Instructions for installing and using the qualified digital certificate issued by DigiSign

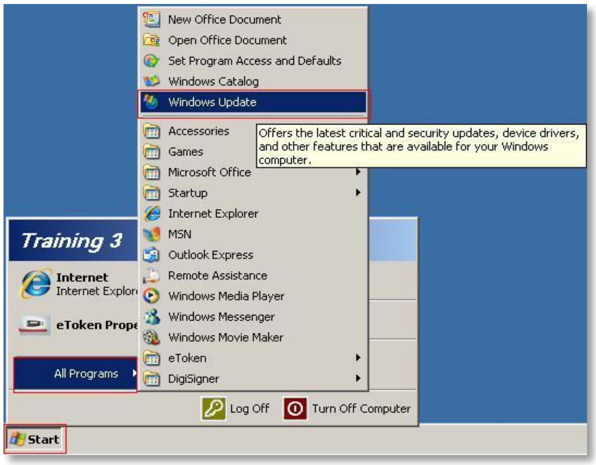
Version 1.3

In order to use the digital certificate properly, please follow the instructions presented in this document. Failure to follow these specifications and the use of other applications than those specified in this document may cause a delay in successfully using the digital certificate or even its loss.

An example of the install process on a Windows XP system will be presented in the following pages. Pictures can differ if other versions of Windows are used but the steps are the same.

Attention: If you renewed your qualified digital certificate and the applications are already installed on your computer, please reinstall the trust chain from point **2.1** (page 2), then continue with the procedure from point **3** (page 12).

1. Please make sure that your operating system is up-to-date and you don't have any firewall/antivirus application that might block the proper installation of the USB Aladdin e-Token PRO device.



Offers the latest critical and security updates, device drivers, and other features that are available for your Windows computer.

Use the **Windows Update** function or follow the instructions on the Microsoft website in order to install the latest updates available for your operating system and for the Internet Explorer browser.

Make sure that:

- **You are logged in as the administrator of the system on which you want to install the digital certificate;**
- **The clock, date and time zone settings of the system are properly set;**
- **The eToken device is NOT connected into the USB port during the installation process of the applications.**

2. The installation process of the applications needed in order to use the e-Token USB device and the qualified digital certificate.

For the proper use of the Aladdin eToken cryptographic USB device which contains the qualified digital certificate issued by DigiSign (used for creating the extended digital signature), you will have to install the DigiSign trust chain and the Aladdin eToken software.

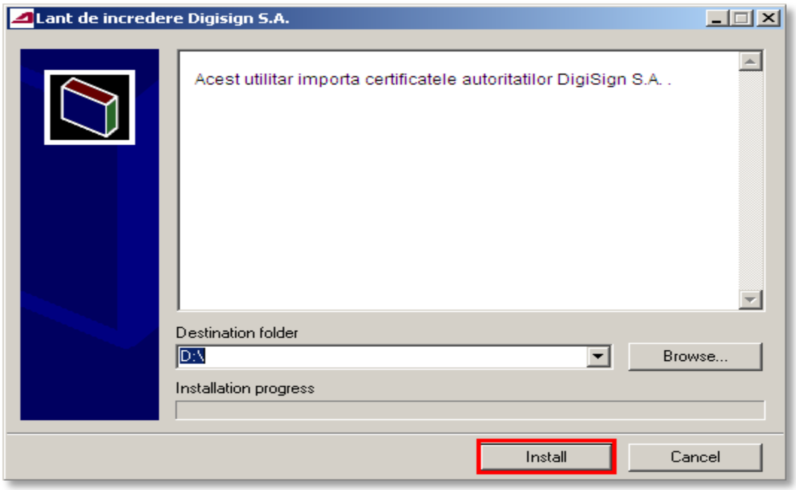
2.1 Installing the chain trust and the Aladdin e-Token software

2.1.1 Installing the DigiSign trust chain

a) Download the trust chain from the following link: http://www.digisign.ro/uploads/cert.zip

b) Open the archive you just downloaded, unzip the *cert.exe* file and open it by double-clicking the executable or, in case you are using **Windows Vista or Windows 7**, open it by right-clicking on the file and selecting the „*Run as Administrator*" option.

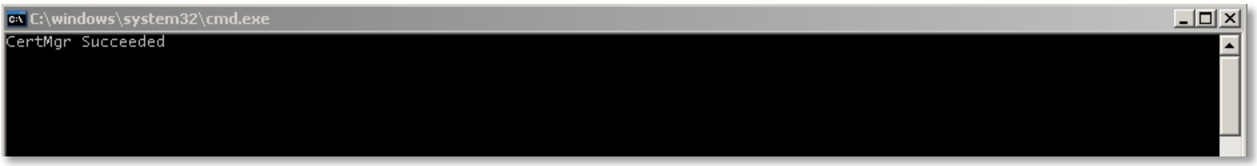
c) Choose the Install button.



Acest utilitar importa certificatele autoritatilor DigiSign S.A. .

IMPORTANT : Please make sure that the trust chain was successfully installed!

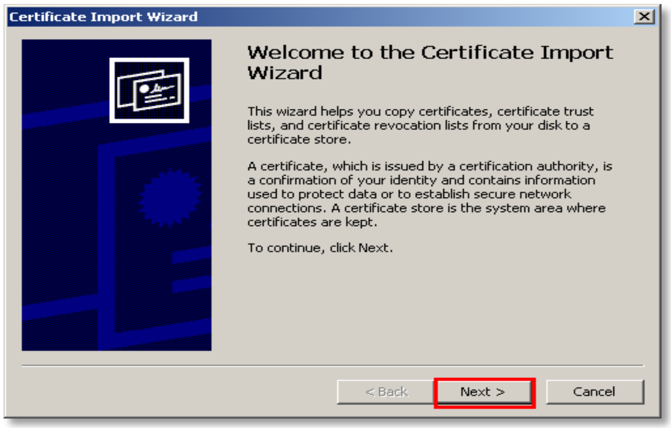
In a similar window like the one below, the *„CertMgr Succeeded"* mesage will be shown if the chain trust was successfully installed:



```
CertMgr Succeeded
```

If you receive the CertMgr Failed mesage, you will have to right-click the *cert.exe* file and select the *„Run as Administrator"* option (!) .

d) Choose the Next button.



