DohatecCA
Certifying Authority

Dohatec CA

User Guide for eToken Pro 72K and iKey 2032

[VERSION 1.0]

Importing PKCS#12 Form into the eToken Pro 72K and iKey 2032

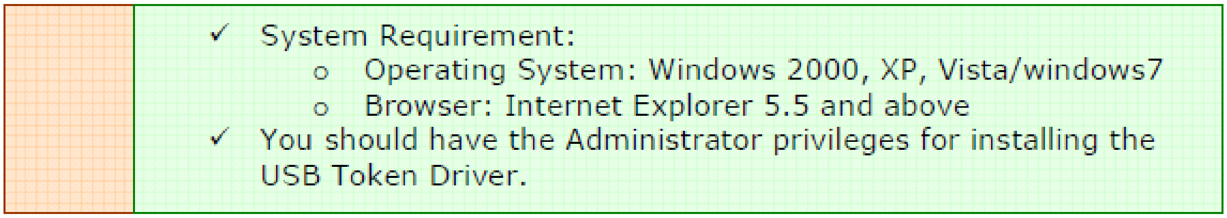
<u>Getting Started</u>

To start the process, procedure of the Digital Certificate Enrollment Kit from Dohatec CA or its Registration Authorities. The kit contains:

- USB Token (Safenet eToken pro 72K and iKey 2032)
- Installation CD contains:
  - ➢ USB Drivers

Note:

- *Use the Installation CD to install the USB Token driver.*
- *Ensure the following before installing the USB token driver.*

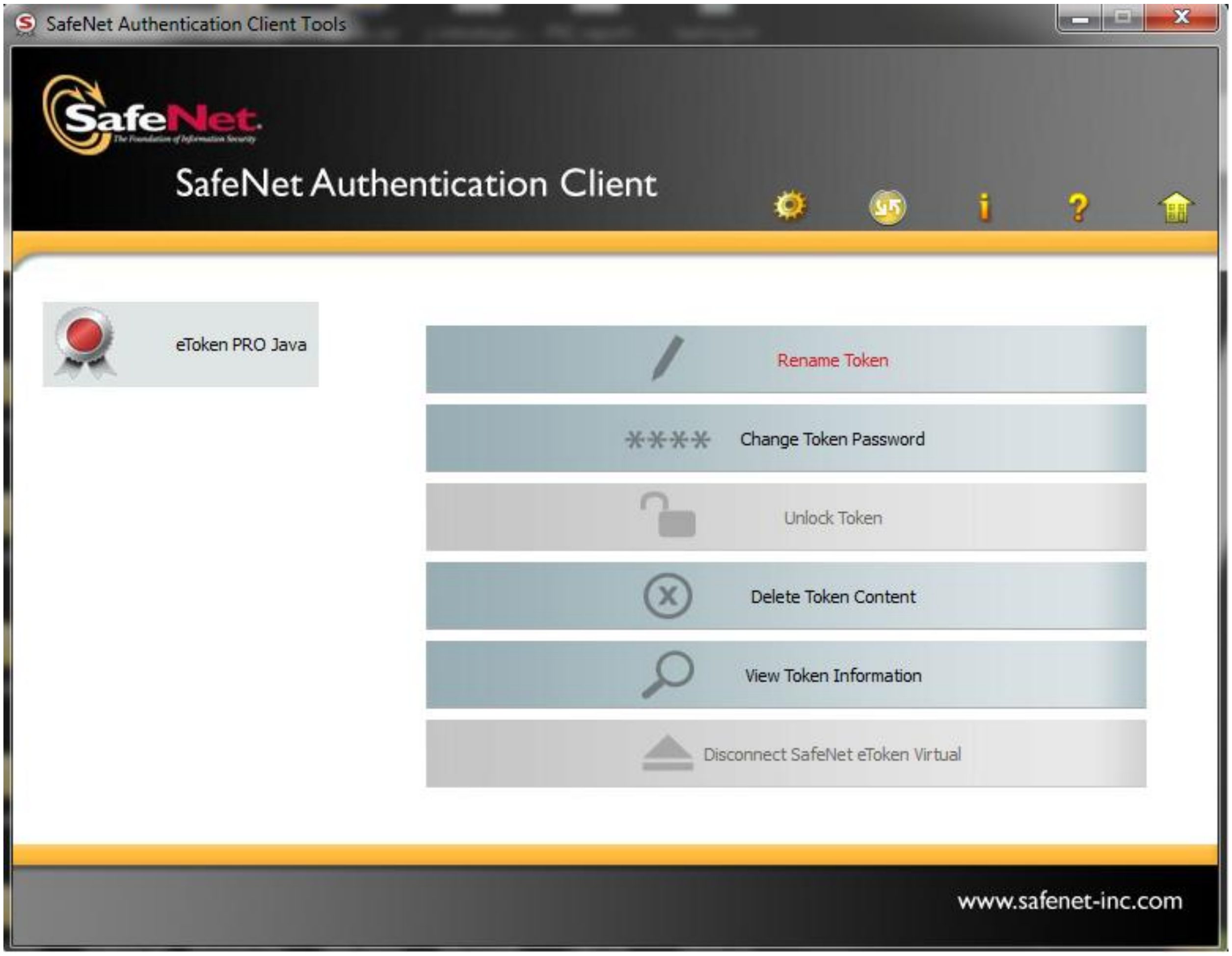


✓ System Requirement:
  - o Operating System: Windows 2000, XP, Vista/windows7
  - o Browser: Internet Explorer 5.5 and above

✓ You should have the Administrator privileges for installing the USB Token Driver.

1. To install eToken Pro 72K drivers, insert the CD.
2. Click on the Windows Installer Package named **'SafeNetAuthenticationClient-x32-x64-8.1-SP1.exe'**, (if the OS is 32/64 bit then click on '**SafeNetAuthenticationClient-x32-x64-8.1-SP1.exe'**) accept the License Agreement and proceed with installation.
3. Insert the token USB Token in the USB port of the computer, if prompted
4. Restart the computer after the installation is complete.

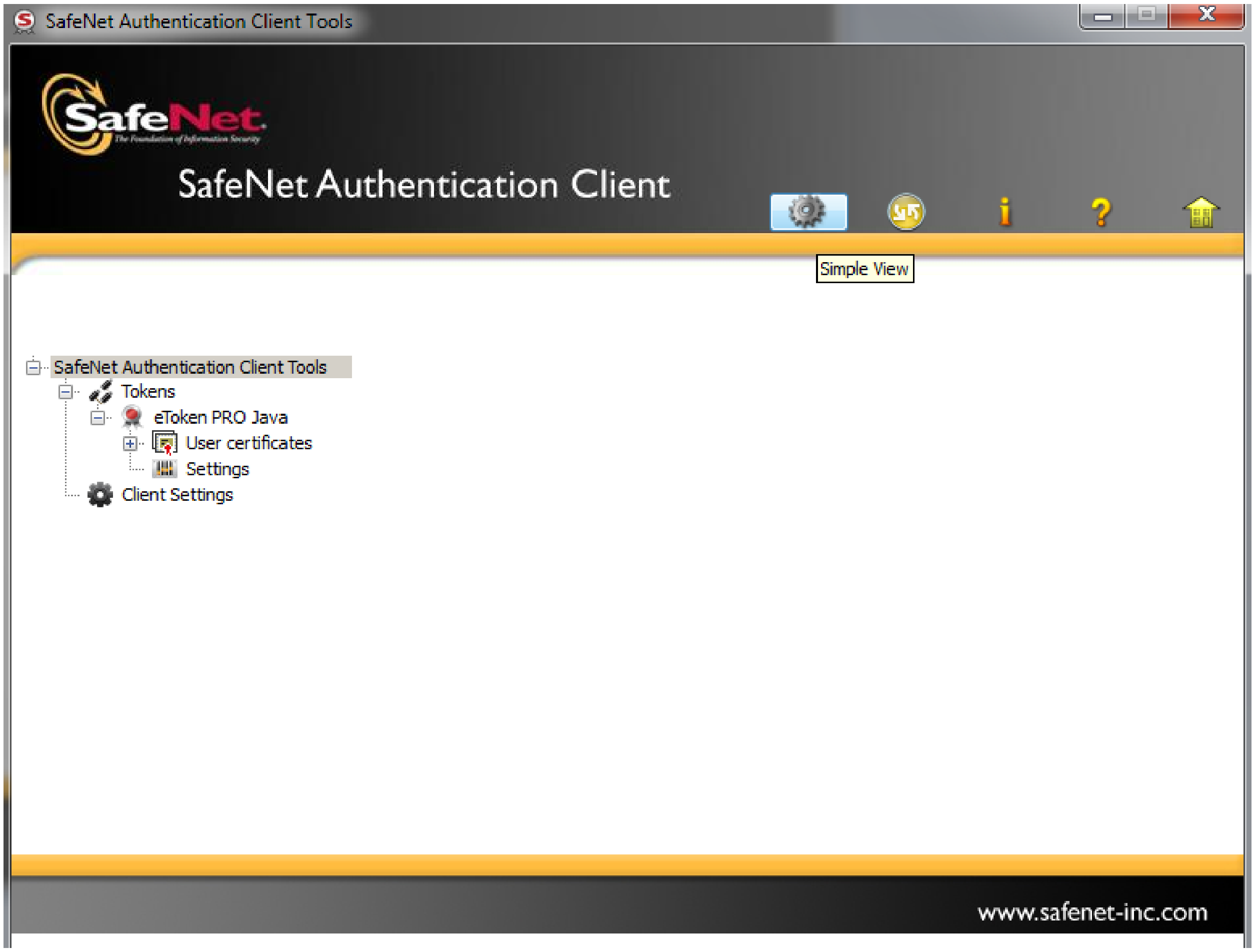
After completing the installation process now go to **Start** > **All Programs** > **Safenet** > **Safenet Authentication Client** > **Safenet Authentication Client Tools** with your Token inserted, the following screen is displayed.


