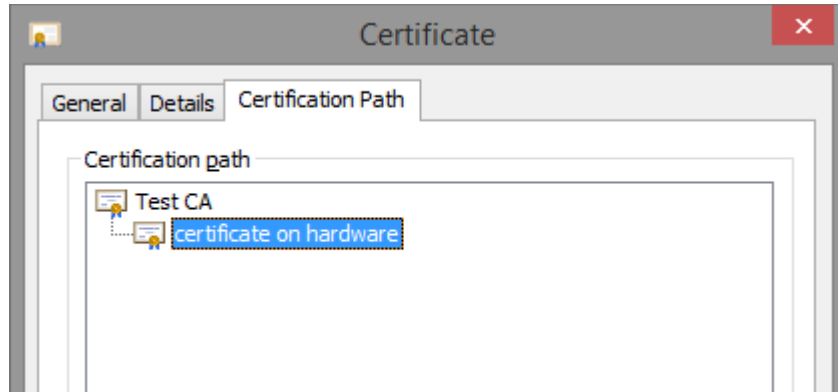


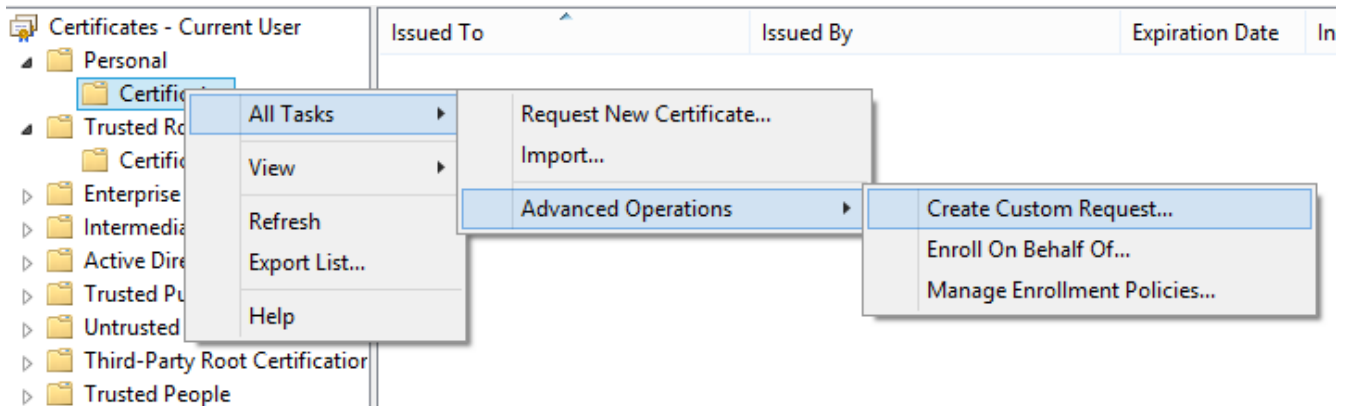
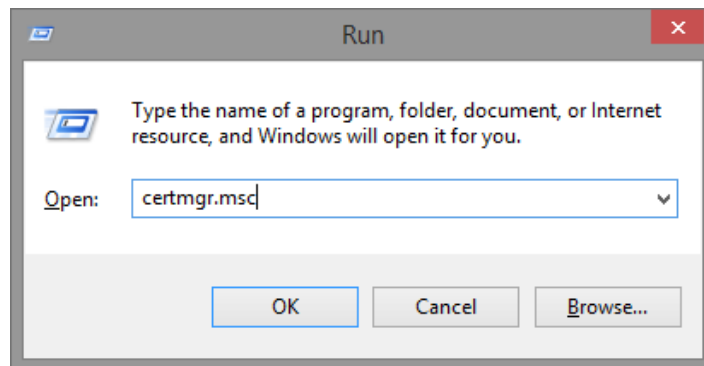
How to Generate a Certificate on a Hardware Device

Generate a Certificate using Certificate Manager (certmgr.msc)

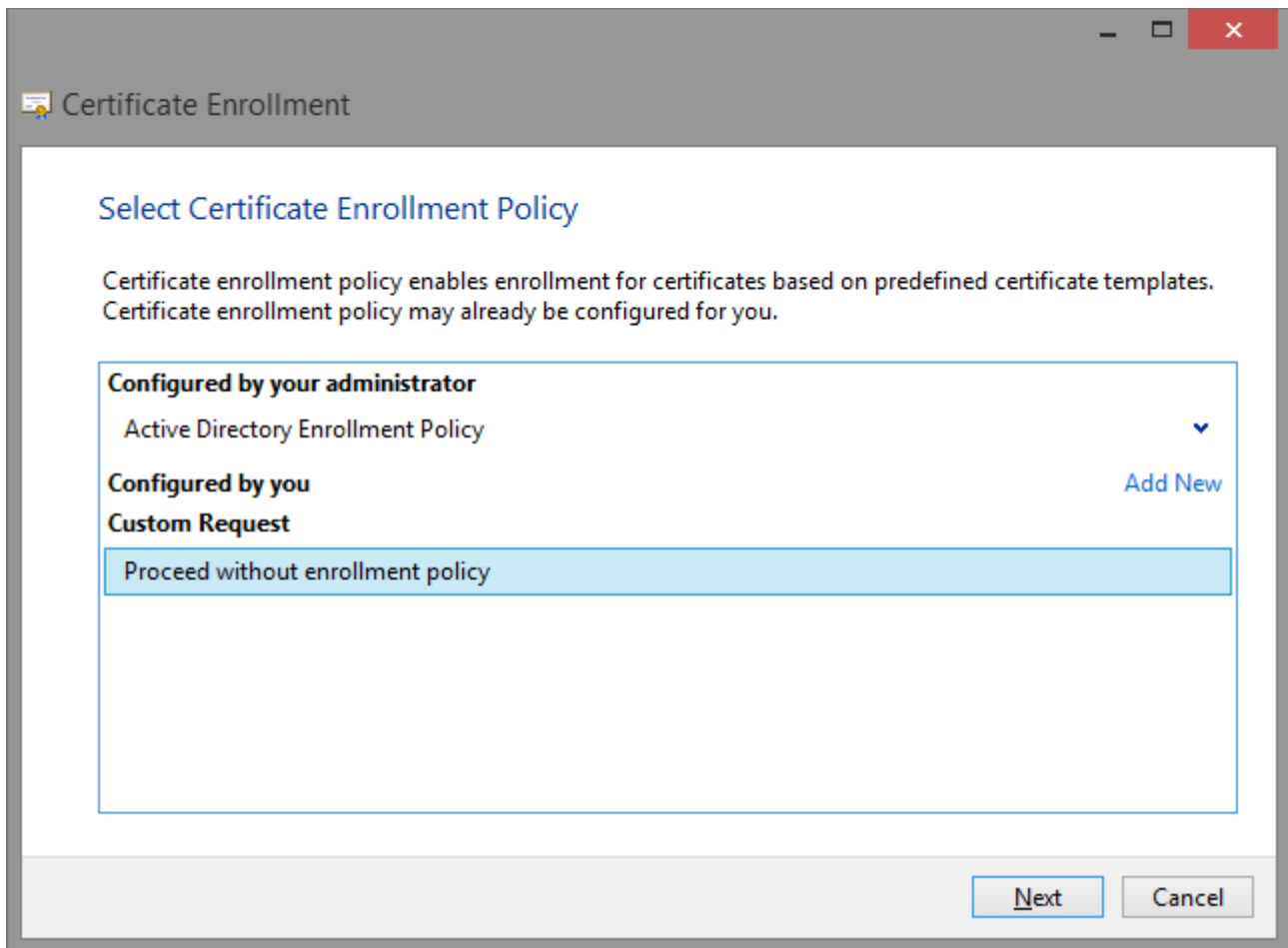
This option can be used to generate a Certificate Signing Request (CSR) on a hardware device like SafeNet/Aladdin eToken, Safenet iKey, Luna HSM. The resulting CSR is signed by the Root Certificate and the .CER response file is imported on the hardware device. The certificate hierarchy will be as follow:



Open *certmgr.msc* and select *Create Custom Request*, as below:

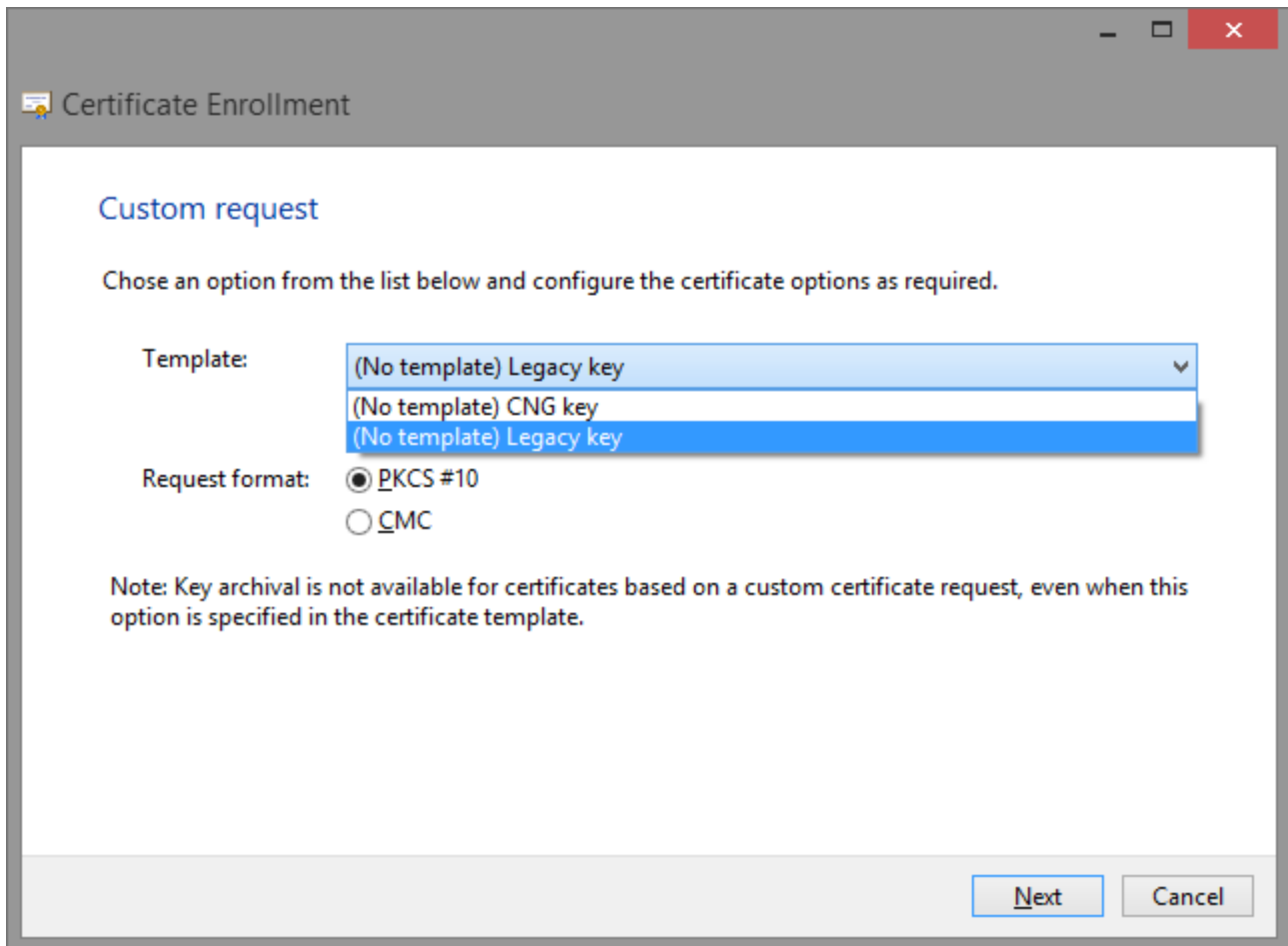


Select *Custom Request*.

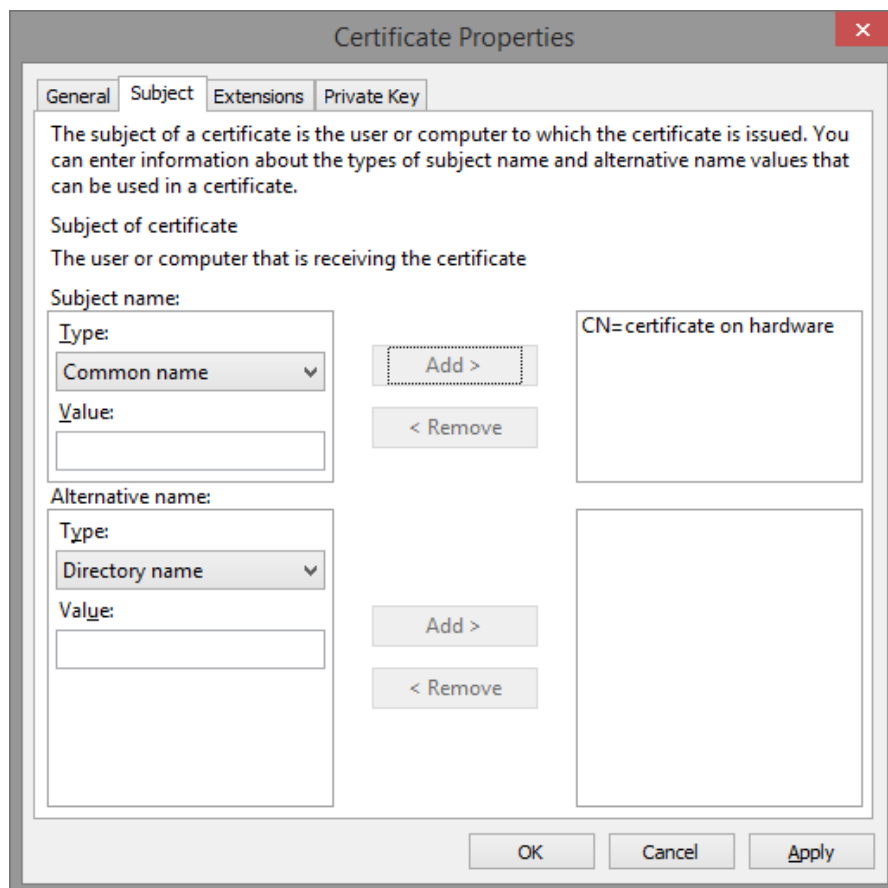
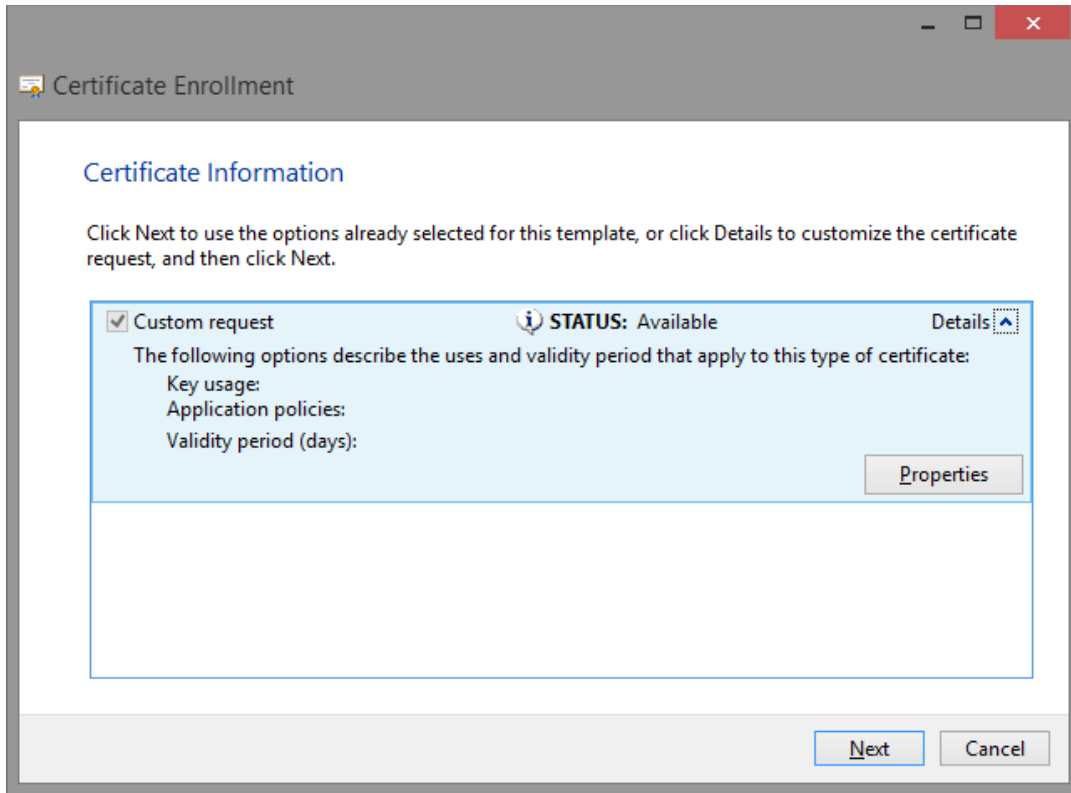