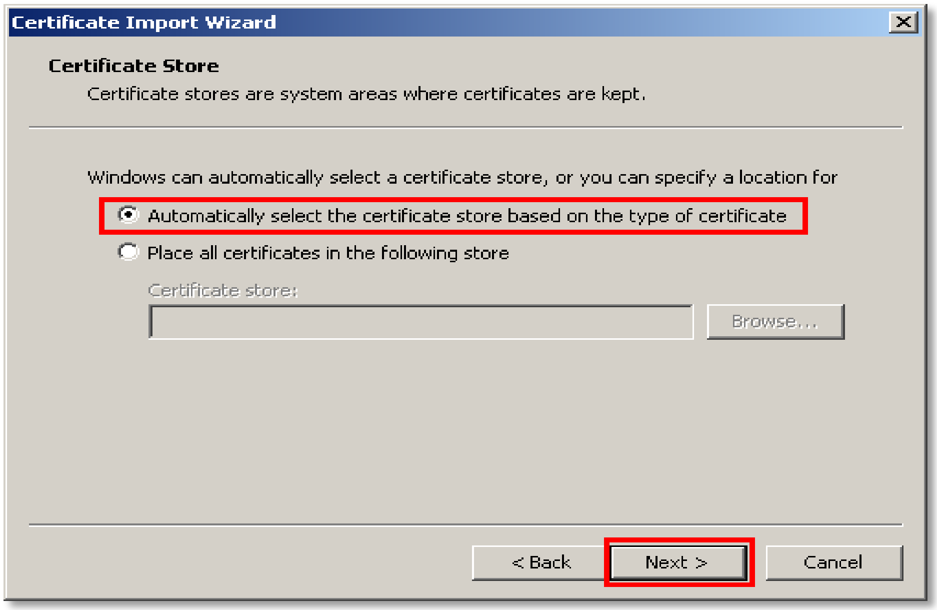
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

e) Leave the •Automatically... button checked and then click Next >



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

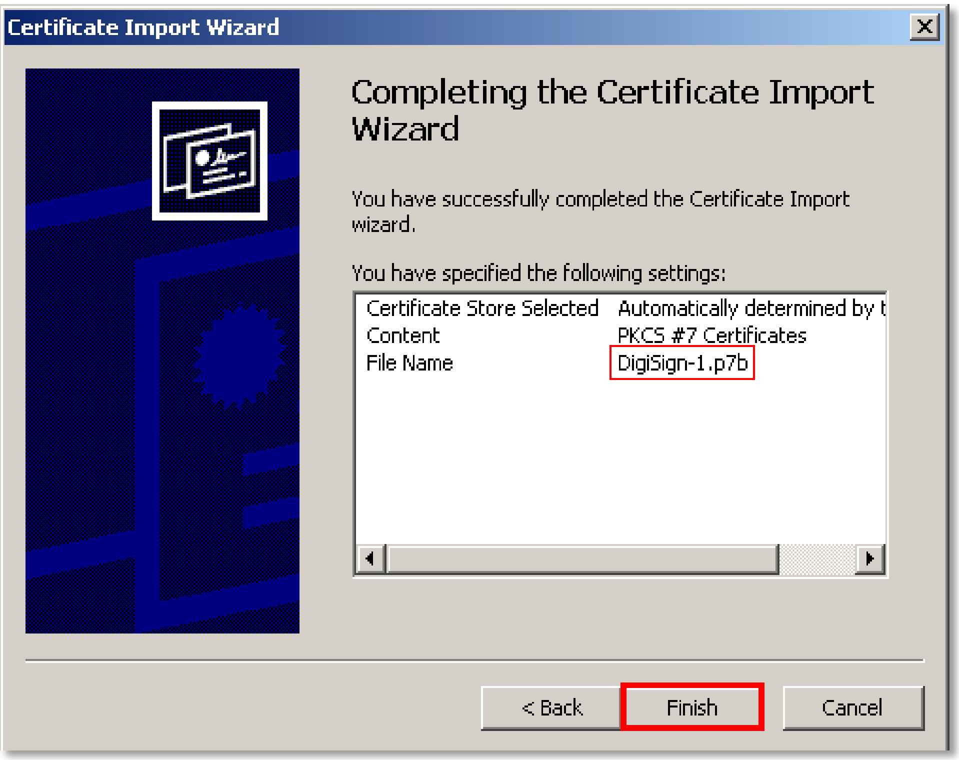
Windows can automatically select a certificate store, or you can specify a location for

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

f) Click Finish



Certificate Import Wizard

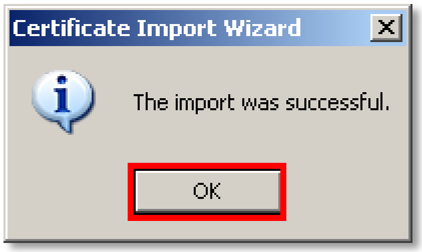
Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PKCS #7 Certificates
File Name	DigiSign-1.p7b

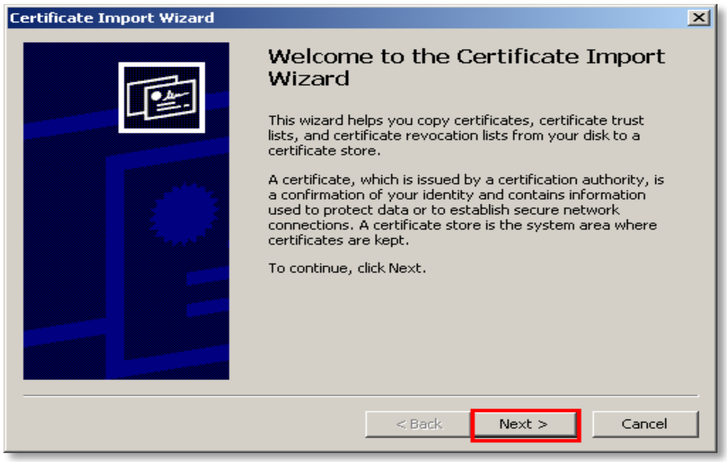
g) Click OK



Certificate Import Wizard

The import was successful.

h) Choose the Next button



Certificate Import Wizard

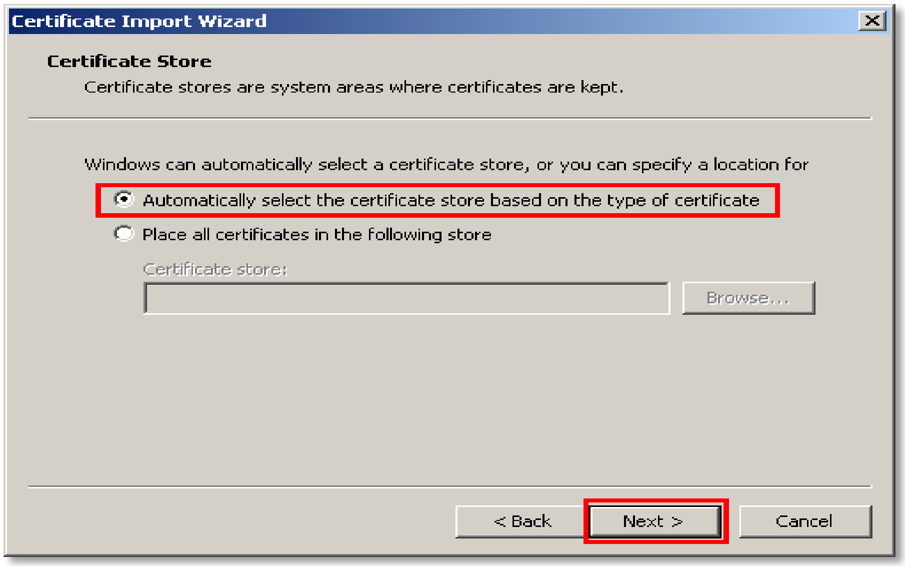
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

