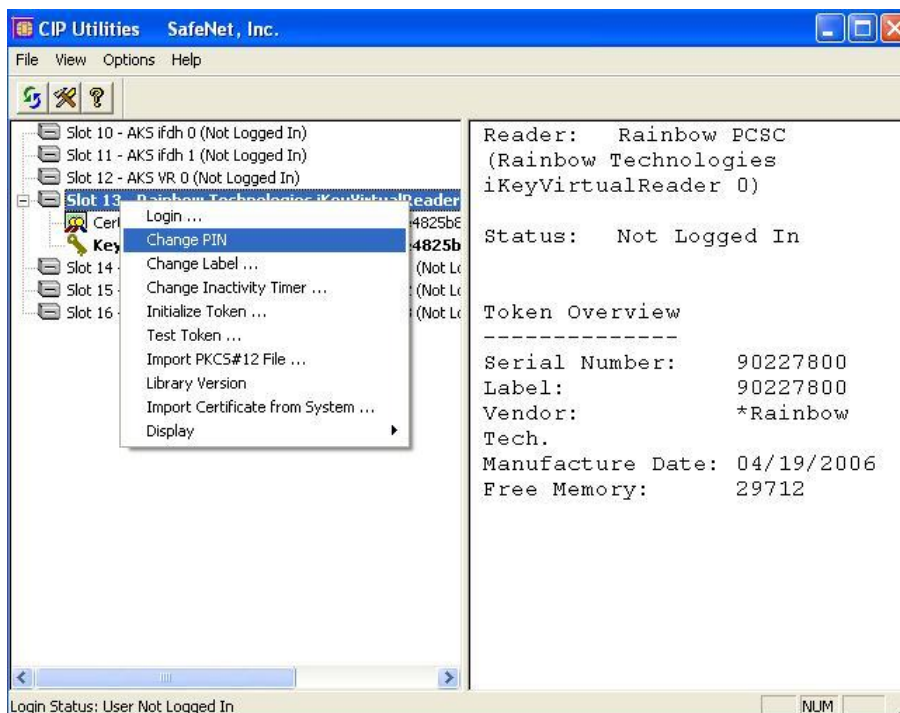
Dispozitivul criptografic dispune de un mecanism de autoblocare în cazul introducerii succesive a 15 coduri PIN-uri greșite. După blocare, informațiile din dispozitiv (cheile criptografice) nu mai pot fi utilizate. Dispozitivul nu dispune de un mecanism de deblocare și drept urmare informațiile blocate sunt irecuperabile.

- În fereastra următoare efectuați click pe butonul **OK**.



3.2.Schimbarea codului PIN pentru dispozitivul criptografic SafeNet iKey 2032

- Conectați dispozitivul criptografic SafeNet iKey 2032 la portul USB.
- Efectuați click pe **Start, All Programs, SafeNet, Borderless Security PK** și apoi pe **SafeNet CHIP Utilities**.
- În fereastra **CIP Utilities**, efectuați click dreapta pe slot-ul activ și apoi efectuați click pe butonul **Change PIN**, întocmai ca în imaginea de mai jos.



- În fereastra **Change PIN** introduceți parola curentă a dispozitivului (cea din scrisoarea primită de la certSIGN, din câmpul numit **Codul PIN aferent dispozitivului dumneavoastră criptografic**), în câmpul **Old PIN** și introduceți noua parolă, ce trebuie să întrunească cerințele unei parole complexe (minim 6 caractere, litere mari și litere mici, cifre și caractere speciale) în câmpul **New PIN**. În câmpul **Reenter New PIN** introduceți din nou această nouă parolă și apoi efectuați click pe butonul **OK**.




A dialog box titled "Change PIN" with a close button (X) in the top right corner. It contains a text field with the value "90227800". Below this are three input fields: "Old PIN" (masked with "XXXX"), "New PIN" (masked with "XXXXXX"), and "Reenter New PIN" (masked with "XXXXXX"). At the bottom are "OK" and "Cancel" buttons.

ATENȚIE!

Dispozitivul criptografic dispune de un mecanism de autoblocare în cazul introducerii succesive a 10 coduri PIN-uri greșite. După blocare, informațiile din dispozitiv (cheile criptografice) nu mai pot fi utilizate. Dispozitivul nu dispune de un mecanism de deblocare și drept urmare informațiile blocate sunt irecuperabile.