Select *Legacy Key*.

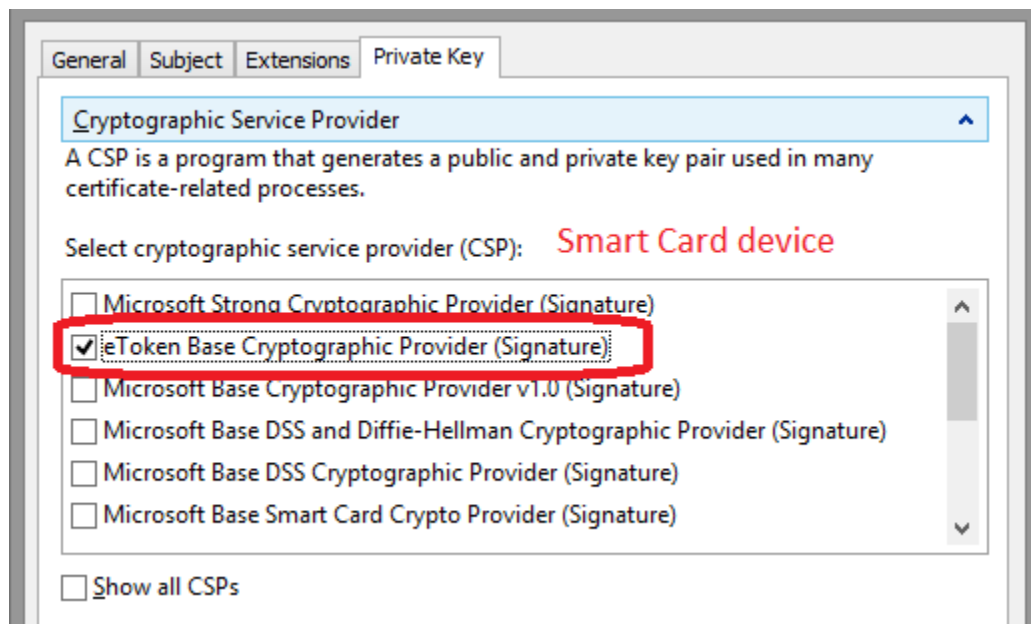
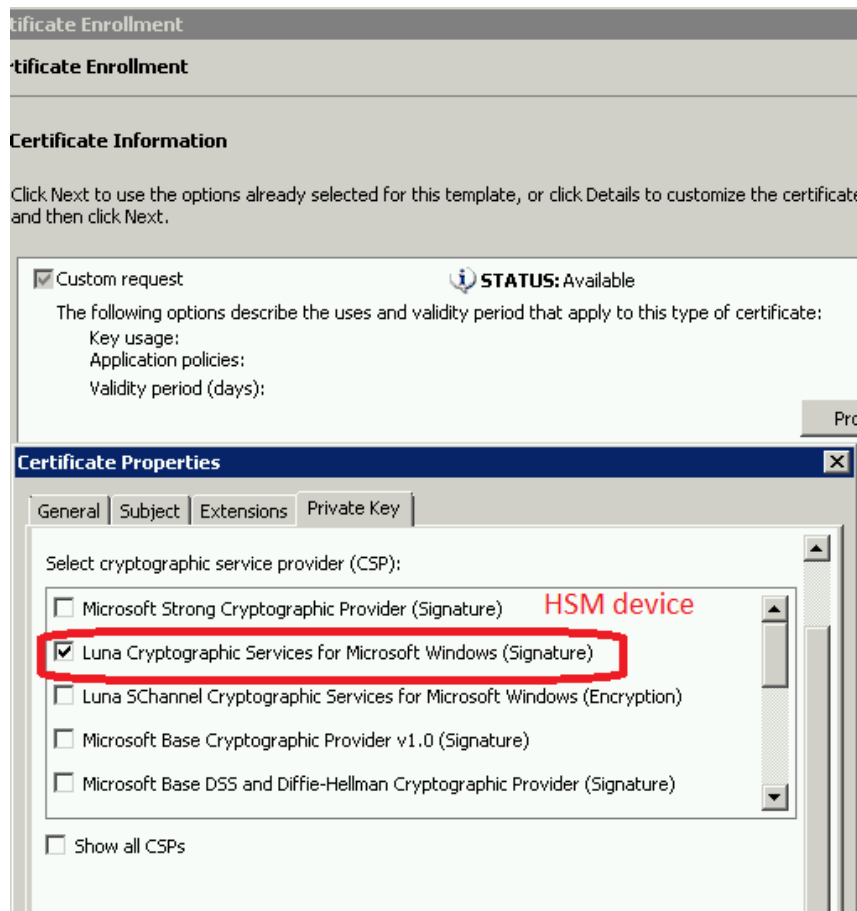
Important: Most of the third party applications and the Secure Soft products (CA Server, TSA Server, PDF Signer, P7S Signer) cannot use CNG (Cryptographic Next Generation) keys so a Legacy key must be created.



Customize the CSR by adding Common Name, extensions and other attributes.