SafeNet Authentication Client Tools
SafeNet
The Foundation of Information Security
SafeNet Authentication Client
eToken PRO Java
Rename Token
Change Token Password
Unlock Token
Delete Token Content
View Token Information
Disconnect SafeNet eToken Virtual
www.safenet-inc.com

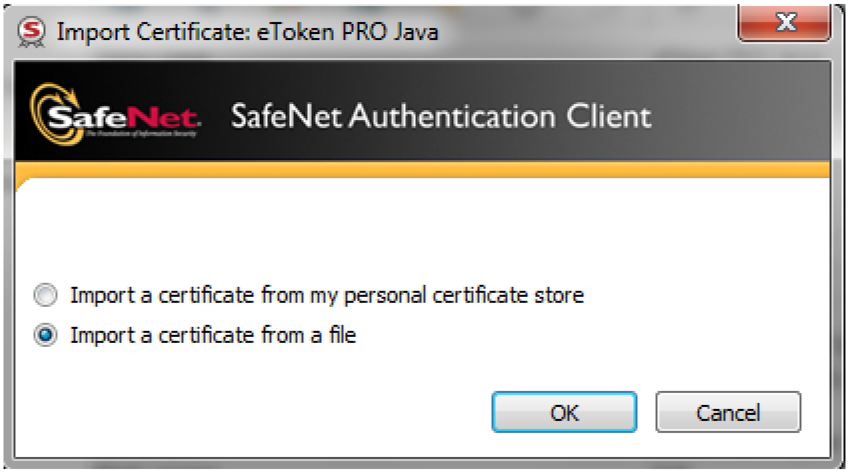
Import Procedure:

Select the 'Advanced' option on the Token properties screen. If password is necessary then provide the Token password to login and start importing the certificate.

➢ Right click on Token name (here eToken Pro72K) then click "Import certificate" to import your certificate from ".PFX file" from a location on your Computer.


SafeNet Authentication Client Tools
SafeNet
The Foundation of Information Security
SafeNet Authentication Client
Simple View
SafeNet Authentication Client Tools
Tokens
eToken PRO Java
User certificates
Settings
Client Settings
www.safenet-inc.com

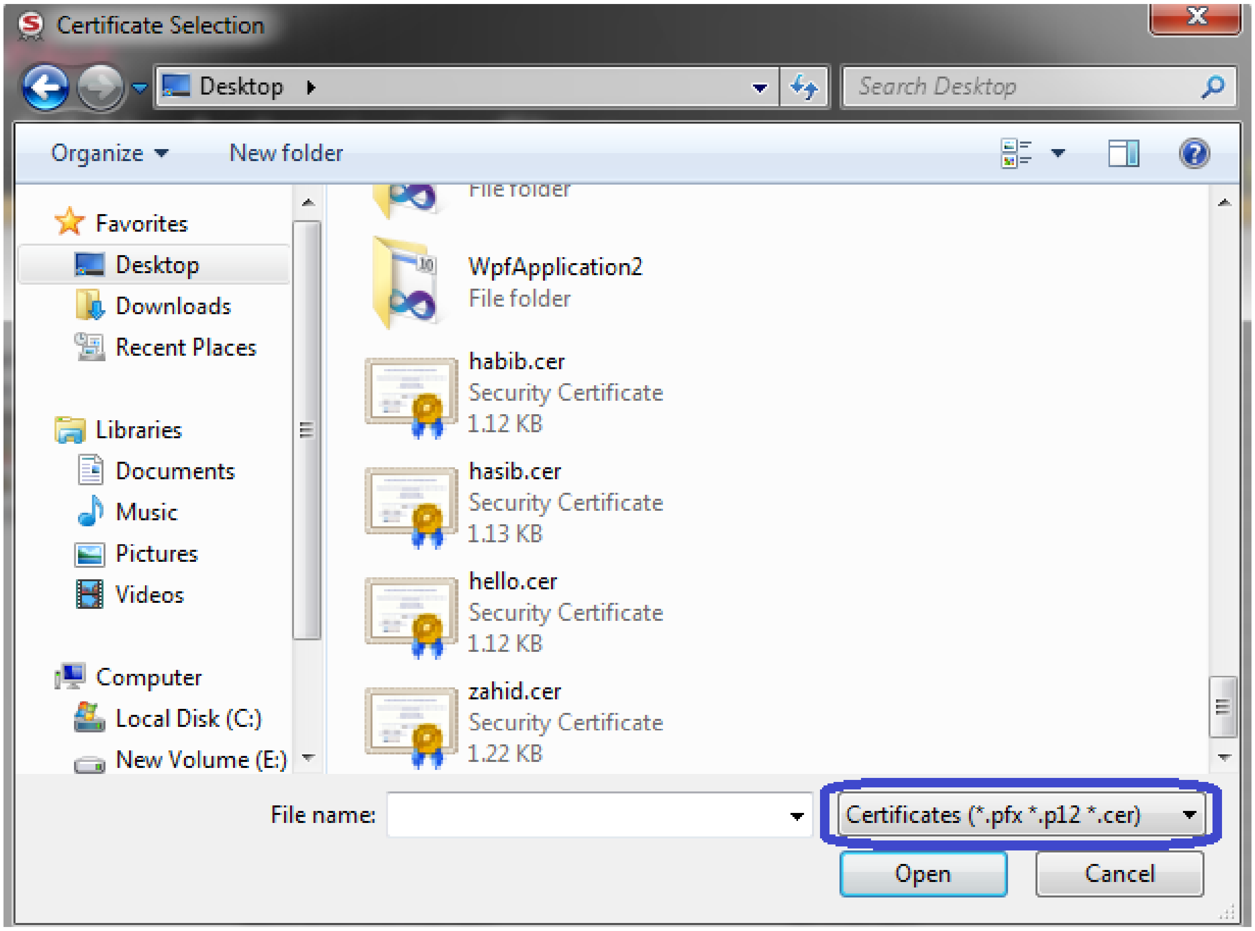
- Select “Import certificate from the file” and click “OK”.


Import Certificate: eToken PRO Java
SafeNet
SafeNet Authentication Client
OK
Cancel

○ Import a certificate from my personal certificate store

● Import a certificate from a file

- Select the path of the “.Pfx” file and click “OK”.