3.3.Schimbarea codului PIN pentru dispozitivul criptografic Oberthur

- Conectați dispozitivul criptografic Oberthur la portul USB.
- Accesați aplicația Authentic Manager din: **Start -> Programs -> Authentic Webpack v4 -> Authentic Manager.**
- În fereastra care se deschide introduceți codul PIN aferent dispozitivului și apăsați butonul **Log In.**



A dialog box titled "Authentic Manager" with "Information" and "Passphrase" tabs. The "Passphrase" tab is active. It contains a text field labeled "Enter Passphrase" and a "Log In" button. Below the text field is a message: "To use your keys, you must log into the smart card with your passphrase. Ensure that you type it correctly; otherwise, your smart card may be locked." On the left side, there is an image of a smart card and the "Oberthur Technologies" logo.

- După autentificarea cu succes la dispozitiv executați click pe tab-ul **Passphrase**
- În tab-ul **Passphrase** introduceți parola curentă a dispozitivului (cea din scrisoarea primită de la certSIGN, din câmpul numit **Codul PIN aferent dispozitivului dumneavoastră criptografic**), în câmpul **Current passphrase** și introduceți noua parolă, ce trebuie să întrunească cerințele unei parole complexe (minim 6 caractere, litere mari și litere mici, cifre și caractere speciale) în câmpul **New passphrase**. În câmpul **Retype new passphrase** introduceți din nou această nouă parolă și apoi efectuați click pe butonul **Change**.



- Fereastra de mai jos anunță schimbarea cu succes a PIN-ului.



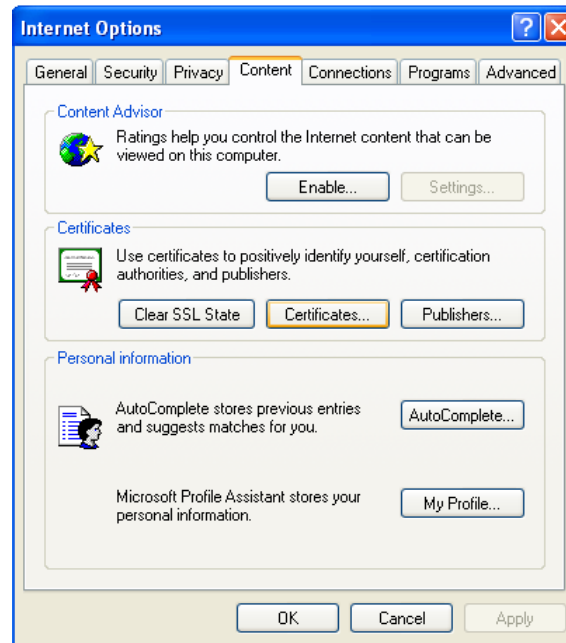
ATENȚIE!

Dispozitivul criptografic dispune de un mecanism de autoblocare în cazul introducerii succesive a 15 coduri PIN greșite. După blocare, informațiile din dispozitiv (cheile criptografice) nu mai pot fi utilizate. Dispozitivul nu dispune de un mecanism de deblocare și drept urmare informațiile blocate sunt irecuperabile.

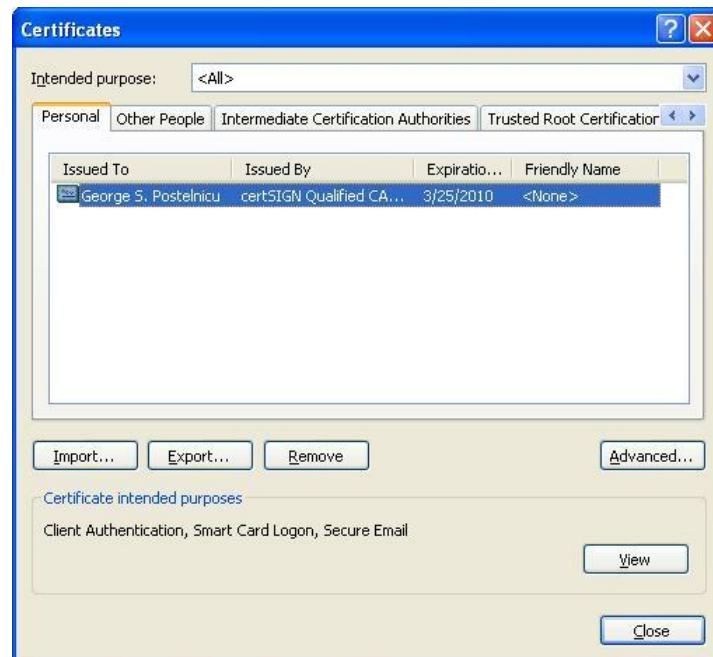
4. Instalarea certificatului în Internet Explorer (opțional)