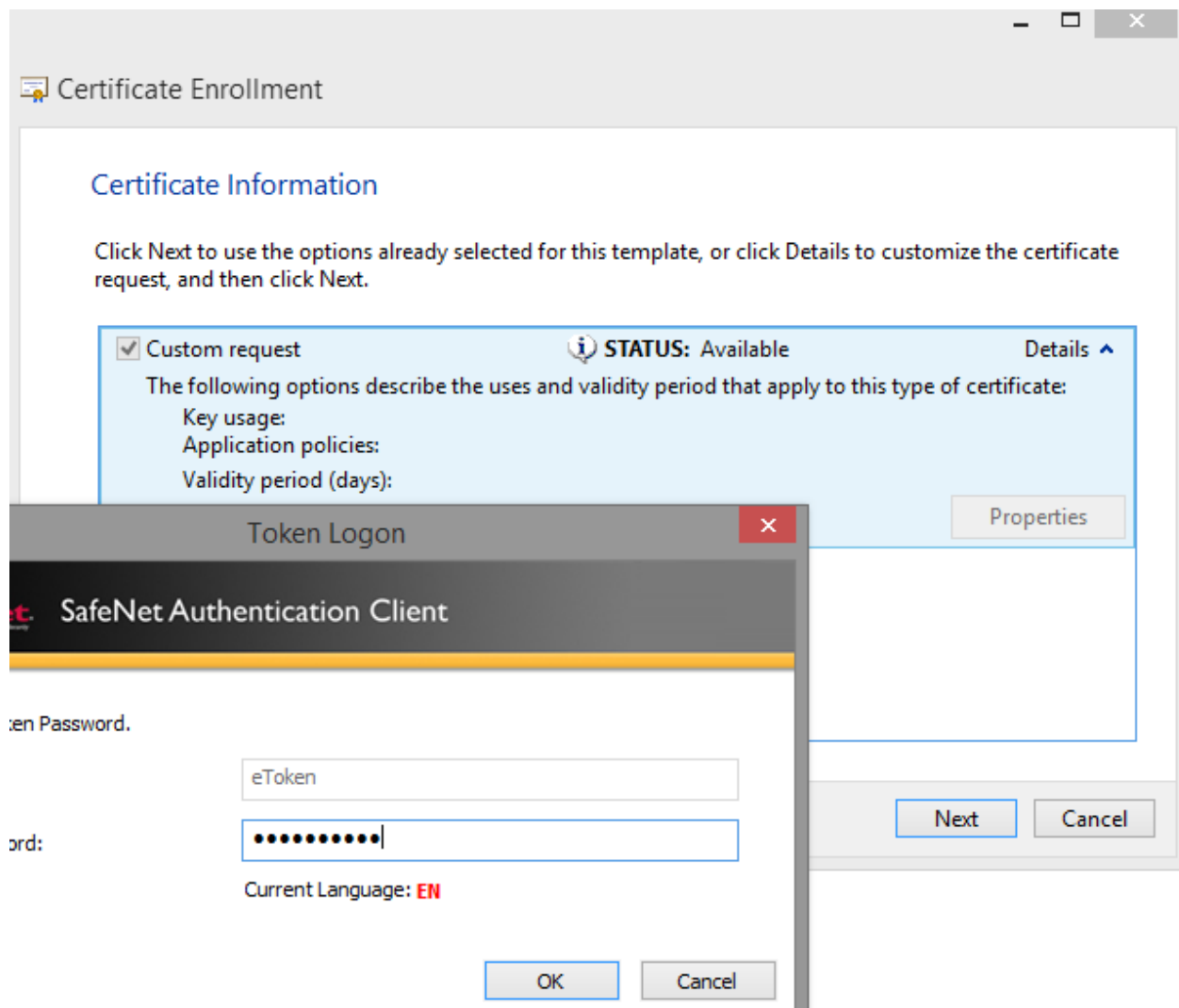
Select the Private Key container that can be a HSM device or a cryptographic smart card device:



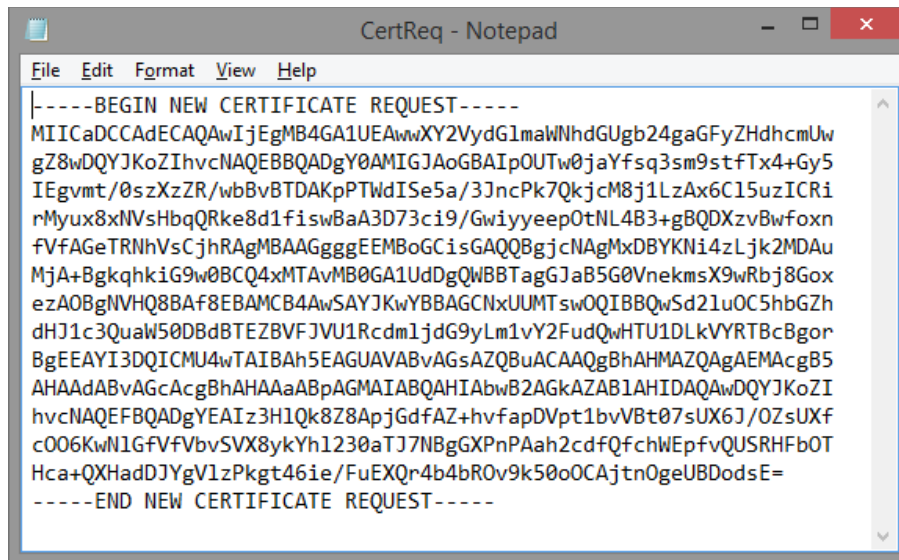
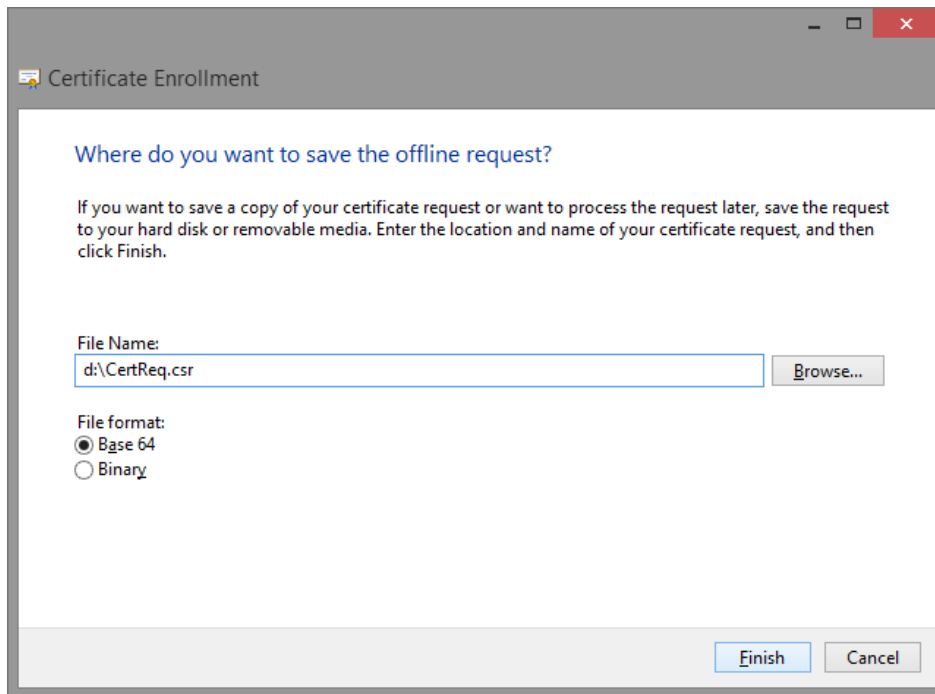
After the certificate request is customized and the private key container is selected, it can be created.

If the CSR is created on a smart card device, the device PIN must be entered.

If the CSR is created on a HSM device (like Luna HSM), the HSM credentials must be entered on the PED or console. More details about this can be found on the manuals offered by the HSM vendor.



When the process is finished, the resulting CSR file must be saved.



The CSR must be passed to the Certification Authority in order to be digitally signed by the Root CA.