File folder

WpfApplication2
File folder

habib.cer
Security Certificate
1.12 KB

hasib.cer
Security Certificate
1.13 KB

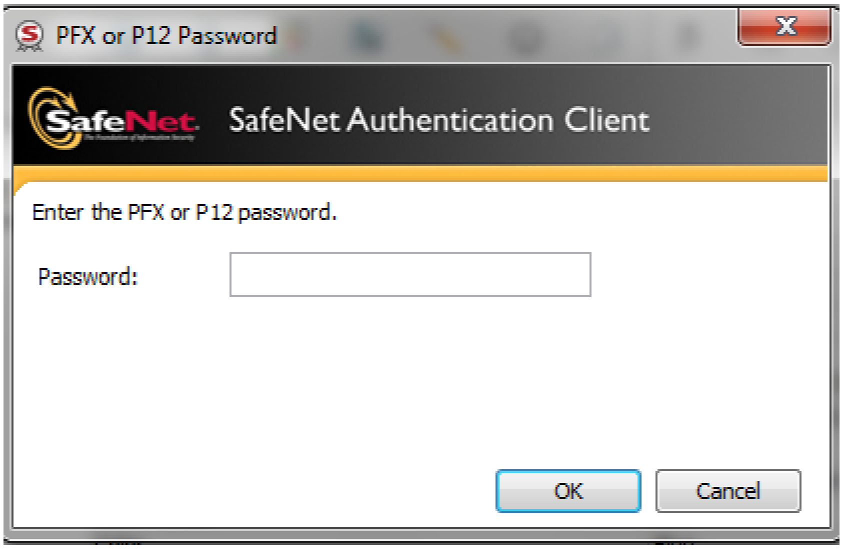
hello.cer
Security Certificate
1.12 KB

zahid.cer
Security Certificate
1.22 KB

File name:

Certificates (*.pfx *.p12 *.cer)

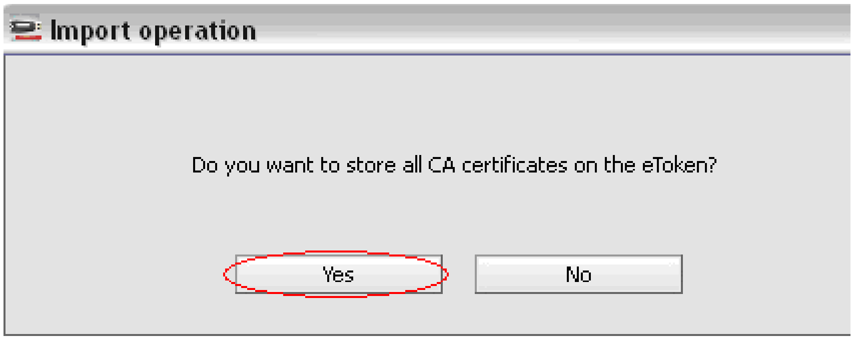
- A prompt for Password for the private key appears. Give the password that you had set to protect the file, while exporting the certificate and click “OK”



Enter the PFX or P12 password.

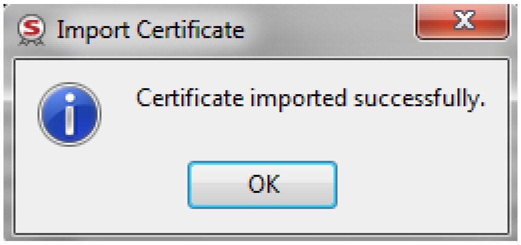
A certificate that is stored on the computer may be part of a hierarchical structure with more than one Certificate in the chain up to the Root CA. Importing a CA Chain takes the CA certificate and the complete CA Chain up to the root certificate that is stored on the computer and places it on the Token.

- When the certificate is imported onto the Token, the following message will confirm the import of the CA certificates. Click on 'Yes' to import the Root certificates.



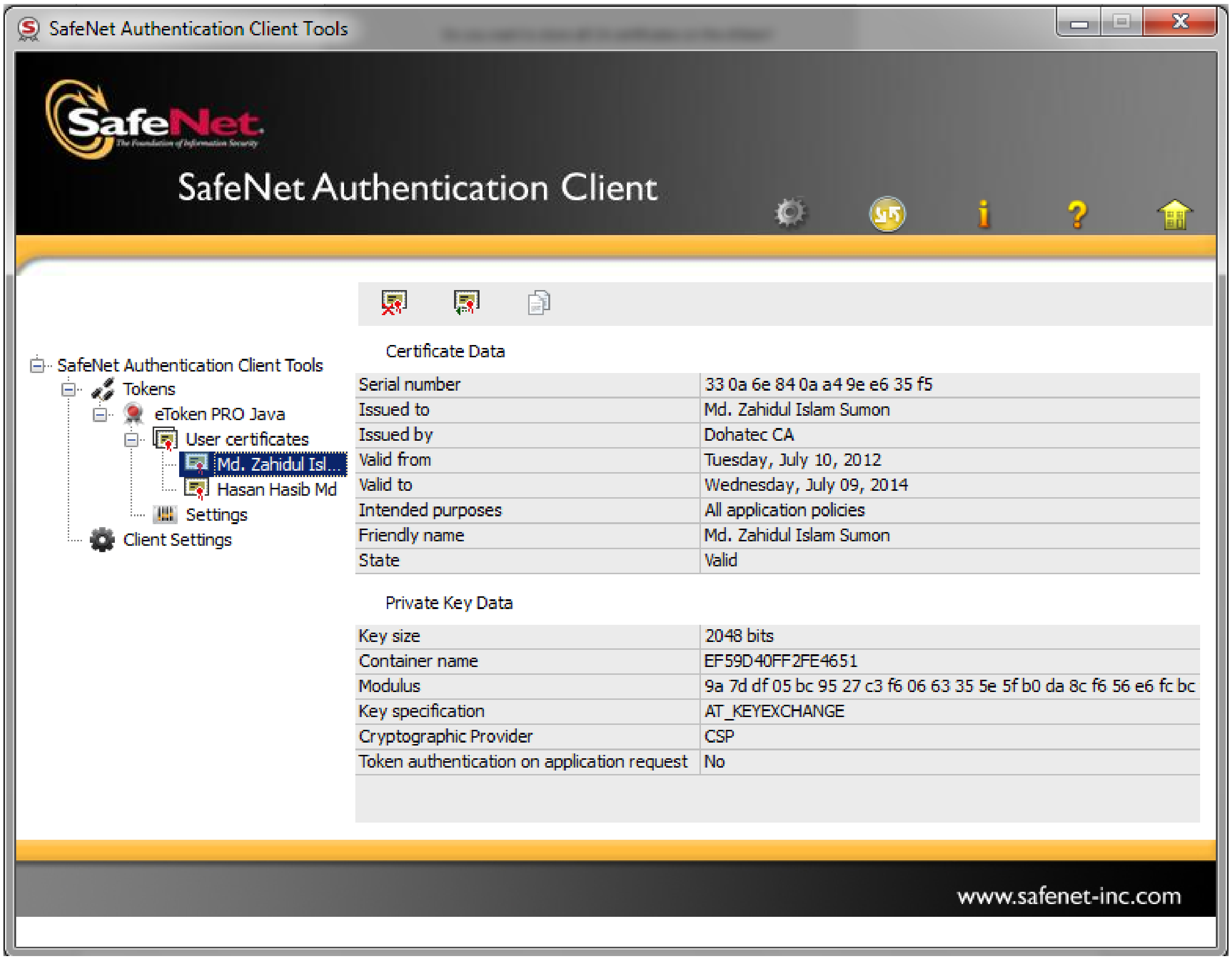
Do you want to store all CA certificates on the eToken?

- A message confirming that the import was successful is displayed.



Certificate imported successfully.

- The imported certificate can be checked under ‘User Certificates’.