După introducerea dispozitivului în portul USB certificatul dumneavoastră se va importa automat în sistemul de operare. Browser-ul Internet Explorer utilizează modulul criptografic și certificatele instalate în sistem fără a fi necesară importul acestora în browser. Puteți verifica acest lucru prin parcurgerea pașilor de mai jos:

- Deschideți Internet Explorer.
- Din meniul efectuați click pe **Tools** și apoi pe **Internet Options**.
- În fereastra care se deschide selectați tab-ul **Content** și apoi efectuați click pe butonul **Certificates**.



- În fereastra nou deschisă veți putea vizualiza în tab-ul **Personal** certificatul dumneavoastră importat în sistem.

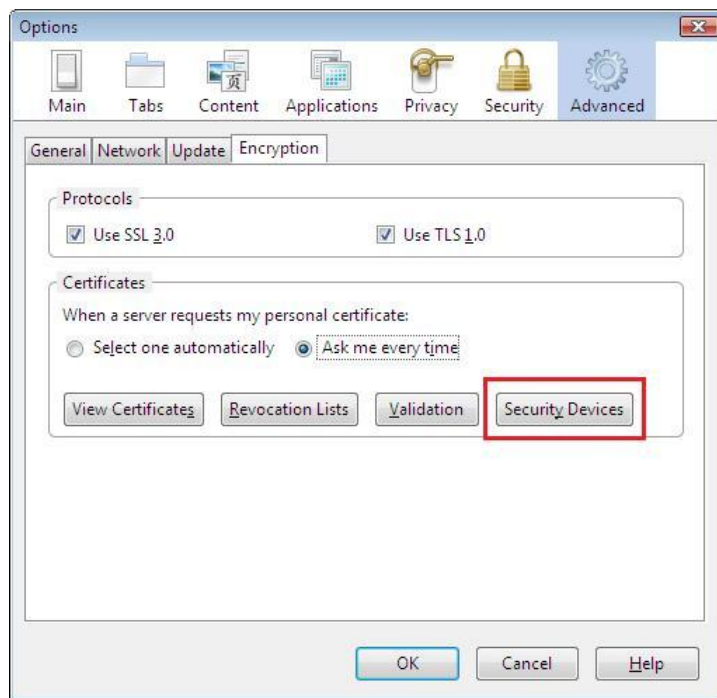


5. Instalarea modului criptografic în Mozilla Firefox (opțional)

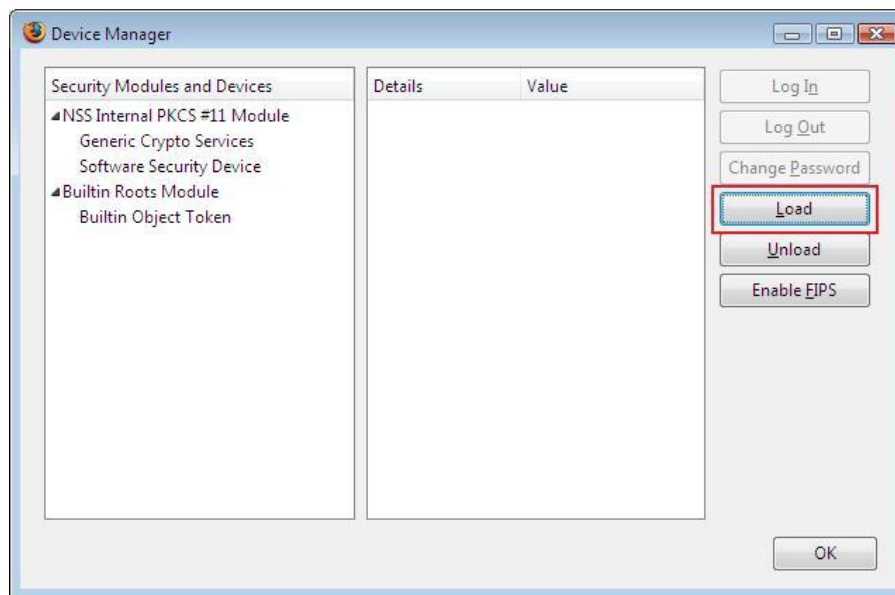
Spre deosebire de Internet Explorer care utilizează modulul instalat în sistem fără a efectua operațiunea de import a acestuia în browser, în Mozilla Firefox modulul criptografic trebuie importat manual.