-----BEGIN NEW CERTIFICATE REQUEST-----
MIICaDCCAdECAQAwIjEgMB4GA1UEAwwXY2VydG1maW5hdG9kb24gaGFyZWhhdcmUw
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAIP0UTw8jaYfsq3sm9stftx4+Gy5
IEgvmt/0szXzZR/wbBvBTDAKpP1Wd1Se5a/3JncPk7QkjcM811LzAx6C1SuzICRi
rMyux8xNVsHbqQRke8d1f1swBaA3D73ci9/Gwiyyeep0tNL4B3+gBQDXzvBwfoxn
fVfAGeTRNhVsC1hRAgMBAAGgggEEMBoGCisGAQQBgjcNAgMxDBYKNi4zLjk2MDAu
MjA+BgkqhkiG9w0BC04xMTAvMB0GA1UdDgQWBBTAgGJaB5G0VnekmsX9wRbj8Gox
ezAOBgNVHQ8BAF8EBAMCB4AwSAYJKwYBBAGCNxUUMTswOQIBBQwSd21uOC5hbGZh
dHJ1c3Quah50DBdBTEZBVFJVU1Rcdm1jdG9yLm1vY2FudQwHTU1DLkVYRTBcBgor
BgEEAYI3DQICMU4wTA1BAh5EAGUAVABvAGsAZQBuACAAQg8hAHMAZQAgAEMAcg85
AHAAdABvAGcAcg8hAHAAaABpAGMAIABQAHIAbwB2AGkAZAB1AHIDAQAwDQYJKoZI
hvcNAQEFBQADgYEA1z3H1Qk8Z8ApJGdFAZ+hvfapDVpt1bvVBt07sUX6J/OZsUXf
c006KwNIGFVfVbvSVX8ykYh1230aTJ7NBgGXPnPAah2cdFQfchwEpfvQUSRHFbOT
Hca+QXHadDJYgVlzPkg461e/FuEXQr4b4bR0v9k500CAjtn0geUBDodsE=
-----END NEW CERTIFICATE REQUEST-----

Certificate Template:

Certificate Validity Period:

Hashing Algorithm:

Revocation Password:

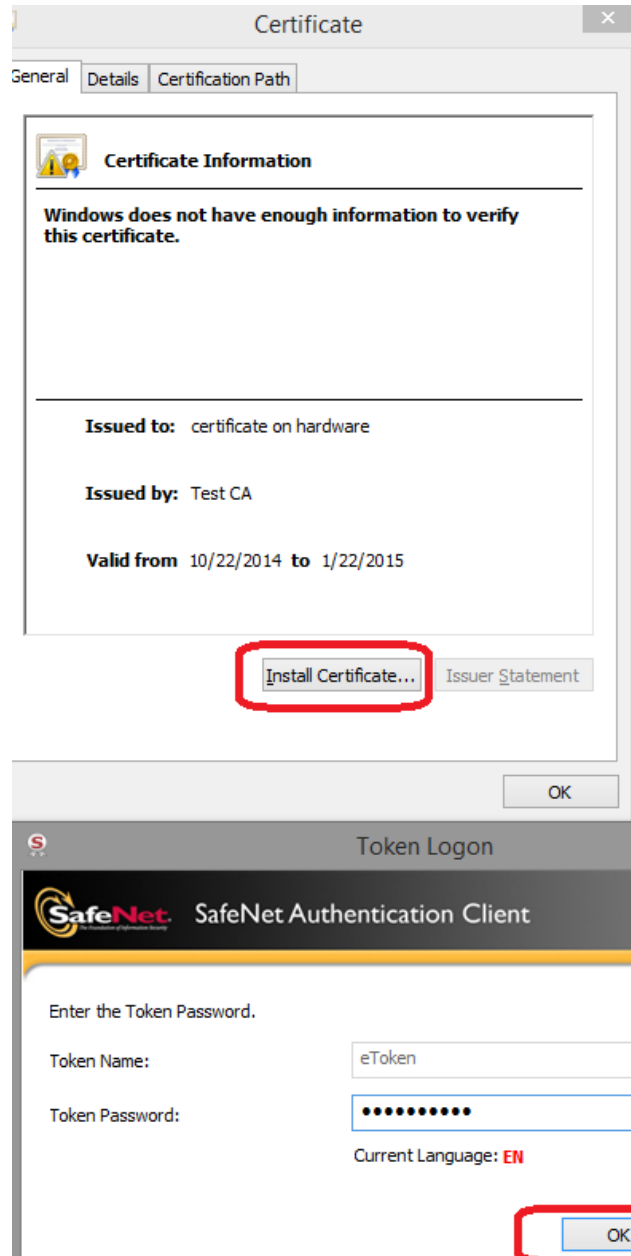
This certificate is issued from a CSR (Certificate Signing Request).

The CA will digitally sign the CSR resulting the .CER file. This .CER file must be copied on the same computer where the CSR was created on the same user account.

Open the .CER file and click install button.

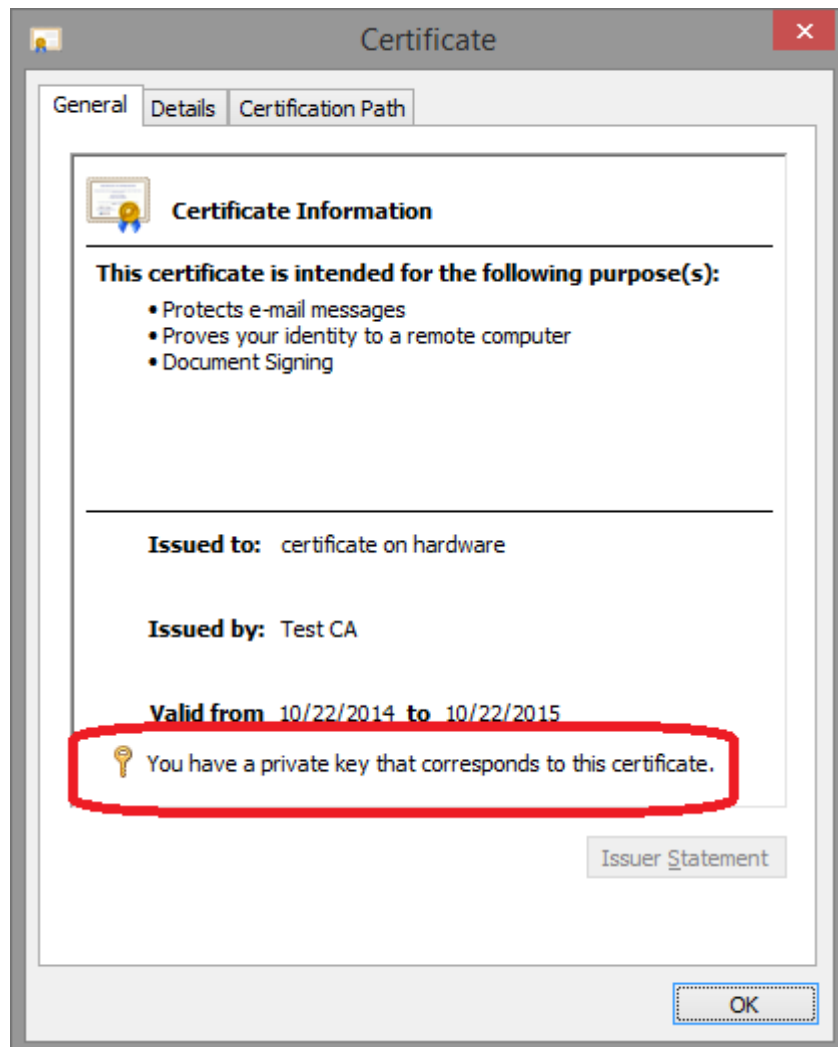
If the CSR is created on a smart card device, the device PIN must be entered.

If the CSR is created on a HSM device (like Luna HSM), the HSM credentials must be entered on the PED or console. More details about this can be found on the manuals offered by the HSM vendor.