SafeNet Authentication Client Tools
SafeNet
The Foundation of Information Security
SafeNet Authentication Client
SafeNet Authentication Client Tools
Tokens
eToken PRO Java
User certificates
Md. Zahidul Isl...
Hasan Hasib Md
Settings
Client Settings
www.safenet-inc.com

Certificate Data

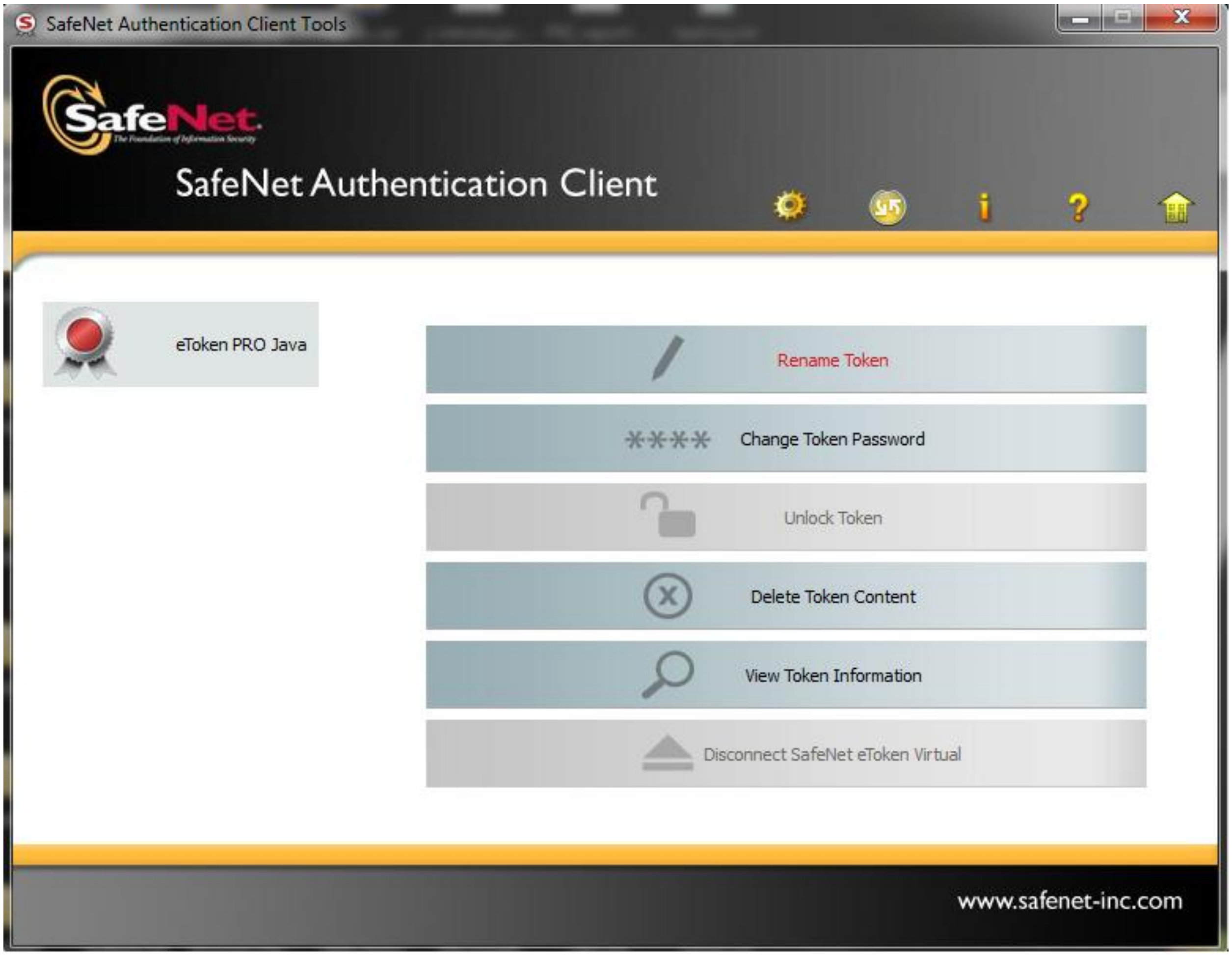
Serial number	33 0a 6e 84 0a a4 9e e6 35 f5
Issued to	Md. Zahidul Islam Sumon
Issued by	Dohatec CA
Valid from	Tuesday, July 10, 2012
Valid to	Wednesday, July 09, 2014
Intended purposes	All application policies
Friendly name	Md. Zahidul Islam Sumon
State	Valid

Private Key Data

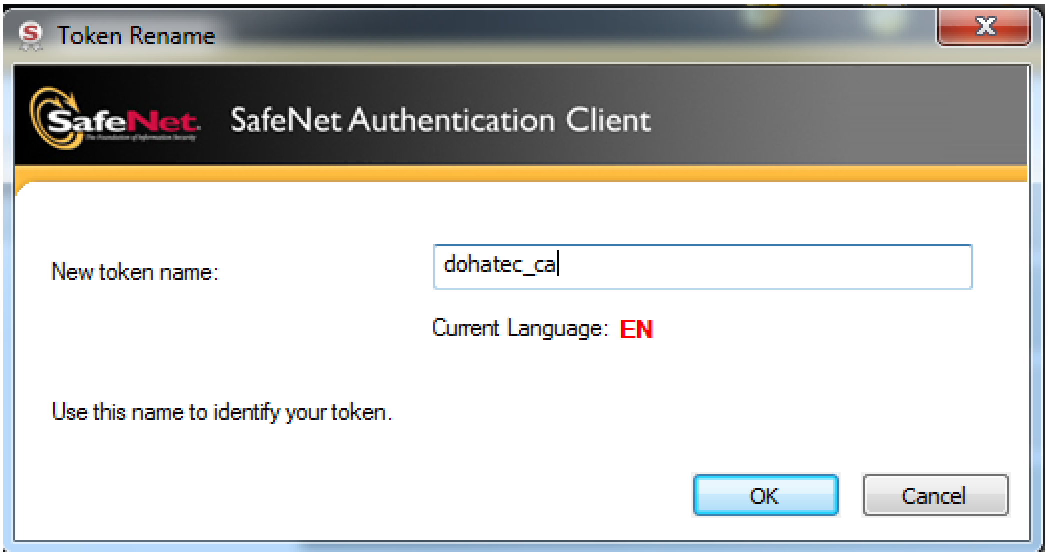
Key size	2048 bits
Container name	EF59D40FF2FE4651
Modulus	9a 7d df 05 bc 95 27 c3 f6 06 63 35 5e 5f b0 da 8c f6 56 e6 fc bc
Key specification	AT_KEYEXCHANGE
Cryptographic Provider	CSP
Token authentication on application request	No

Renaming the Token:

For additional convenience and ease of identification, the Token names can also be personalized. Click “Rename Token” on the Token Properties screen.


SafeNet Authentication Client Tools
SafeNet
The Foundation of Information Security
SafeNet Authentication Client
eToken PRO Java
Rename Token
Change Token Password
Unlock Token
Delete Token Content
View Token Information
Disconnect SafeNet eToken Virtual
www.safenet-inc.com

- ➢ Enter the new Token name in the Token name field and click on "OK" to set the Token name.
- ➢ Click “OK” and in the Token Properties window the new Token name is displayed