i) Leave the ●Automatically... button checked and then click Next >



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

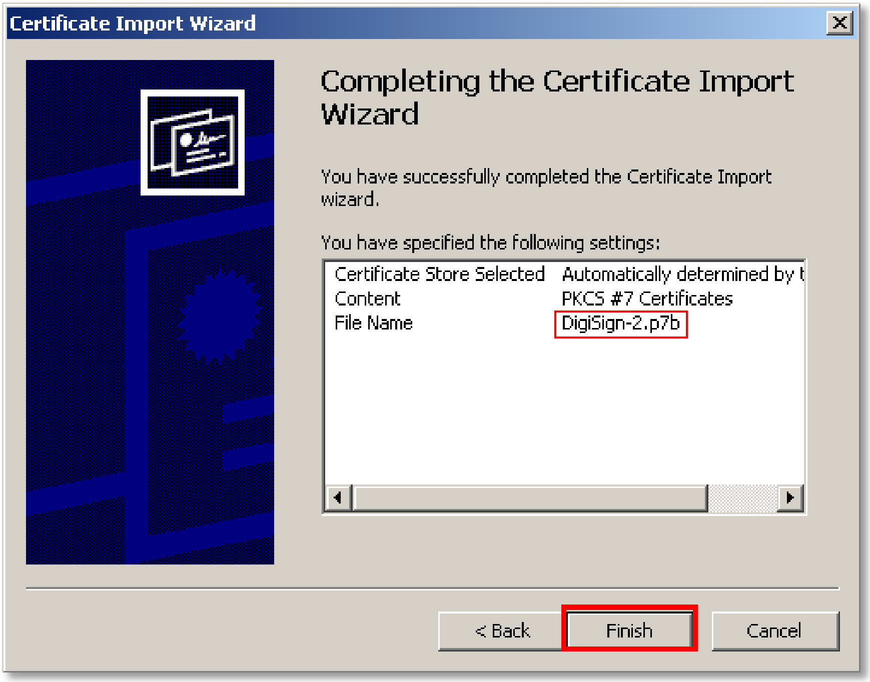
Windows can automatically select a certificate store, or you can specify a location for

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

j) Click Finish



Certificate Import Wizard

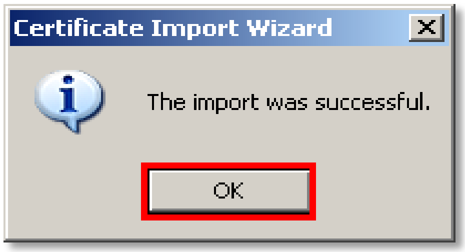
Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PKCS #7 Certificates
File Name	DigiSign-2.p7b

k) Click the OK button



Certificate Import Wizard

The import was successful.

2.2 Installing the Aladdin e-Token PRO software

Please choose the following driver depending on the version of the operating system used:
Compatibility: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10 , Windows Server 2003, Windows Server 2008 :

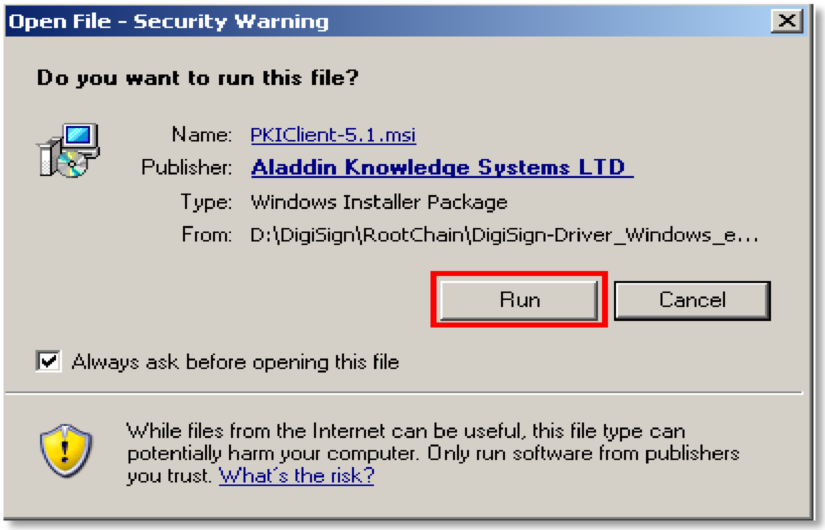
a. 32 bit : http://www.digisign.ro/uploads/PKIClient-5.1.msi
b. 64 bit : http://www.digisign.ro/uploads/PKIClient-5.1_X64.msi

Make sure that the USB e-Token device is not connected to the computer!

a) Double-click the downloaded application (***PKIClient-5.1.msi*** for the 32-bit operating systems or ***PKIClient-5.1_x64.msi*** for the 64-bit operating systems)

ATENTION: If the operating system is **Windows Vista** or **Windows 7**, you will have to right-click the file and select the *„Run as Administrator”* option !

b) Choose the Run button


Open File - Security Warning

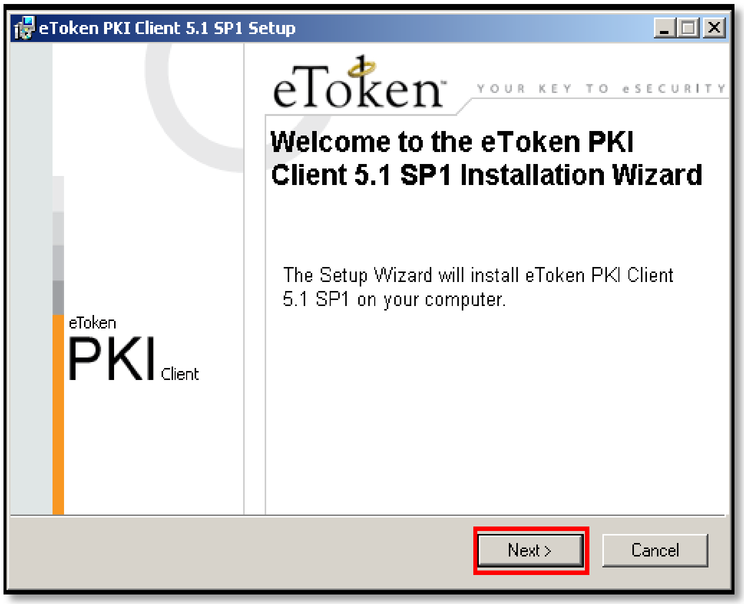
Do you want to run this file?

Name: PKIClient-5.1.msi
Publisher: Aladdin Knowledge Systems LTD
Type: Windows Installer Package
From: D:\DigiSign\RootChain\DigiSign-Driver_Windows_e...

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

c) Choose the Next button

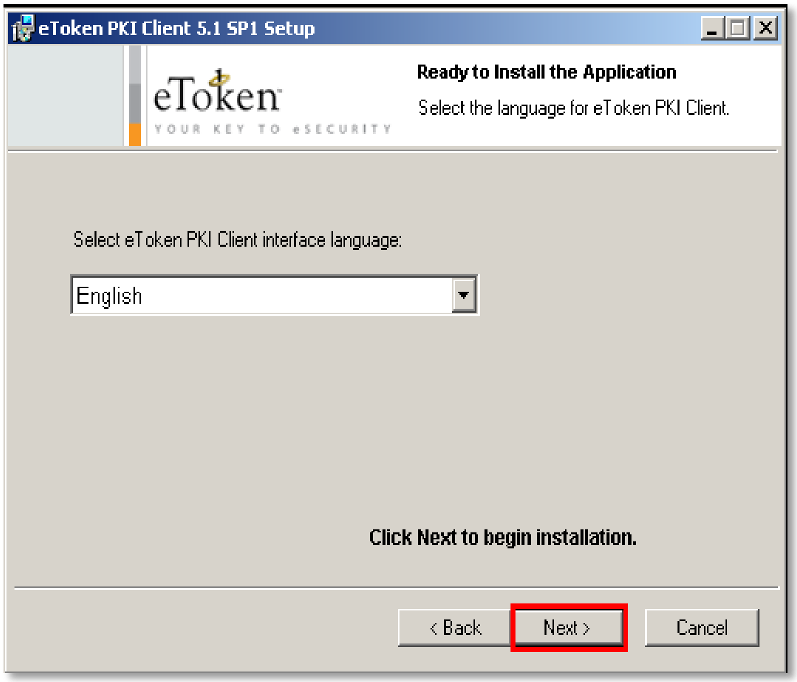


eToken PKI Client 5.1 SP1 Setup

Welcome to the eToken PKI Client 5.1 SP1 Installation Wizard

The Setup Wizard will install eToken PKI Client 5.1 SP1 on your computer.