Pentru a importa modulul criptografic în browser-ul Mozilla Firefox este necesară parcurgerea pașilor de mai jos:

1. Deschideți Mozilla Firefox.
2. Din meniul principal selectați: *Tools ->Options ->Advanced*. În fereastra care se deschide selectați tab-ul *Security Devices*.



3. În fereastra care se deschide veți putea încărca modulul criptografic eToken. Efectuați click pe butonul *Load*.



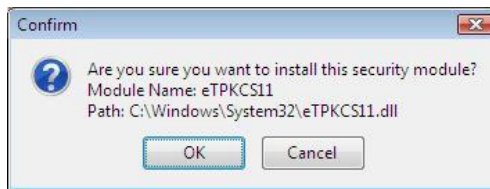
1. În fereastra care se deschide editați numele modulului: *eTPKCS11* și efectuând click pe butonul *Browse* selectați fișierul cu același nume *eTPKCS11.dll* din locația *C:\Windows\System32* și apoi efectuați click pe butonul *OK*.



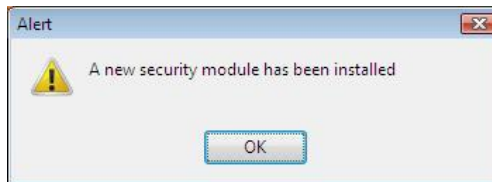
Pentru celelalte tipuri de dispozitive consultați tabelul de mai jos pentru a găsi numele fișierului PKCS11 corespunzător:

| Dispozitiv | Fișier PKCS11 |
|-------------------|-------------------------------------|
| Aladdin eToken | C:\Windows\system32\etpkcs11.dll |
| SafeNet iKey 2032 | C:\Windows\system32\dkck201.dll |
| Oberthur Cosmo64 | C:\Windows\system32\OCSCryptoki.dll |

2. În fereastra care se deschide efectuați click pe butonul *OK* pentru a confirma instalarea modulului criptografic.



3. În fereastra care se deschide efectuați click pe butonul *OK*.

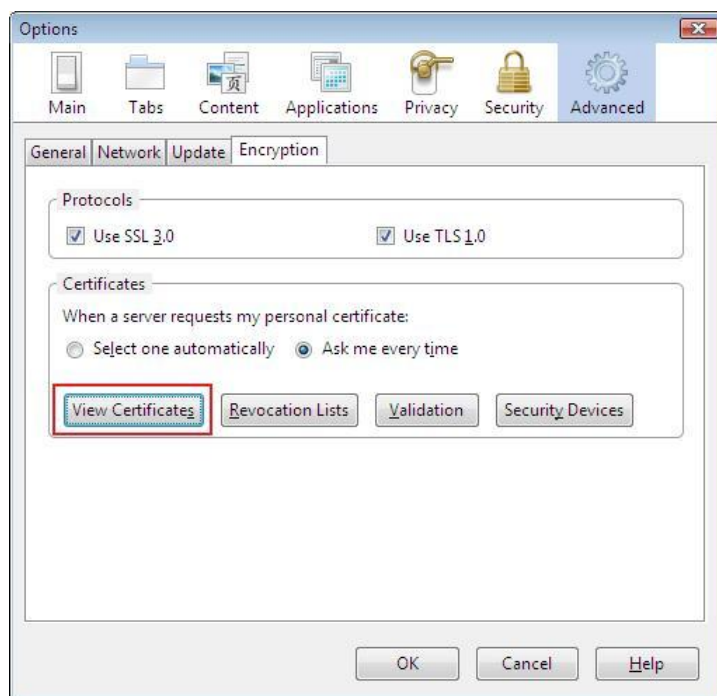


6. Instalarea certificatului în Mozilla Firefox (opțional)

După instalarea modului criptografic în Mozilla Firefox, certificatul dvs. se va importa automat în store-ul *Your Certificates* din Mozilla Firefox.