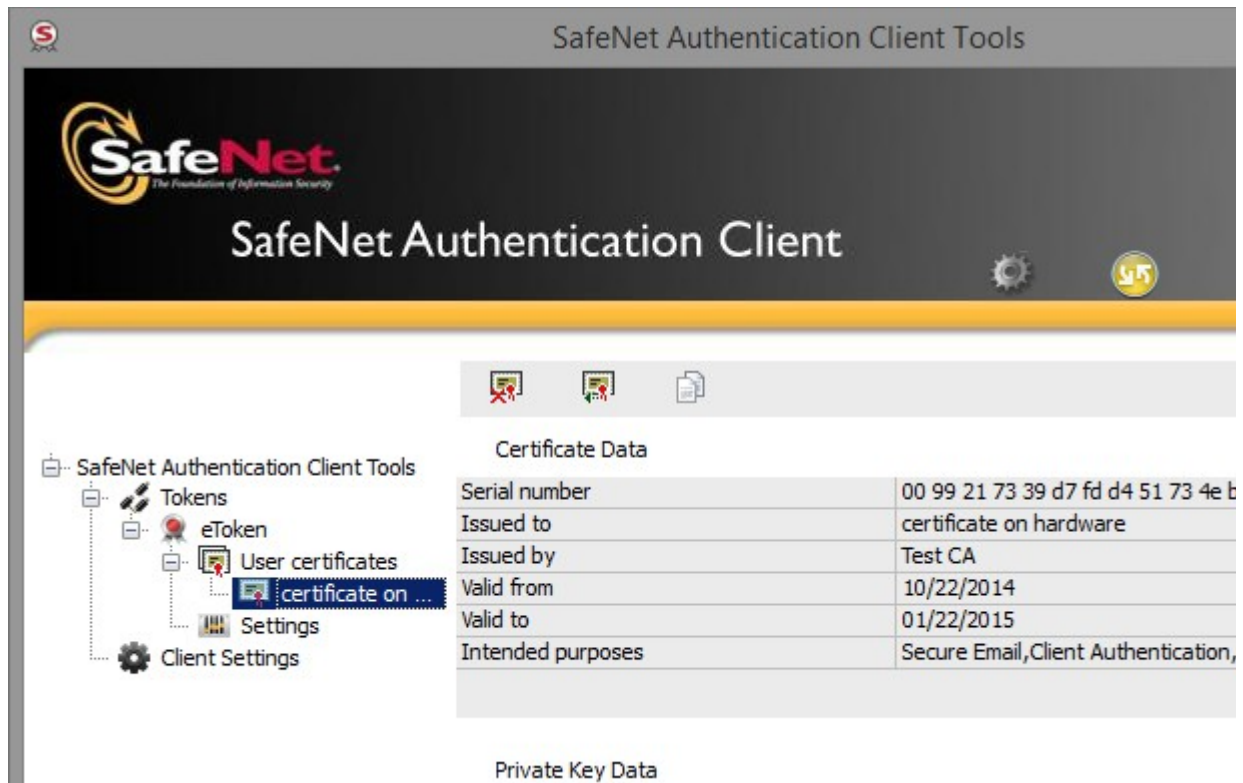


After the .CER certificate (public part) is installed on the device, the private key is now binded with the public part of the certificate resulting a fully functional certificate, as below.

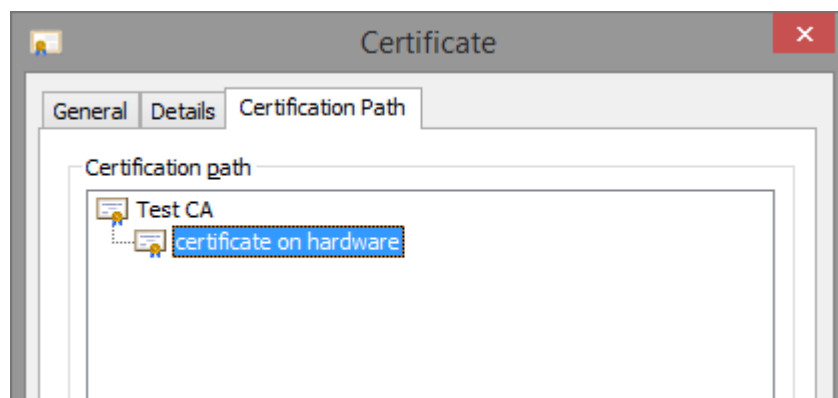
If the private key will not correctly bind with the public part (the message “*You have a private key that corresponds to this certificate*” not appear on the certificate window) you must do this manually. More information can be found on the product manual but a good start is to use *certutil - repairstore* (more details on [this article](#) or [this article](#)).



The certificate appears on the smart card device.



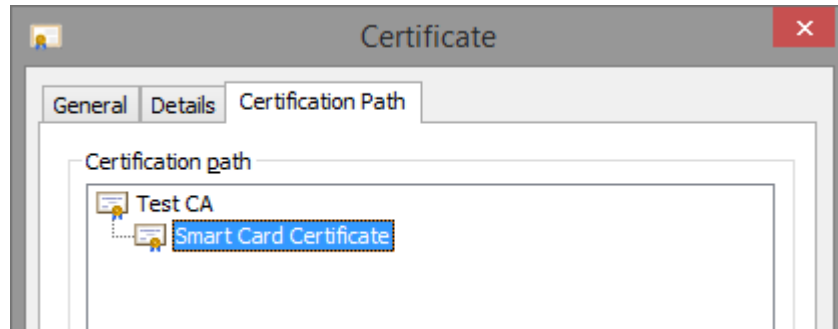
The certificate is ready to be used.



Generate a Certificate using Smart Card Generator

Download X.509 Digital Certificate Generator from here: <http://www.signfiles.com/x509-certificate-generator/>

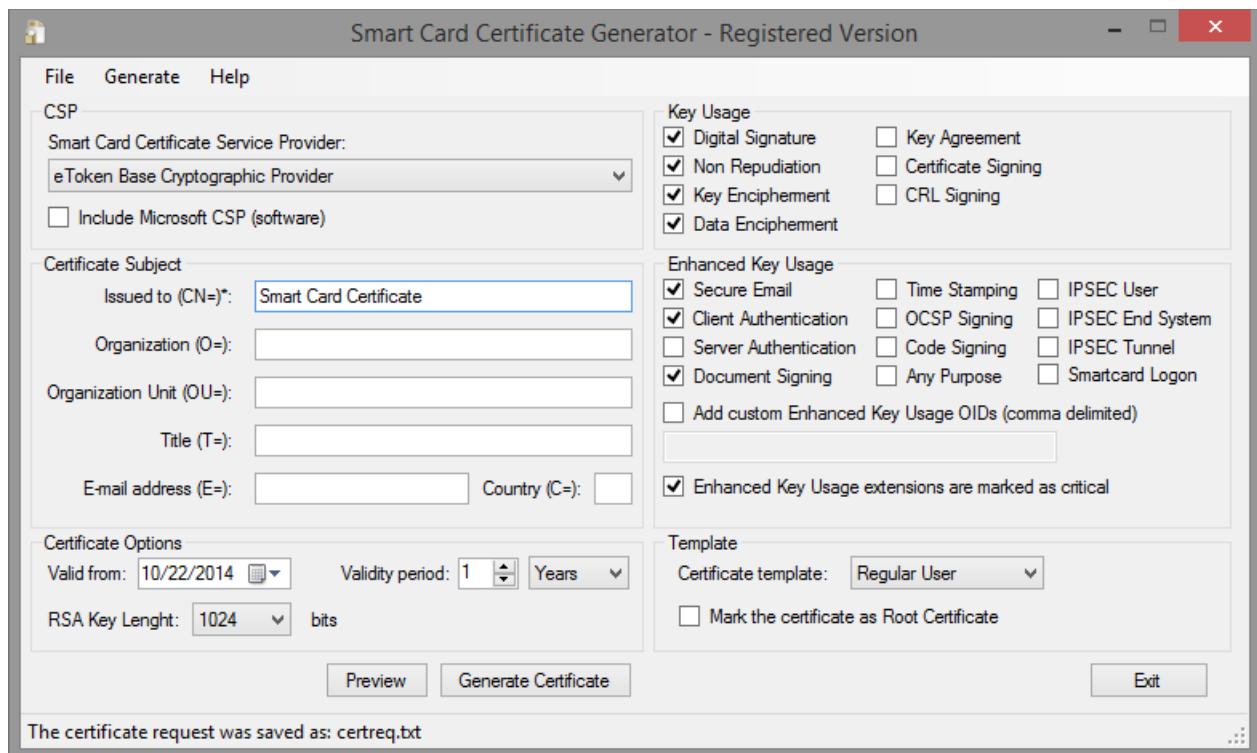
Smart Card Generator can be used to generate a Certificate Signing Request (CSR) on a hardware device like SafeNet/Aladdin eToken, Safenet iKey, Luna HSM. The resulting CSR is signed by the Root Certificate and the .CER response file is imported on the hardware device. The certificate hierarchy will be as follow:



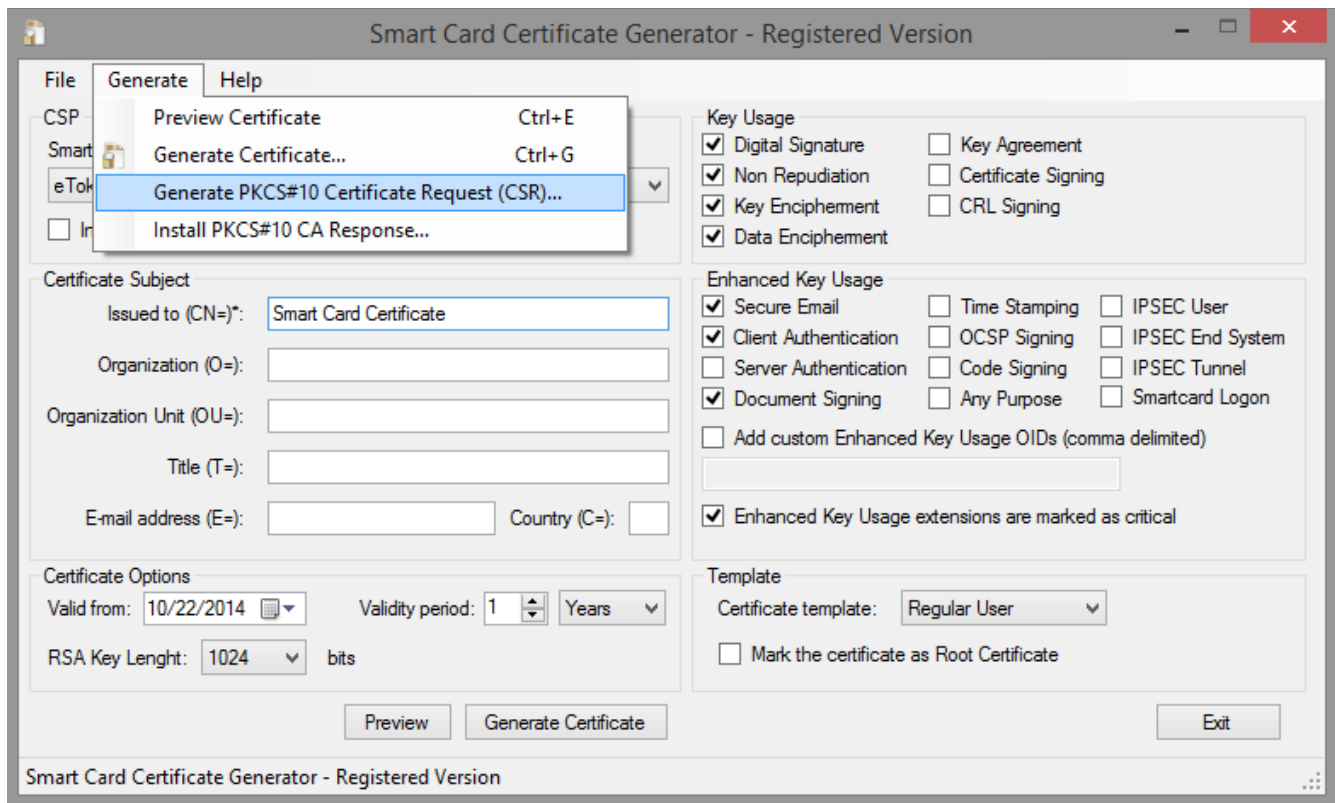
If the certificate is created on a smart card device, the device PIN must be entered.

If the certificate is created on a HSM device (like Luna HSM), the HSM credentials must be entered on the PED or console. More details about this can be found on the manuals offered by the HSM vendor.

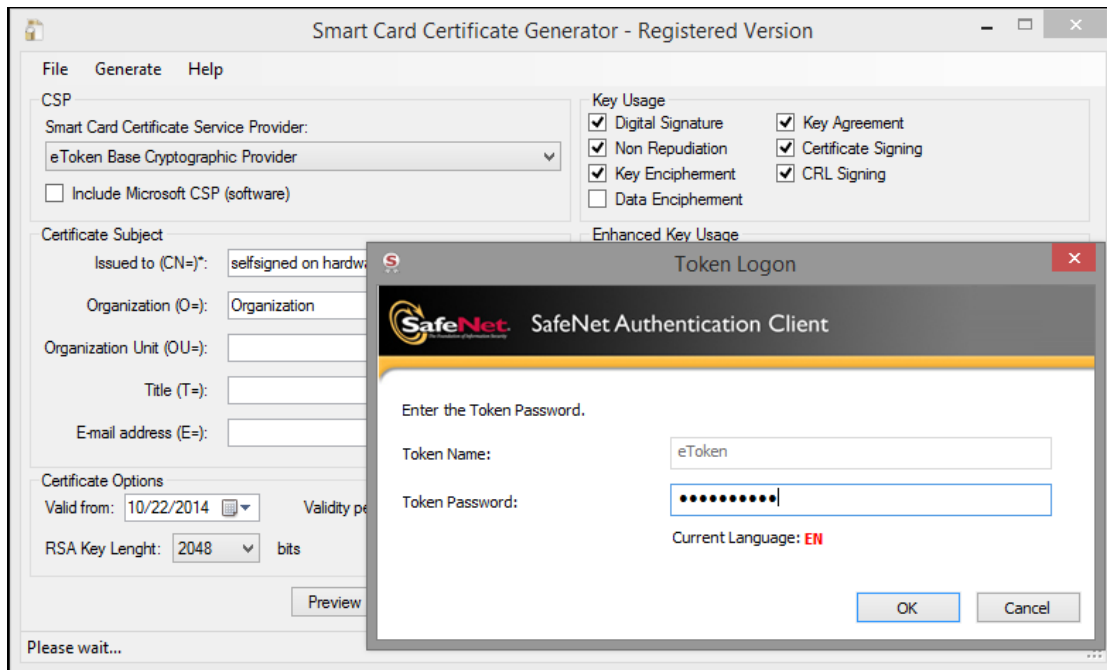
Note that this product will not work for all types of hardware devices and HSM's.