d) Click Next



eToken PKI Client 5.1 SP1 Setup

Ready to Install the Application

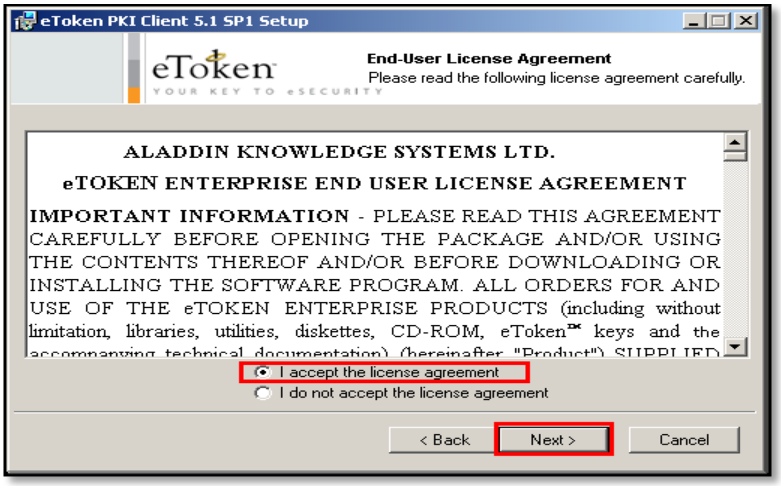
Select the language for eToken PKI Client.

Select eToken PKI Client interface language:

English

Click Next to begin installation.

e) Check the ●I accept the license agreement option and click Next



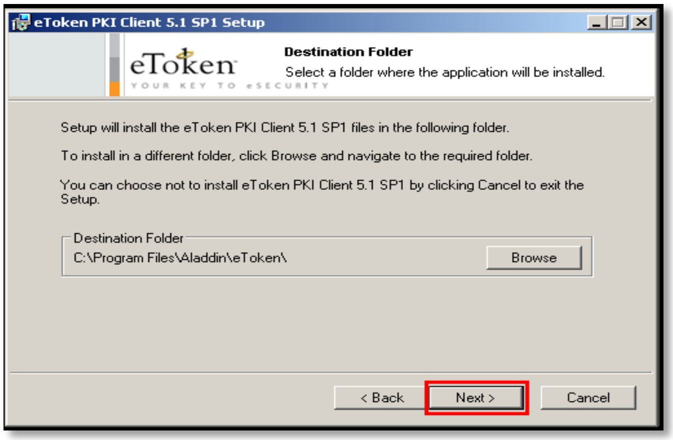
End-User License Agreement
Please read the following license agreement carefully.

ALADDIN KNOWLEDGE SYSTEMS LTD.
eTOKEN ENTERPRISE END USER LICENSE AGREEMENT

IMPORTANT INFORMATION - PLEASE READ THIS AGREEMENT CAREFULLY BEFORE OPENING THE PACKAGE AND/OR USING THE CONTENTS THEREOF AND/OR BEFORE DOWNLOADING OR INSTALLING THE SOFTWARE PROGRAM. ALL ORDERS FOR AND USE OF THE eTOKEN ENTERPRISE PRODUCTS (including without limitation, libraries, utilities, diskettes, CD-ROM, eToken™ keys and the accompanying technical documentation) (hereinafter "Product") SUPPLIED

● I accept the license agreement
○ I do not accept the license agreement

f) Choose the Next button



Destination Folder
Select a folder where the application will be installed.

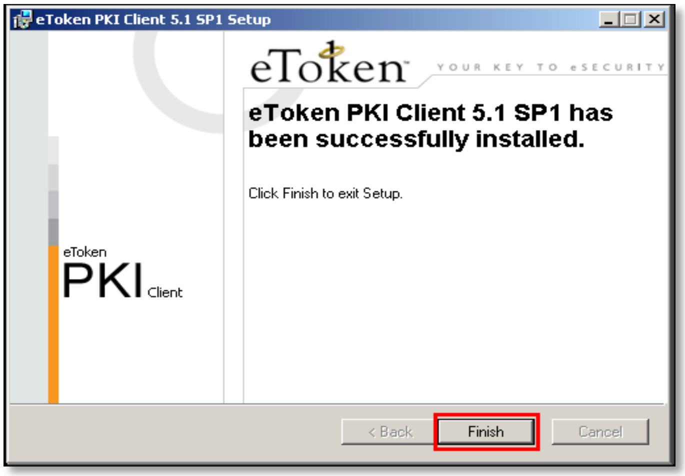
Setup will install the eToken PKI Client 5.1 SP1 files in the following folder.

To install in a different folder, click Browse and navigate to the required folder.

You can choose not to install eToken PKI Client 5.1 SP1 by clicking Cancel to exit the Setup.

Destination Folder
C:\Program Files\Aladdin\eToken\

g) Click Finish



eToken PKI Client 5.1 SP1 has been successfully installed.

Click Finish to exit Setup.

2.3 Verificarea instalării lanțului de încredere

Choose **one** of the options below in order to verify that the DigiSign chain trust was successfully installed. If you notice that one of the following certificates are missing from the application, you will have to repeat the trust chain installation process presented at point 2.1 (page 2) of this document.

2.3.1 Using the Internet Explorer browser

O

R

- Open the *Internet Explorer* browser. From the *Tools* menu, select → *Internet Options* → *Content* → *Certificates* → *Intermediate Certification Authorities* .

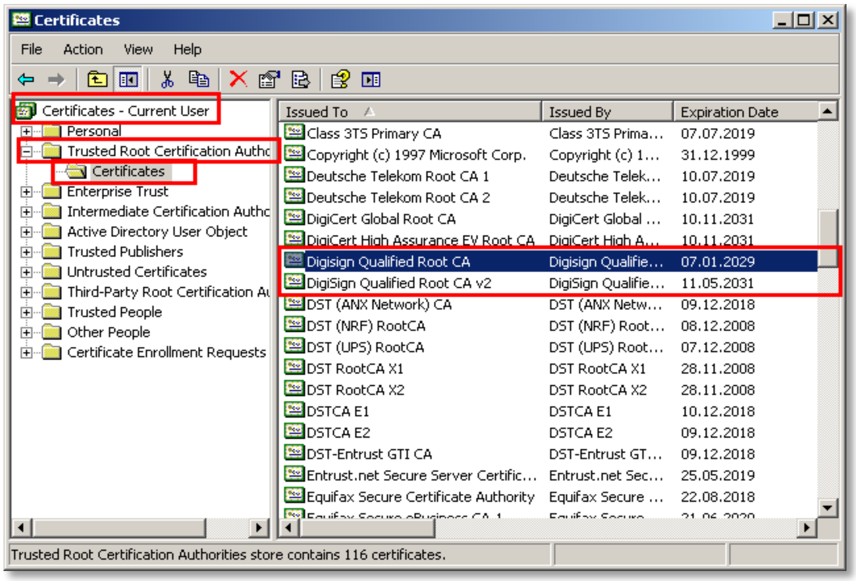
  In that list you should find the following certificates: *DIGISIGN FOR UNNPR*, *DIGISIGN PUBLIC* and *DigiSign Qualified Public CA* if the trust chain installation was properly made.