Puteți verifica acest lucru prin parcurgerea pașilor de mai jos:

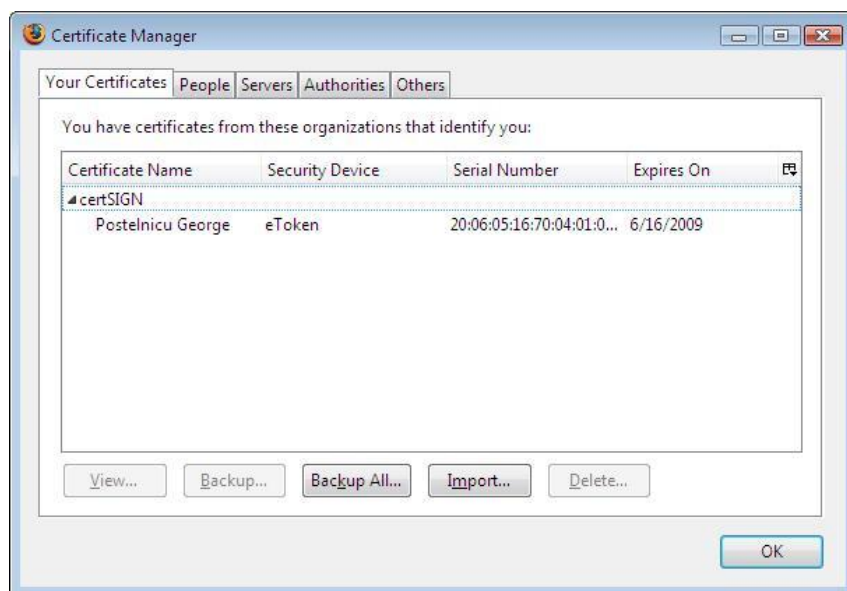
1. Deschideți Mozilla Firefox.
2. Din meniul principal selectați: *Tools -> Options -> Advanced* și efectuați click pe butonul *View Certificates*.



3. În fereastra care se deschide introduceți PIN-ul dispozitivului criptografic și apoi efectuați click pe butonul *OK*.



4. În fereastra care se deschide veți putea vizualiza în tab-ul *Your Certificates* certificatul dvs. importat în Mozilla Firefox.



Atenție! Nu ștergeți certificatul dumneavoastră din store-ul *Your Certificates* din Mozilla Firefox.

Atenție! Prin ștergerea certificatului dumneavoastră din store-ul *Your Certificates* din Mozilla Firefox, veți șterge și certificatul și cheile aferente acestuia de pe dispozitivul dumneavoastră criptografic, fapt ce va duce la imposibilitatea de a genera semnătură electronică și prin urmare va fi necesară achiziționarea unui nou certificat digital.

7. Instalarea certificatului autorității certSIGN ROOT CA în Mozilla Firefox (opțional)

Certificatul autorității certSIGN ROOT CA trebuie importat manual în browser-ul Mozilla Firefox numai pentru versiunile mai vechi de 3.6.

Pentru aceasta parcurgeți pașii de mai jos:

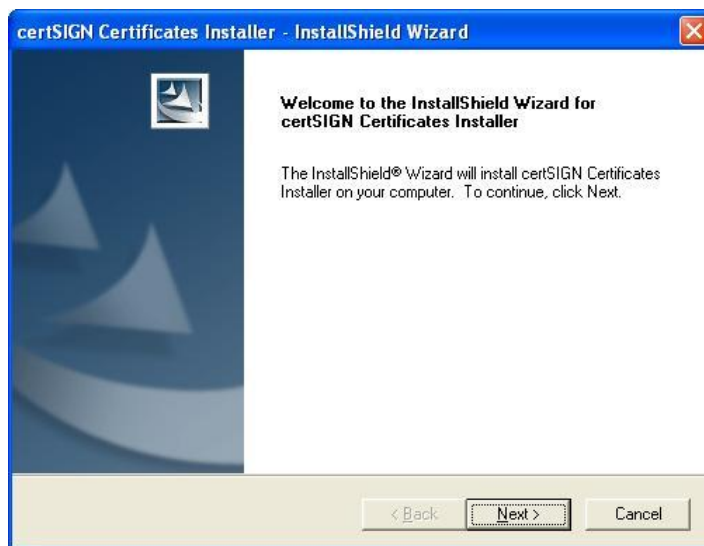
1. Deschideți Mozilla Firefox.
2. Accesați link-ul <http://www.certsign.ro/certcrl/root.crt>
3. În fereastra care se deschide bifați cele trei check-box-uri (trust this CA to identify websites, Trust this CA to identify email users, Trust this CA to identify software developers) și apoi efectuați click pe butonul *OK*.