Token Rename

SafeNet Authentication Client

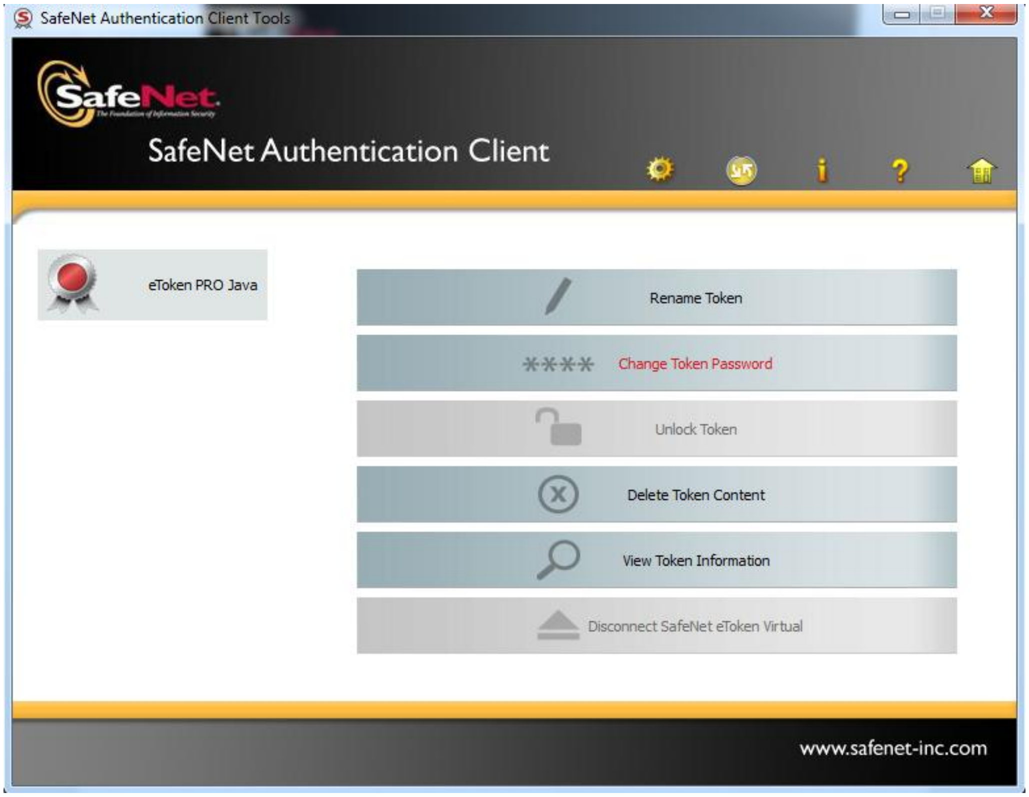
New token name: dohatec_ca

Current Language: EN

Use this name to identify your token.

Changing the Token Password:

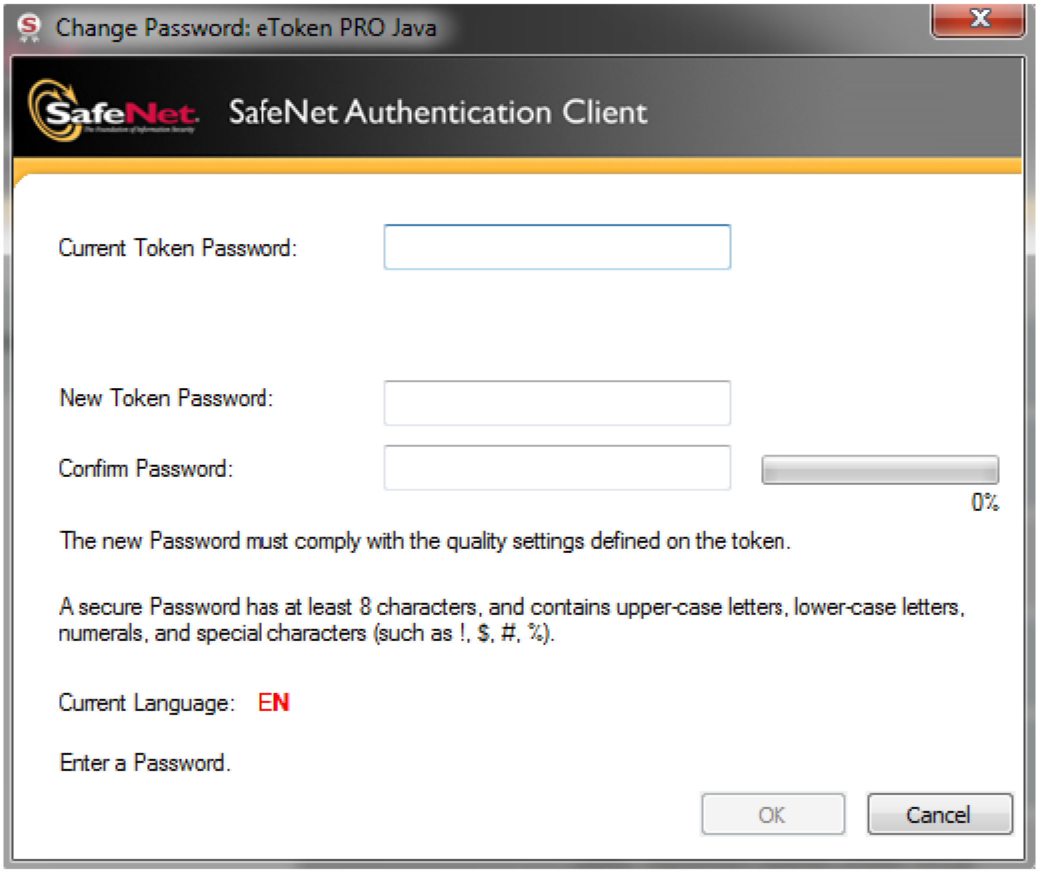
All Tokens are configured at manufacture with the factory default password (This password is normally “1234567890” for eToken Pro and “Password#1” for iKey 2032). Click “Change Token password” on the Token Properties screen and the following Token Properties dialog is displayed:



SafeNet Authentication Client Tools

SafeNet Authentication Client

Enter your current Token password in the "Current Token Password" field and, the new password in the "New Token Password" field. Confirm new Password and click "OK" to set the new Password.



The new Password must comply with the quality settings defined on the token.

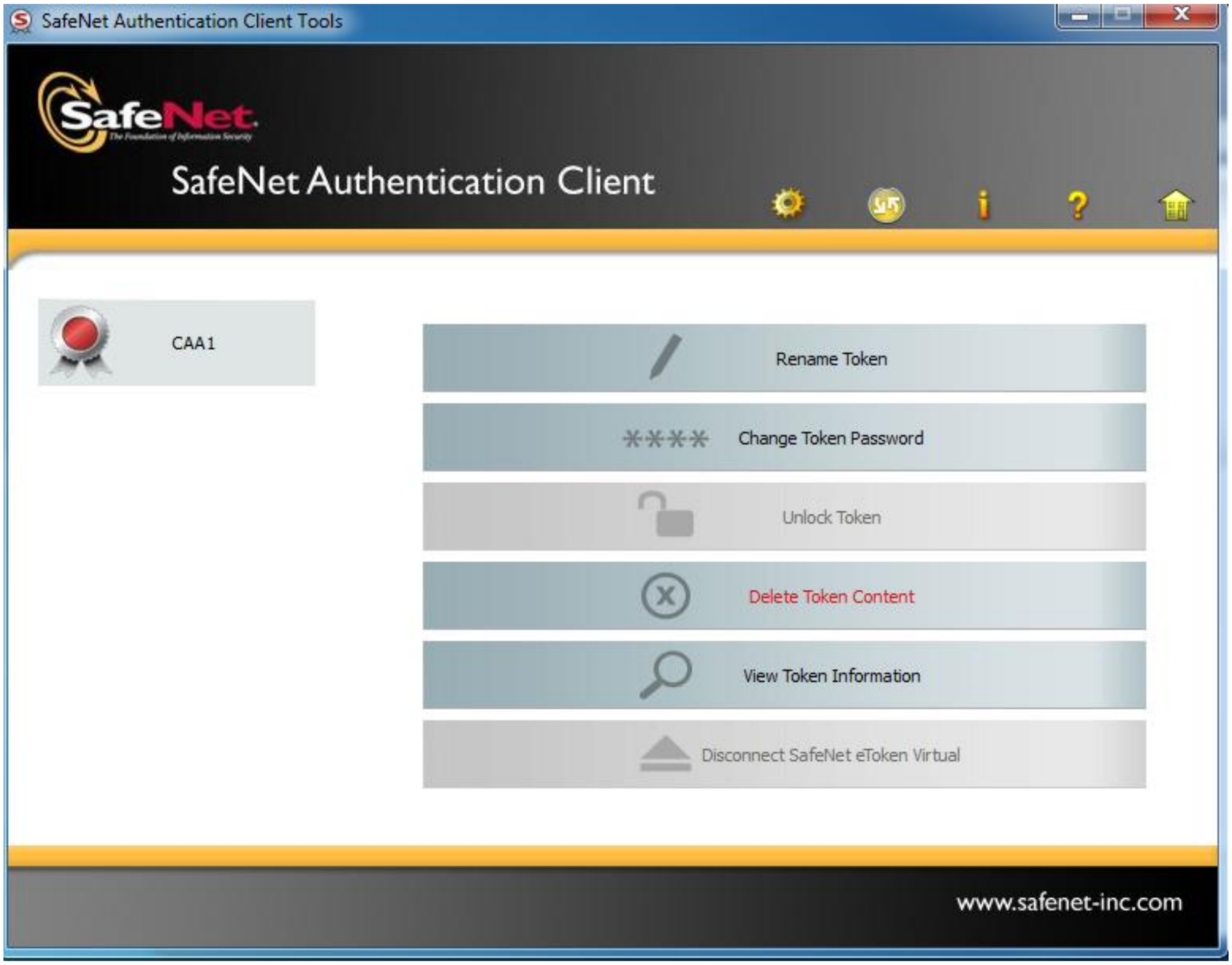
A secure Password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, $, #, %).