- Open the *Internet Explorer* browser. From the *Tools* menu, select → *Internet Options* → *Content* → *Certificates* → *Trusted Root Certification Authorities* .
  In that list you should find the following certificates: *DigiSign Qualified Root CA* si *DigiSign Qualified Root CA v2* if the trust chain installation was properly made.

2.3.2 Using the Certificate Manager tool

From the *Windows Start* menu, choose the *Run* option. Type *certmgr.msc* and then click *OK.*

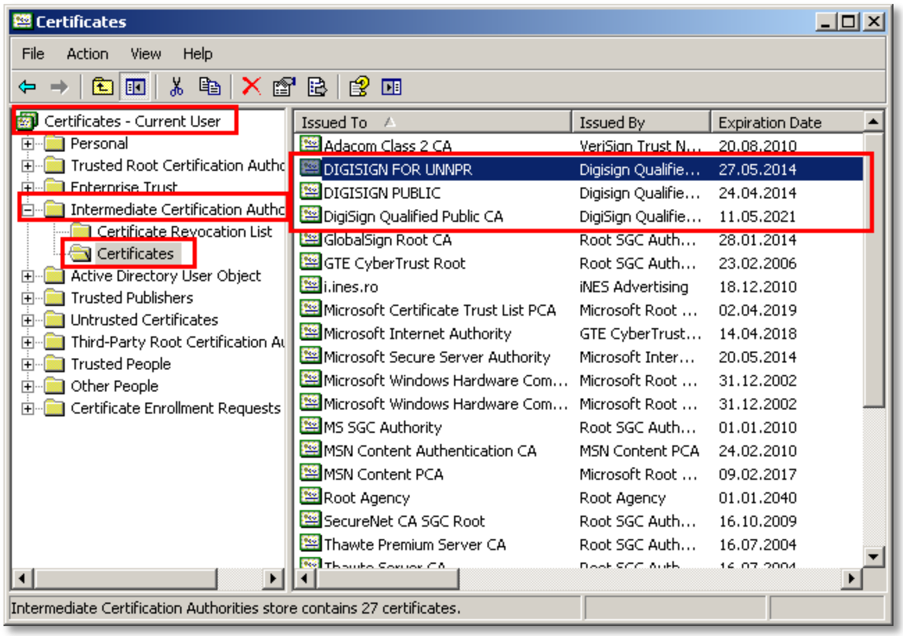
- Select *Certificates - Current User* → *Trusted Root Certification Authorities* → *Certificates* . In the right panel you should be able to find the 2 certificates named: *DigiSign Qualified Root CA* and *DigiSign Qualified Root CA v2* if the trust chain installation was properly made.


Certificates
File
Action
View
Help
Certificates - Current User
Personal
Trusted Root Certification Authc
Certificates
Enterprise Trust
Intermediate Certification Authc
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Au
Trusted People
Other People
Certificate Enrollment Requests

Issued To	Issued By	Expiration Date
Class 3TS Primary CA	Class 3TS Prima...	07.07.2019
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1...	31.12.1999
Deutsche Telekom Root CA 1	Deutsche Telek...	10.07.2019
Deutsche Telekom Root CA 2	Deutsche Telek...	10.07.2019
DigiCert Global Root CA	DigiCert Global ...	10.11.2031
DigiCert High Assurance EV Root CA	DigiCert High A...	10.11.2031
Digisign Qualified Root CA	Digisign Qualifie...	07.01.2029
DigiSign Qualified Root CA v2	DigiSign Qualifie...	11.05.2031
DST (ANX Network) CA	DST (ANX Netw...	09.12.2018
DST (NRF) RootCA	DST (NRF) Root...	08.12.2008
DST (UPS) RootCA	DST (UPS) Root...	07.12.2008
DST RootCA X1	DST RootCA X1	28.11.2008
DST RootCA X2	DST RootCA X2	28.11.2008
DSTCA E1	DSTCA E1	10.12.2018
DSTCA E2	DSTCA E2	09.12.2018
DST-Entrust GTI CA	DST-Entrust GT...	09.12.2018
Entrust.net Secure Server Certific...	Entrust.net Sec...	25.05.2019
Equifax Secure Certificate Authority	Equifax Secure ...	22.08.2018

Trusted Root Certification Authorities store contains 116 certificates.

- Select *Certificates - Current User* → *Intermediate Certification Authorities* → *Certificates* . In the right panel you should find the 3 certificates named: *DIGISIGN FOR UNNPR*, *DIGISIGN PUBLIC* and *DigiSign Qualified Public CA* if the trust chain installation was properly made.



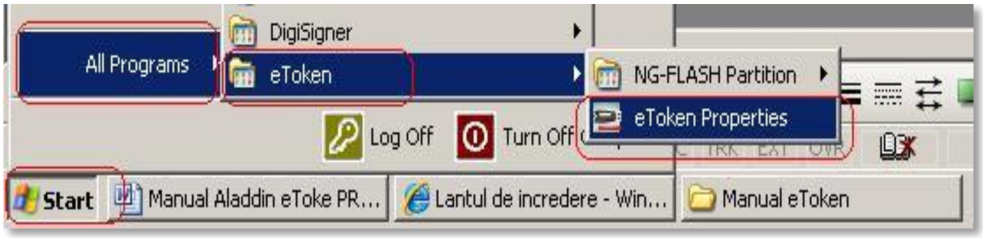
Certificates - Current User
- Personal
- Trusted Root Certification Authc
- Enterprise Trust
- Intermediate Certification Authc
  - Certificate Revocation List
  - Certificates
- Active Directory User Object
- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certification Au
- Trusted People
- Other People
- Certificate Enrollment Requests

Issued To	Issued By	Expiration Date
Adacom Class 2 CA	VeriSign Trust N...	20.08.2010
DIGISIGN FOR UNNPR	Digisign Qualifie...	27.05.2014
DIGISIGN PUBLIC	Digisign Qualifie...	24.04.2014
DigiSign Qualified Public CA	DigiSign Qualifie...	11.05.2021
GlobalSign Root CA	Root SGC Auth...	28.01.2014
GTE CyberTrust Root	Root SGC Auth...	23.02.2006
i.ines.ro	iNES Advertising	18.12.2010
Microsoft Certificate Trust List PCA	Microsoft Root ...	02.04.2019
Microsoft Internet Authority	GTE CyberTrust...	14.04.2018
Microsoft Secure Server Authority	Microsoft Inter...	20.05.2014
Microsoft Windows Hardware Com...	Microsoft Root ...	31.12.2002
Microsoft Windows Hardware Com...	Microsoft Root ...	31.12.2002
MS SGC Authority	Root SGC Auth...	01.01.2010
MSN Content Authentication CA	MSN Content PCA	24.02.2010
MSN Content PCA	Microsoft Root ...	09.02.2017
Root Agency	Root Agency	01.01.2040
SecureNet CA SGC Root	Root SGC Auth...	16.10.2009
Thawte Premium Server CA	Root SGC Auth...	16.07.2004
Thawte Server CA	Root SGC Auth...	16.07.2004