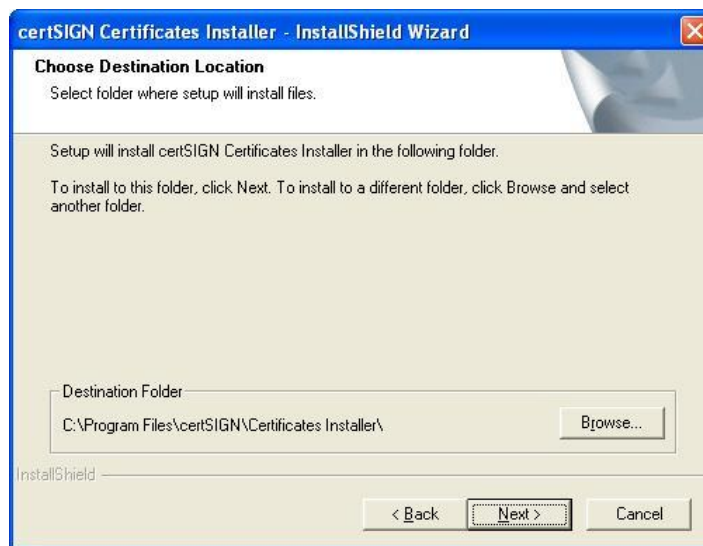
8. Instalarea lanțului de încredere certSIGN (recomandat)

Certificatul dumneavoastră face parte dintr-un lanț de încredere compus din autorități de certificare certSIGN. Pentru a instala certificatele autorităților de certificare certSIGN parcurgeți pașii de mai jos:

- Accesați directorul de pe CD-ul certSIGN unde sunt localizate certificatele:
<CDROM Drive>:\Certificates
- În directorul **Certificates** efectuați dublu click pe **certSIGN Certificates Installer.exe**.
- În fereastra următoare efectuați click pe butonul **Next**, întocmai ca în imaginea de mai jos.



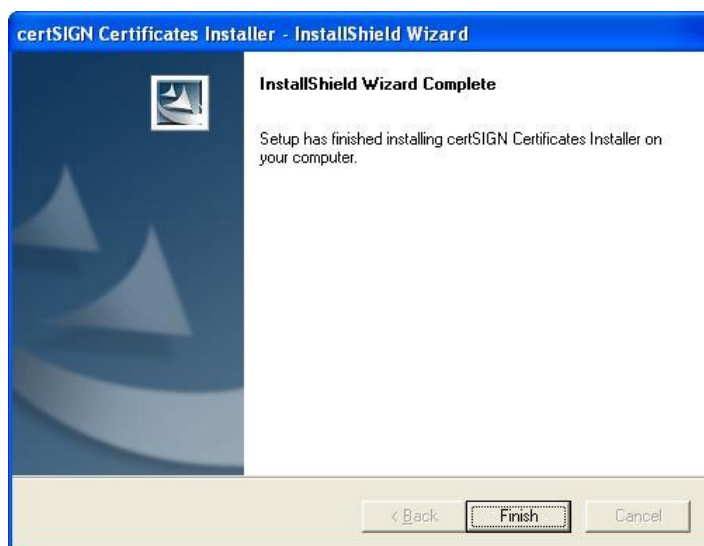
- În fereastra nou apărută, efectuați click pe butonul **Next**.



- În fereastra următoare vă asigurați că opțiunile: **Install Certificates in System Store** și **Install Certificates in User Store** sunt bifate și apoi efectuați click pe butonul **Next**, întocmai ca în imaginea de mai jos.



- În fereastra următoare finalizați instalarea efectuând click pe butonul **Finish**.



9. Utilizarea certificatului digital (obligatoriu)

Dispozitivul ce conține certificatul dumneavoastră calificat are un PIN ce protejează accesul neautorizat la informațiile stocate pe dispozitiv. Pentru a utiliza certificatul trebuie să instalați o aplicație software proiectată în acest scop, de exemplu clickSIGN clickSIGNPDF sau shellSAFE. Înaintea utilizării informațiilor stocate pe dispozitiv va trebui să vă autentificați introducând PIN-ul corect.

Puteți semna electronic folosind aplicația Adobe Reader și formulare pdf ce conțin câmpuri de semnătură (un exemplu de astfel de formulare îl reprezintă declarațiile fiscale puse la dispoziția contribuabililor de către ANAF).

Dacă ați achiziționat și aplicația clickSIGN urmați și procedura de instalare din secțiunea 10 a acestui ghid.