Current Language: EN

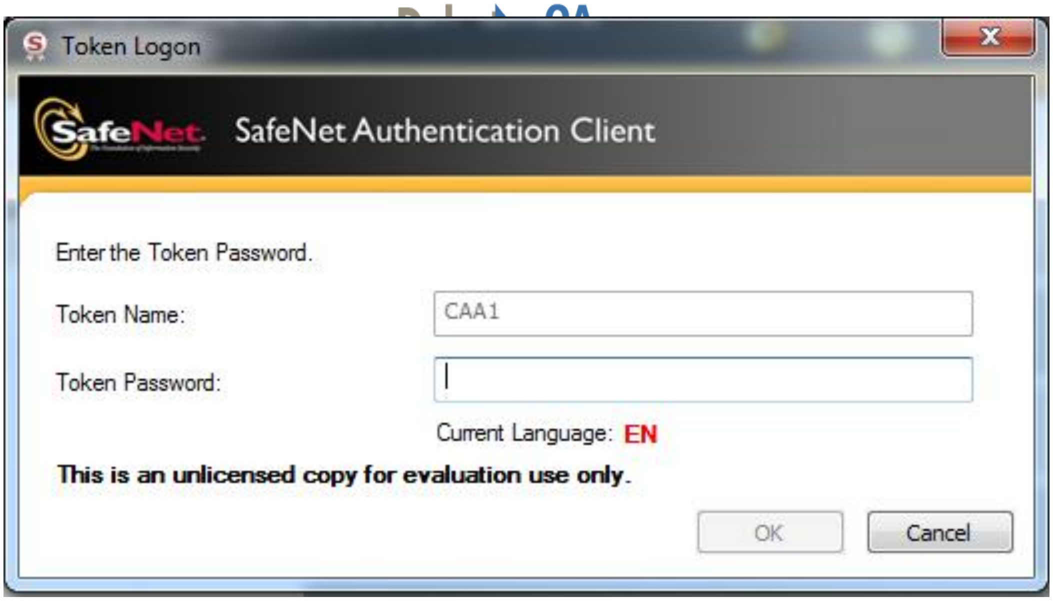
Enter a Password.

Deleting Token Content:

Step 1: If anyone wants to delete the certificates inserted into Token, then he or she may select 'Delete Token Content' option from the driver software.


SafeNet Authentication Client Tools
SafeNet
The Foundation of Information Security
SafeNet Authentication Client
CAA1
Rename Token
Change Token Password
Unlock Token
Delete Token Content
View Token Information
Disconnect SafeNet eToken Virtual
www.safenet-inc.com

Step 2: After selecting the option 'Delete Token Content', a window will be popped up to insert the device password.



SafeNet Authentication Client

Enter the Token Password.

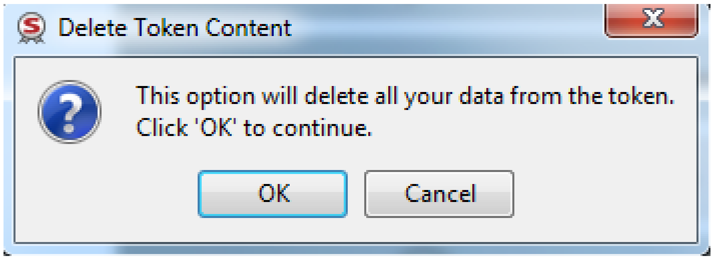
Token Name: CAA1

Token Password:

Current Language: EN

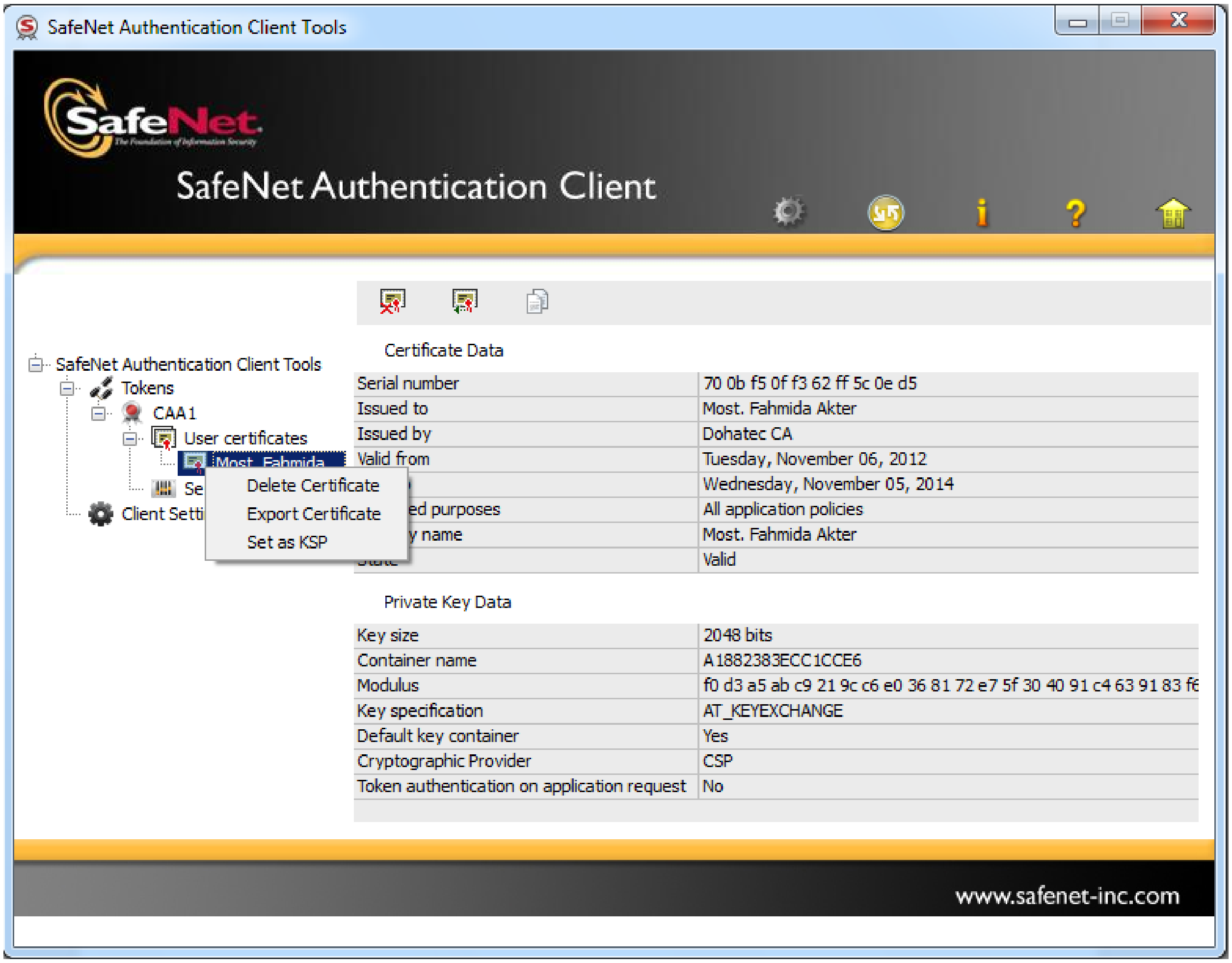
This is an unlicensed copy for evaluation use only.