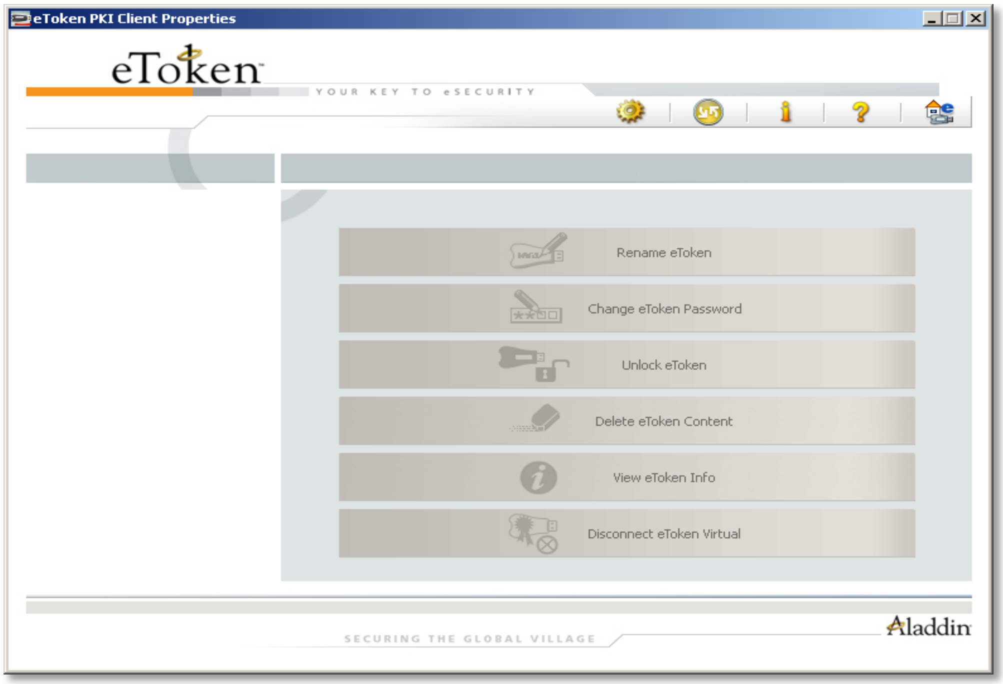
Intermediate Certification Authorities store contains 27 certificates.

2.4 Verificarea instalării driverului Aladdin eToken

From the **Windows Start** menu, choose **All Programs** → **eToken** → **eToken Properties .**



If the application was successfully installed, the following window will be opened:



3. Obtaining the e-Token device password

The initial access password (PIN CODE) of the e-Token device is sent within the envelope that holds the USB Aladdin e-Token PRO device which contains the digital qualified certificate.

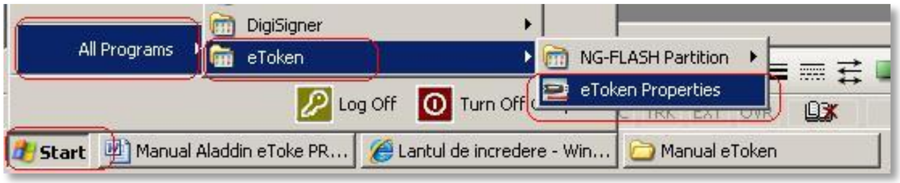
1. **AFTER THE ONLINE RENEWAL OF THE CERTIFICATE, THE PIN CODE WON'T CHANGE.**

2. **AFTER THE OFFLINE RENEWAL OF THE CERTIFICATE, THE PIN CODE WILL BE CHANGED.**

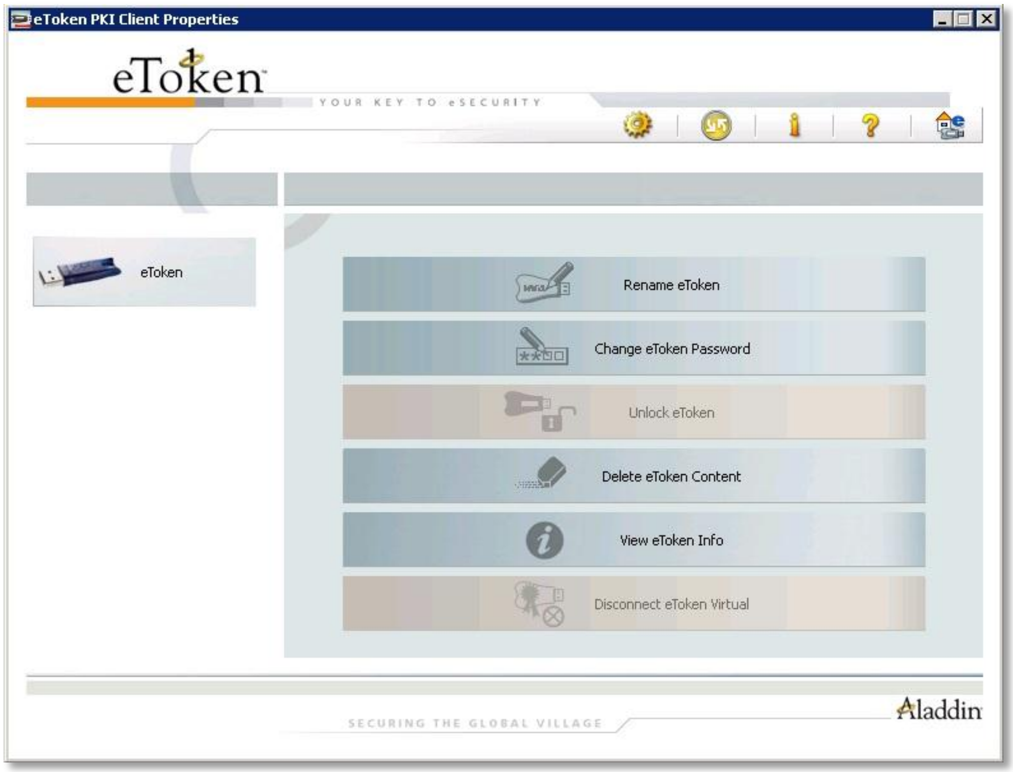
4. Using the Aladdin eToken utility

Connect the USB Aladdin e-Token device to the computer.

From the **Windows Start** menu, choose ***All Programs*** → ***eToken*** → ***eToken Properties*** .