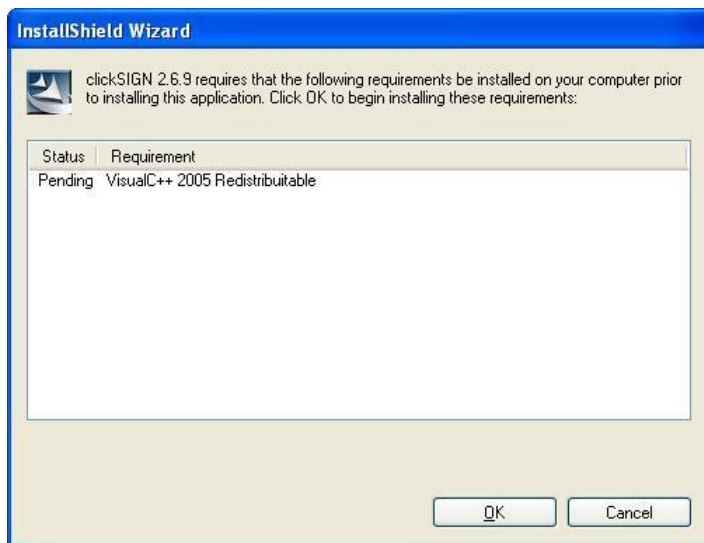
10. Instalarea aplicației clickSIGN (obligatoriu)

Dacă ați achiziționat și aplicația clickSIGN urmați și procedura de instalare de mai jos.

clickSIGN este o aplicație pentru semnarea electronică și marcarea temporală a documentelor conform standardului PKCS#7. Pentru a instala aplicația clickSIGN parcurgeți pașii de mai jos:

- Accesați directorul de pe CD-ul certSIGN unde este localizată aplicația clickSIGN: **<CDROM Drive>:\clickSIGN 2.6.9.326**
- Executați dublu-click pe **setup.exe**.

În fereastra care se deschide veți fi notificat de instalarea **VisualC++ Redistributable**. Apăsați butonul **OK** pentru continuare. Dacă aveți deja instalată această componentă, fereastra următoare nu va apărea.



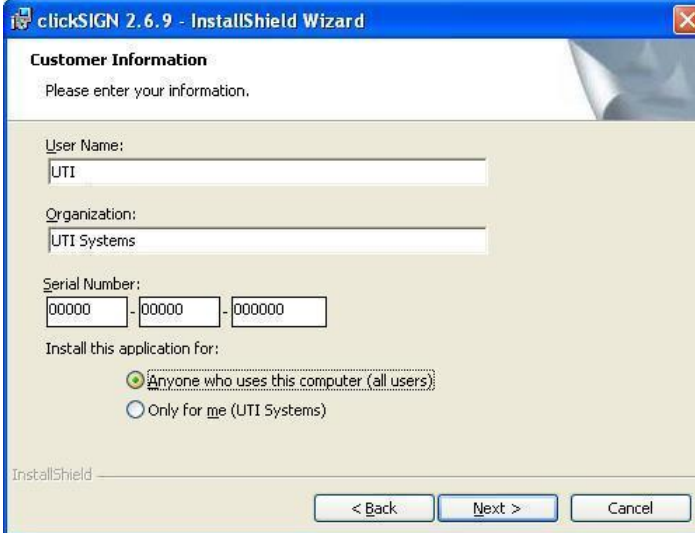
- În fereastra următoare apăsați butonul **Next**.



- În pasul următor selectați opțiunea ***“I accept the terms in the license agreement”*** pentru a confirma că sunteți de acord cu condițiile de licențiere a aplicației clickSIGN și pentru a putea continua.



- În următoarea fereastră introduceți **User Name** și **Serial Number** corespunzătoare licenței clickSIGN. Pentru continuare apăsați butonul **Next**.




The screenshot shows the 'clickSIGN 2.6.9 - InstallShield Wizard' window. The title bar reads 'clickSIGN 2.6.9 - InstallShield Wizard'. The main content area is titled 'Customer Information' and contains the following fields and options:

- 'Please enter your information.'
- 'User Name:' field with the text 'UTI' entered.
- 'Organization:' field with the text 'UTI Systems' entered.
- 'Serial Number:' field with three sub-fields containing '00000', '000000', and '000000' respectively.
- 'Install this application for:' section with two radio buttons:
 - 'Anyone who uses this computer (all users):'
 - 'Only for me (UTI Systems)'

At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted.