Step 3: After providing the password, a confirmation window will be generated so that all certificates will be deleted or not.



This option will delete all your data from the token.
Click 'OK' to continue.

Step 4: If someone has more than one certificate in token, he may want to delete some of the existing certificates from the device. In this case, user can browse his/her certificate in simple view and select the certificate he wants to delete. He should right click on all the selected certificates and select the 'delete certificate' option.



SafeNet Authentication Client Tools
SafeNet
The Foundation of Information Security
SafeNet Authentication Client
SafeNet Authentication Client Tools
Tokens
CAA1
User certificates
Most. Fahmida
Se
Client Setti
Delete Certificate
Export Certificate
Set as KSP
www.safenet-inc.com

Certificate Data

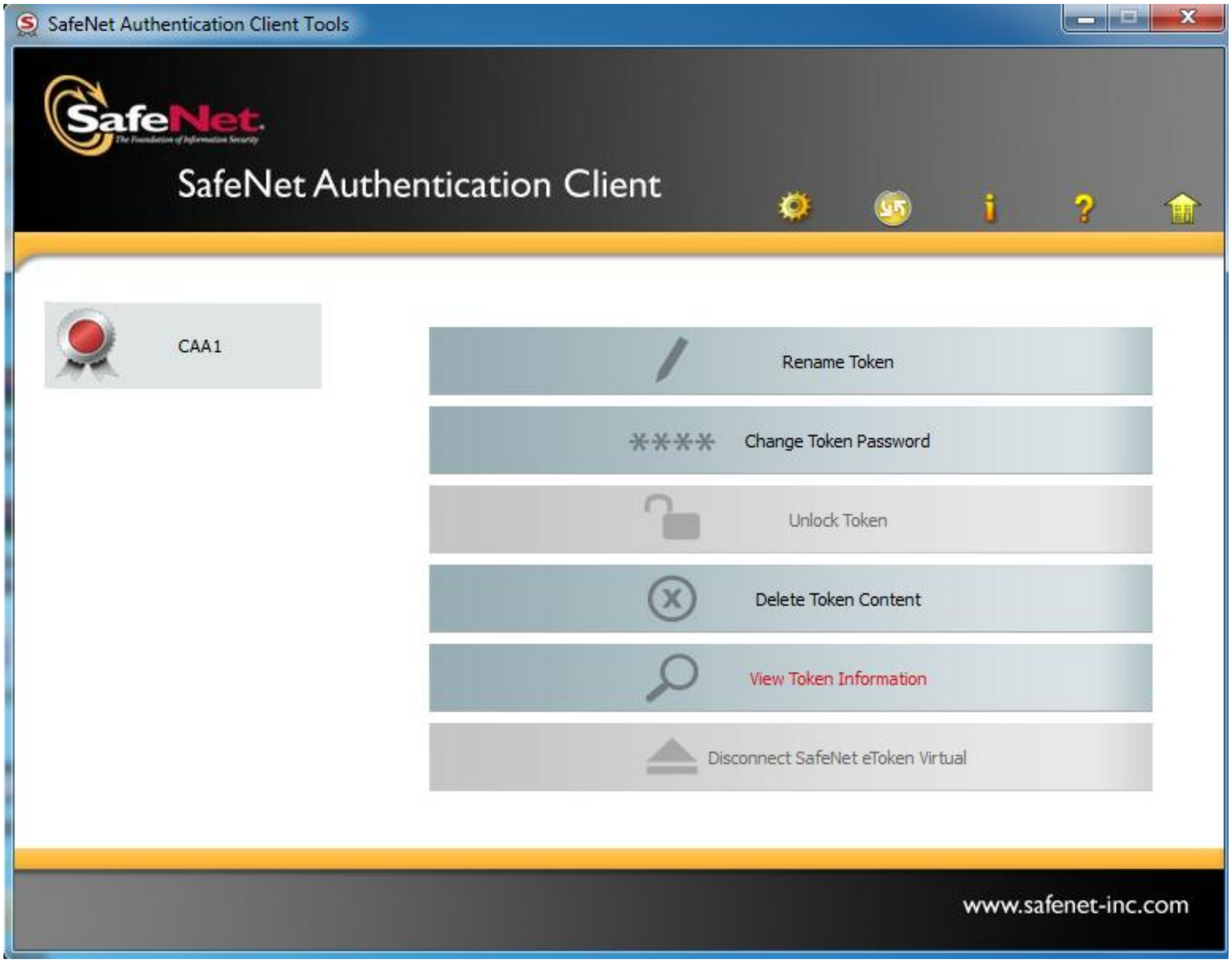
Serial number	70 0b f5 0f f3 62 ff 5c 0e d5
Issued to	Most. Fahmida Akter
Issued by	Dohatec CA
Valid from	Tuesday, November 06, 2012
)	Wednesday, November 05, 2014
ed purposes	All application policies
y name	Most. Fahmida Akter
State	Valid

Private Key Data

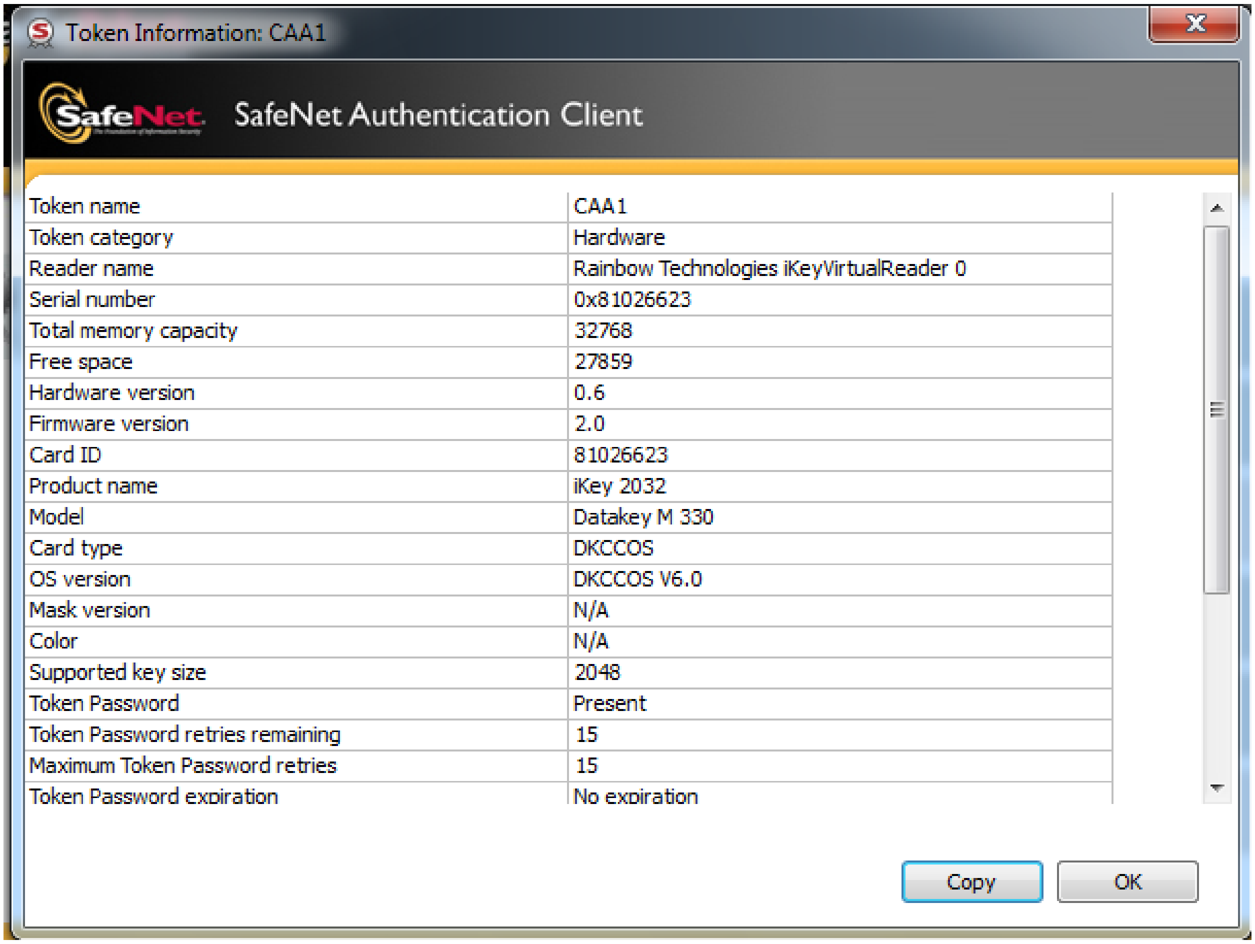
Key size	2048 bits
Container name	A1882383ECC1CCE6
Modulus	f0 d3 a5 ab c9 21 9c c6 e0 36 81 72 e7 5f 30 40 91 c4 63 91 83 f6
Key specification	AT_KEYEXCHANGE
Default key container	Yes
Cryptographic Provider	CSP
Token authentication on application request	No

Viewing Token Information:

For accessing information of the token, one needs to click the option 'View Token Information' from the 'Advanced view'.