On your screen, the following eToken PKI Client Properties window will be displayed:



4.1. Rename eToken

This function is optional and allows the user to change the device name (for customization purposes):

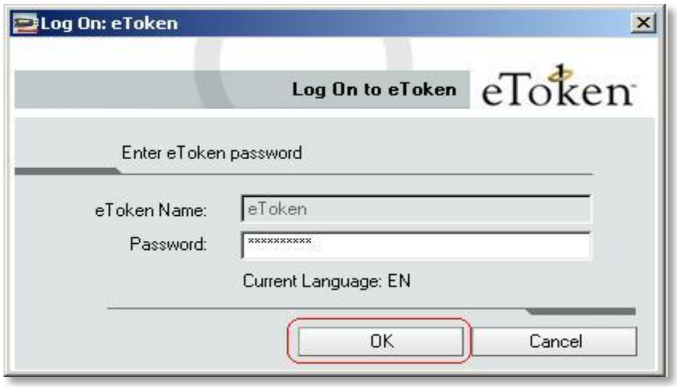
a) Choose the **Rename eToken** option;

b) In the **Password** field, you will have to fill in the e-Token device pin code.

WARNING (!):

If you will provide a wrong password for more than 15 times consecutively, the e-Token security device will automatically lock itself and there will be no possibility of unlocking it.

If the Pin Code is correct then you should continue by clicking the OK button.



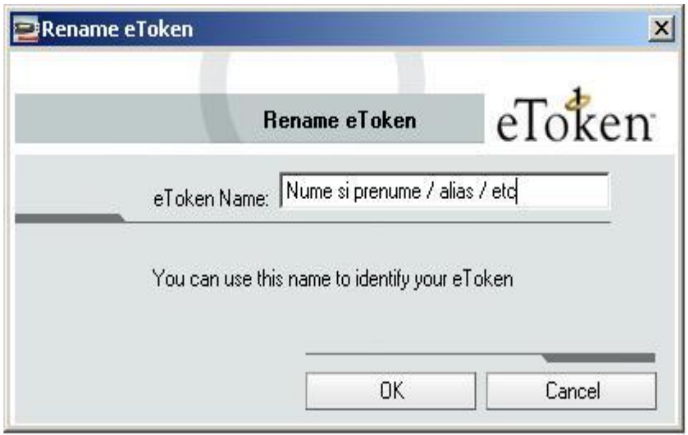
Enter eToken password

eToken Name: eToken

Password: **********

Current Language: EN

In the **eToken Name** field you should type your desired e-Token name:



eToken Name: Nume si prenume / alias / etc

You can use this name to identify your eToken

4.2. Change Password

This function is recommended.

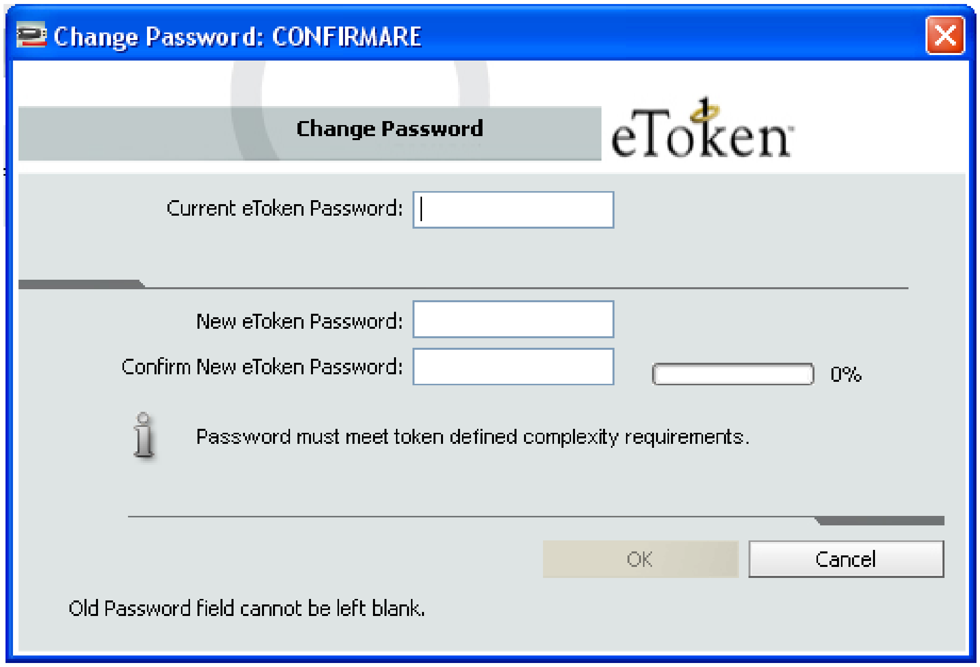
OBS: If you want to change the password of the eToken device, the utility will force you to enter a new password that meets the following criteria :

- minimum number of characters – 8;
- maximum number of characters - 24;
- the password must contain at least one lowercase, one uppercase and one number.

IMPORTANT (!):

If you will provide a wrong password for more than 15 times consecutively, the e-Token security device will automatically lock itself and there will be no possibility of unlocking it.

a) In the first field, **Current eToken Password,** you'll have to type the password supplied by DigiSign.
b) In the second field, **New eToken Password,** you must type a new password (the desired one).
c) In the third field, **Confirm New eToken Password,** you'll have to re-type the new password in order to confirm it.



Change Password: CONFIRMARE

Change Password

eToken

Current eToken Password:

New eToken Password:

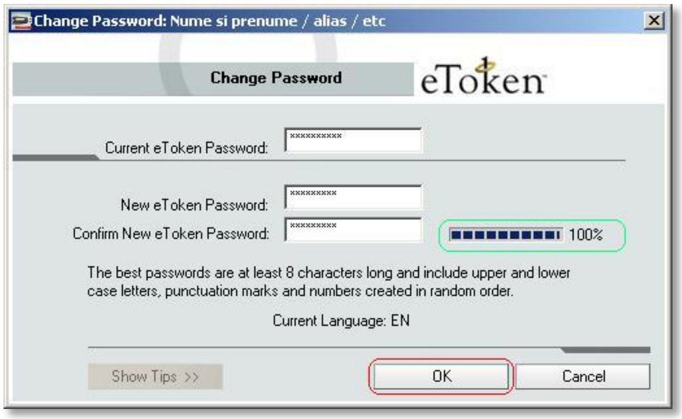
Confirm New eToken Password:

0%

Password must meet token defined complexity requirements.

Old Password field cannot be left blank.

d) If the new password meets the requirements listed above, click the OK button.



Change Password: Nume si prenume / alias / etc

Change Password

Current eToken Password: **********

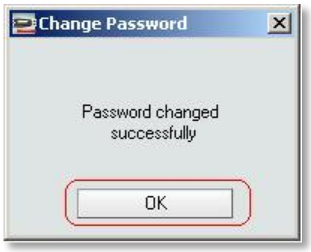
New eToken Password: *********

Confirm New eToken Password: ********* 100%

The best passwords are at least 8 characters long and include upper and lower case letters, punctuation marks and numbers created in random order.

Current Language: EN

e) Press the OK button.



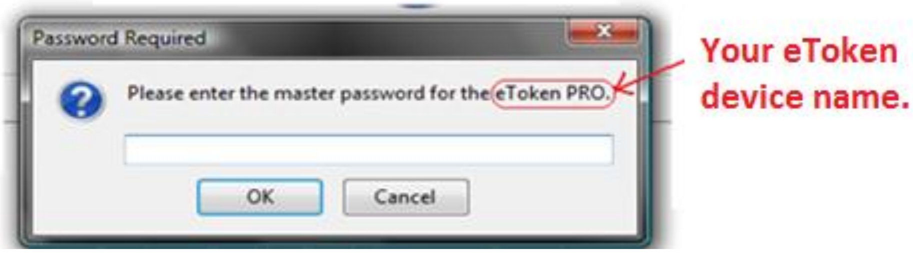
Change Password

Password changed successfully

At this point, the utility is properly configured. There are no other necessary actions needed and you can start using the DigiSign qualified digital certificate.