- Pentru a începe instalarea apăsați butonul **Install** în fereastra nou deschisă.



The screenshot shows the 'clickSIGN 2.6.9 - InstallShield Wizard' window. The title bar reads 'clickSIGN 2.6.9 - InstallShield Wizard'. The main content area is titled 'Ready to Install the Program' and contains the following text:

- 'The wizard is ready to begin installation.'
- 'Click Install to begin the installation.'
- 'If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.'

At the bottom of the window, there are three buttons: '< Back', 'Install', and 'Cancel'. The 'Install' button is highlighted.

- Fereastra de mai jos confirmă finalizarea procesului de instalare a aplicației clickSIGN. Apăsați butonul **Finish** pentru a încheia instalarea.



- Pentru detalii legate de modul de utilizare al aplicației clickSIGN consultați Manualul de utilizare. Acest manual poate fi accesat din locația:
Start -> All Programs -> UTI Systems -> clickSIGN -> clickSIGN Help (RO) – pentru versiunea în limba română.
sau
Start -> All Programs -> UTI Systems -> clickSIGN -> clickSIGN Help (EN) – pentru versiunea în limba engleză.

ATENȚIE!

- **REȚINEȚI CODUL PIN AL TOKEN-ULUI**, întrucât introducerea consecutivă a 15 PIN-uri incorecte în cazul dispozitivelor eToken Pro și Oberthur Cosmo64, respectiv a 10 PIN-uri incorecte în cazul dispozitivului SafeNet iKey 2032, are ca rezultat blocarea dispozitivului, fapt ce va duce la imposibilitatea de a genera semnătură electronică și prin urmare va fi necesară achiziționarea unui nou certificat digital.
- **NU FORMATAȚI/INIȚIALIZAȚI** dispozitivul criptografic întrucât această operațiune are ca rezultat ștergerea materialului criptografic (certificat și chei) de pe token, fapt ce va duce la imposibilitatea de a genera semnătură electronică și prin urmare va fi necesară achiziționarea unui nou certificat digital.
- **NU ȘTERGEȚI OBIECTE DE PE TOKEN**, întrucât această operațiune are ca rezultat ștergerea certificatului sau a cheilor de pe token, fapt ce va duce la imposibilitatea de a genera semnătură electronică și prin urmare va fi necesară achiziționarea unui nou certificat digital.

11. Definiții și acronime

- ✓ **Dispozitiv criptografic** - este un dispozitiv cu o structură specială în care sunt înglobați algoritmi criptografici (simetrici și asimetrici) ce permit realizarea în siguranță a operațiilor criptografice. Acesta poate fi de tip smartcard sau token USB și conține un cip criptografic care permite generarea de chei și implementarea algoritmilor criptografici.
- ✓ **Chei** - O cheie este o bucată de informație care controlează operația unui algoritm criptografic. Ele sunt private sau publice. Scopul cheii private este decriptarea sau crearea de semnătură electronică pentru uzul exclusiv al proprietarului. De asemenea, reprezintă acea cheie dintr-o pereche de chei care este cunoscută numai proprietarului. În schimb, cheia publică poate fi cunoscută de toată lumea și definește transformarea de verificare a semnăturii sau de criptare a mesajelor.
- ✓ **Driver** - Un driver este un software care permite computerului să comunice cu un element hardware sau cu un dispozitiv în vederea unei bune funcționări a acestuia.
- ✓ **Cod PIN** – Este o parolă formată din mai multe caractere (litere, cifre, semne de punctuație, caractere speciale) cunoscută numai de persoana pe numele căreia se emite certificatul digital și care se folosește pentru a avea acces la token-ul USB pe care este stocat respectivul certificat. Codul PIN se deosebește de **parola de administrare (sau de management)** a certificatului, care se utilizează în cazul reînnoirii sau revocării acestuia.

- ✓ **Calea de certificare** – este calea ordonată a certificatelor, pornind de la un certificat considerat punct de încredere (ales de verificator) până la certificatul de verificat.

- ✓ **Autoritatea de certificare** - reprezintă un sistem complex care este alcătuit din aplicații software, hardware, precum și proceduri și reguli de securitate. Toate acestea au rolul de a asigura emiterea și gestiunea în cele mai bune condiții de securitate a certificatelor digitale.

- ✓ **Lanțul de încredere** - o secvență ordonată de certificate, în care un certificat digital asigură autenticitatea certificatului anterior.