SafeNet Authentication Client Tools
SafeNet
The Foundation of Information Security
SafeNet Authentication Client
CAA1
Rename Token
Change Token Password
Unlock Token
Delete Token Content
View Token Information
Disconnect SafeNet eToken Virtual
www.safenet-inc.com

After clicking ‘View Token Information’, the following window will popped up.



Token Information: CAA1

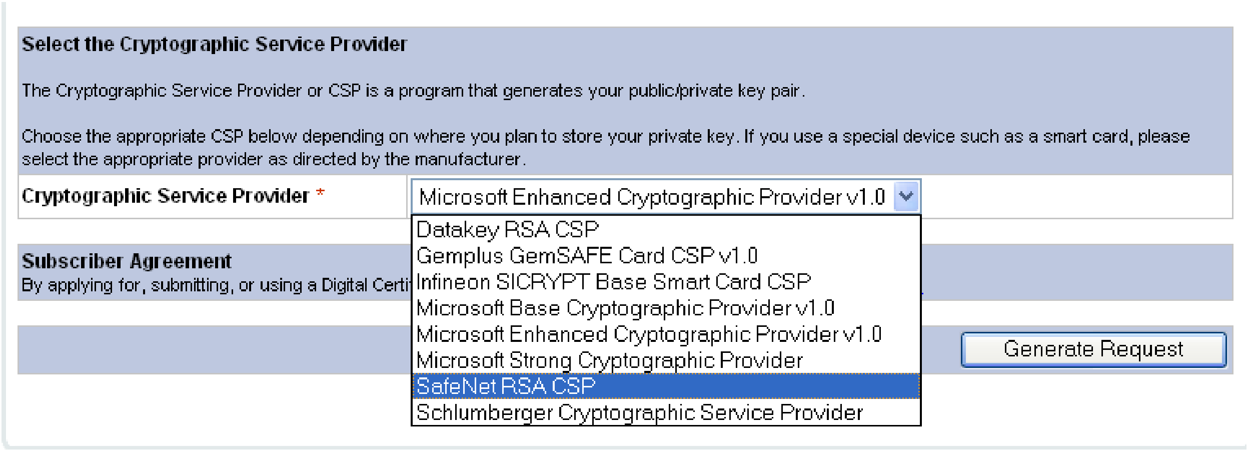
SafeNet Authentication Client

Token name	CAA1
Token category	Hardware
Reader name	Rainbow Technologies iKeyVirtualReader 0
Serial number	0x81026623
Total memory capacity	32768
Free space	27859
Hardware version	0.6
Firmware version	2.0
Card ID	81026623
Product name	iKey 2032
Model	Datakey M 330
Card type	DKCCOS
OS version	DKCCOS V6.0
Mask version	N/A
Color	N/A
Supported key size	2048
Token Password	Present
Token Password retries remaining	15
Maximum Token Password retries	15
Token Password expiration	No expiration

Using the Token in Dohatec CA website:

Generate Request with Token:

If the Subscriber uses the token then he/she need to insert his/her token first for doing the Enrollment. In the Enrollment Form, he/she have to select that token from the Cryptographic Service provider. Then he/she will generate his/her request.



Select the Cryptographic Service Provider

The Cryptographic Service Provider or CSP is a program that generates your public/private key pair.

Choose the appropriate CSP below depending on where you plan to store your private key. If you use a special device such as a smart card, please select the appropriate provider as directed by the manufacturer.

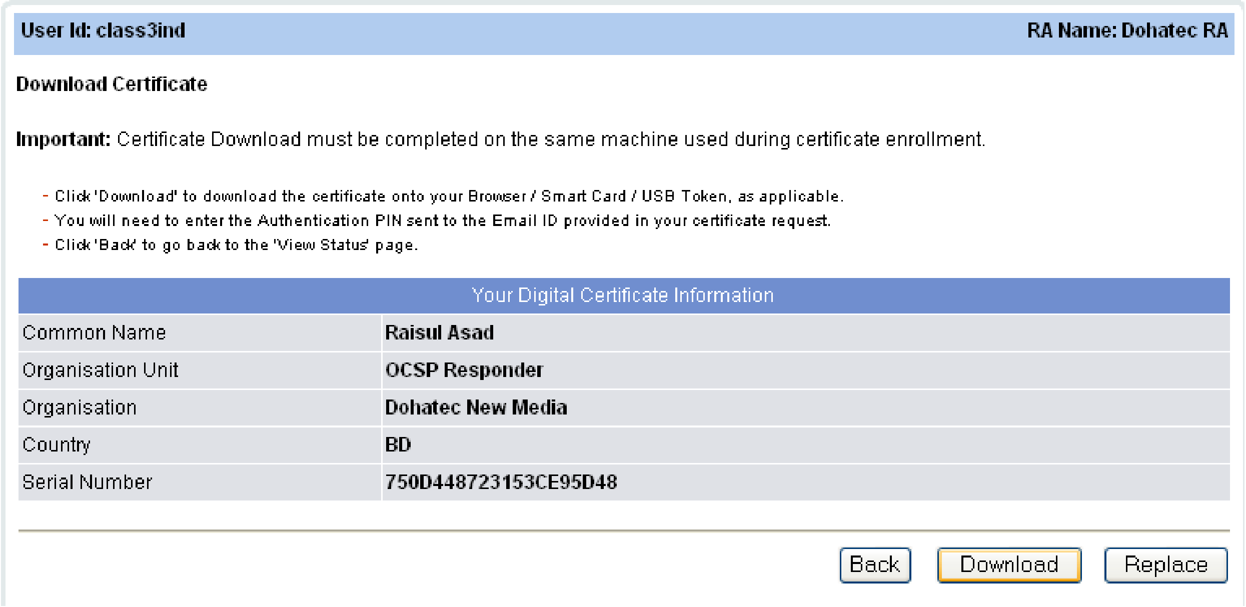
Cryptographic Service Provider *	Microsoft Enhanced Cryptographic Provider v1.0

Subscriber Agreement
By applying for, submitting, or using a Digital Certi

Datakey RSA CSP
Gemplus GemSAFE Card CSP v1.0
Infineon SICRYPT Base Smart Card CSP
Microsoft Base Cryptographic Provider v1.0
Microsoft Enhanced Cryptographic Provider v1.0
Microsoft Strong Cryptographic Provider
SafeNet RSA CSP
Schlumberger Cryptographic Service Provider
Generate Request

Download Certificate with the same Token:

Next step of the Subscriber is to download the request which he/she generated before. Because in the time of generating the request, he/she used the token that same token he/she has to use the same token for downloading his/her certificate.



User Id: class3ind **RA Name: Dohatec RA**

Download Certificate

Important: Certificate Download must be completed on the same machine used during certificate enrollment.

- Click 'Download' to download the certificate onto your Browser / Smart Card / USB Token, as applicable.
- You will need to enter the Authentication PIN sent to the Email ID provided in your certificate request.
- Click 'Back' to go back to the 'View Status' page.

Your Digital Certificate Information	
Common Name	**Raisul Asad**
Organisation Unit	**OCSP Responder**
Organisation	**Dohatec New Media**
Country	**BD**
Serial Number	**750D448723153CE95D48**