IMPORTANT:

If you regulary use the Mozilla Firefox Internet Browser, when you will install the Aladdin eToken application, its module is automatically uploaded into the Mozilla Browser. Each time you will connect the USB token to your computer, the browser will automatically prompt for the eToken password.



Password Required

Please enter the master password for the eToken PRO.

Your eToken device name.

DO NOT press the OK button without entering the correct e-Token password because empty spaces are considered characters and will be taken into consideration for the 15 allowed attempts to provide the correct password.

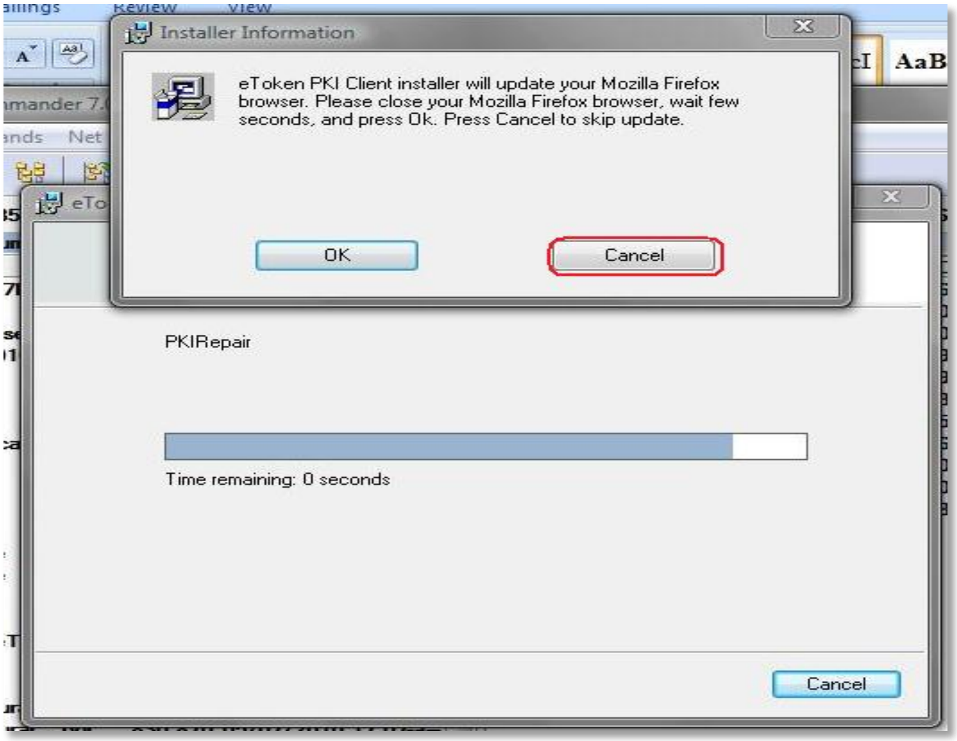
<u>There are two ways of unloading this module:</u>

1. During the installation..

   a) Disconnect the USB eToken device

   b) Open Mozilla Firefox before you start the eToken device installer

   c) While installing, you will be asked if you want the installer to update your Mozilla Firefox browser or not. We advise that you to press the „***Cancel***" button.



Installer Information

eToken PKI Client installer will update your Mozilla Firefox browser. Please close your Mozilla Firefox browser, wait few seconds, and press Ok. Press Cancel to skip update.

PKIRepair

Time remaining: 0 seconds

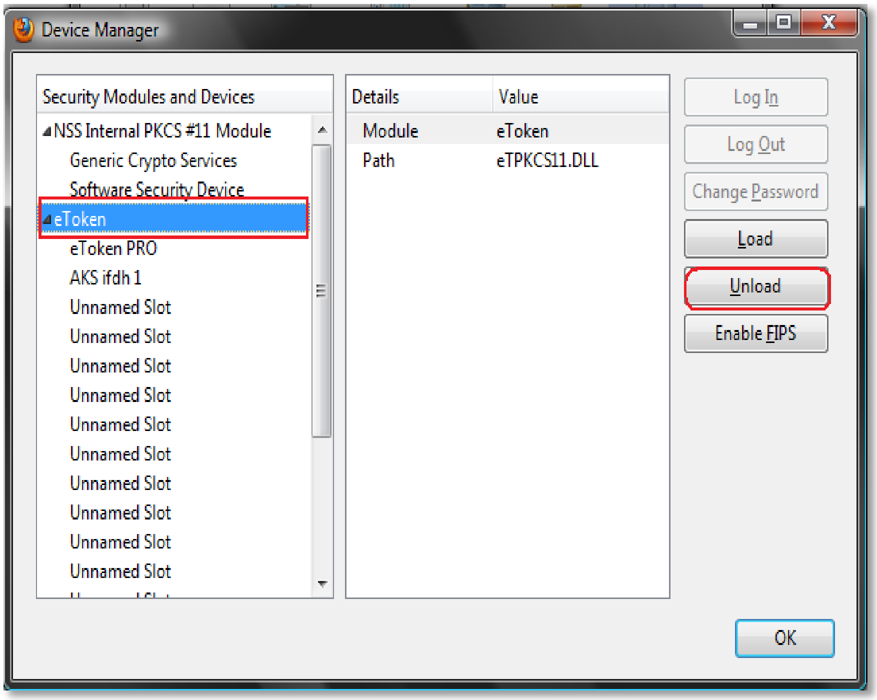
2. If the eToken device driver was already installed:

   a) Disconnect the USB eToken device

   b) Open Mozilla Firefox

   c) Go to Tools→ Options → Advanced → Encryption → Security Devices

   d) Select the eToken module, click the **Unload** button and then OK.



Details	Value
Module	eToken
Path	eTPKCS11.DLL

   e) Restart the Mozilla Firefox Internet Browser.

S.C. DigiSign S.A. provides qualified digital certificates issued under the 455/2001 (Law on electronic signature) Law. These qualified certifcates can be used in different systems (eg. **ANAF, NSC, NTC, CSSPP AEGRM, CSA CEDAM, SEAP**), where **S.C. DigiSign S.A.** is not an operator and does not have the possibility to offer advice or support in order to use those facilities offered by the public state institutions.
In order to obtain access to those platforms and further guidance for using the DigiSign qualified digital certificate therein, please contact the administrators of those systems.

Useful links:

- Installing and using the digital signature with Microsoft Office 2007
- Installing and using the digital signature with Microsoft Outlook 2007
- Installing and using the digital signature with Outlook Express 6
- Setting up the option for checking the validity of public hierarchy certificates for Adobe Reader
- Download Adobe Acrobat Reader 8.2
- Download Adobe Reader 10.1.0

Video tutorials:

- How to install a digital certificate – video tutorial
- How to register a digital certificate to ANAF - video tutorial

Revisions:

No.	Version	Date
1	1.0	12.07.2011
2	1.1	05.09.2011
3	1.2	12.09.2011
4	1.3	12.10.2012