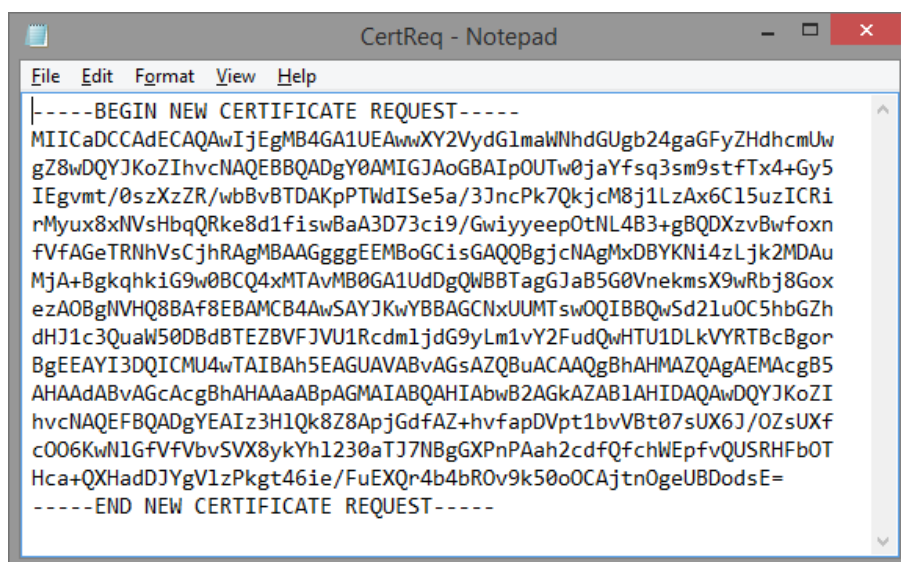
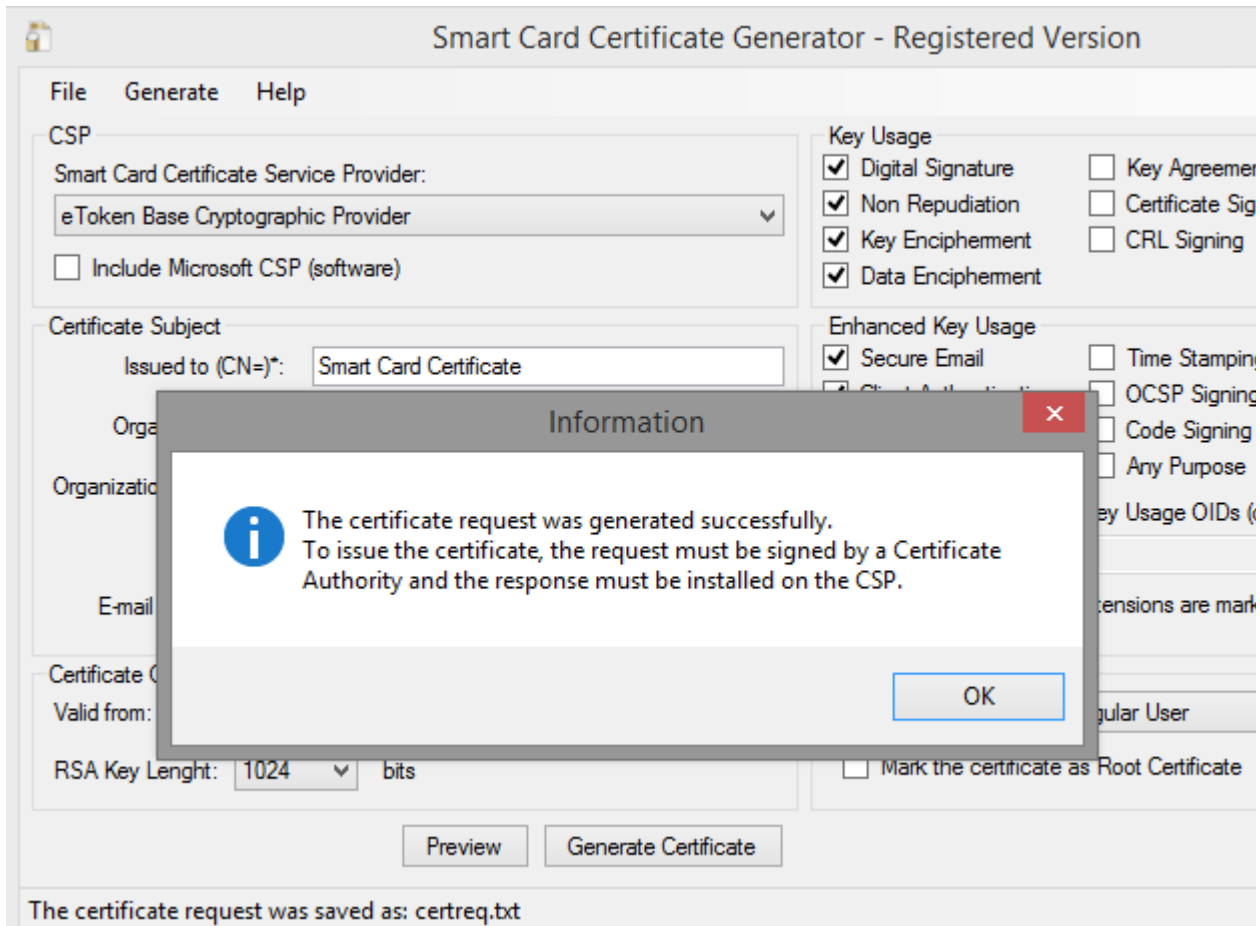
Choose *Generate PKCS#10 Certificate Request (CSR)* option:



If the certificate is created on a smart card device, the device PIN must be entered, as below:



The CSR is now issued and ready to be passed to the Certification Authority in order to be digitally signed.



The CSR must be passed to the Certification Authority in order to be digitally signed by the Root CA.

-----BEGIN NEW CERTIFICATE REQUEST-----
MIICADCCAdECAQAwIjEgMB4GA1UEAwY2VydG1maW5hdG9uZ24gaGFyZDhcmUw
gZ8wDOYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAIP0UTw0jaYfsq3sm9stftx4+Gy5
IEgVmt/0szXzZR/wbBvBTDAPtWdIse5a/3JncPk7QkjcM8j1LzAx6C15uzICRi
rMyux8xNVsHbqQRke8d1f1swBaA3D73ci9/GwiyyepOtNL4B3+gBQDXzvBwF0xn
fvfAGETRNhVscJhRAgMBAAGgggEEMBoGCisGA0QBgcNAgMxDBYKNI4zLjk2MDAu
MjA+BgkqhkiG9w0BCQ4xMTAvMB0GA1UdDgQWBBTagGJaB5G0VnekmsX9wRbj8Gox
eza0BgNVHQ8BAF8EBAMCB4AwSAYJKwYBAGCNxUUMTswOQIBBQw5d21uOC5hbGZ
dHJ1c3Quaw50DBdBTEZBVfJVU1Rcdm1jdG9yLm1vY2FudQwHTU1DLkVYRTBcBgor
BgEEAYI3DQICMU4wTAIBAh5EAGUAVABvAGsAZ0BuACAAQg8hAHMAZOAgAEMAcg85
AHAAdABvAGcAcg8hAAAAABPAGMAIABQAHIAbwB2AGkAZABIAHIDAQAwDOYJKoZI
hvcNAQEFBQADgYEAIZ3H10k8Z8ApjGdfAZ+hfapDVpt1bvVBt07sUX6J/OZsUXf
c006KwN1GFVfVbvSVX8ykYh1230aTJ7NBggXpNPAah2cdfQfchwEpfvQUSRHFb0T
Hca+OXHadDJYgV1zPkg46ie/FuEXQr4b4bROv9k50o0CAjtn0geUBDodsE=
-----END NEW CERTIFICATE REQUEST-----

Certificate Template:

Certificate Validity Period:

Hashing Algorithm:

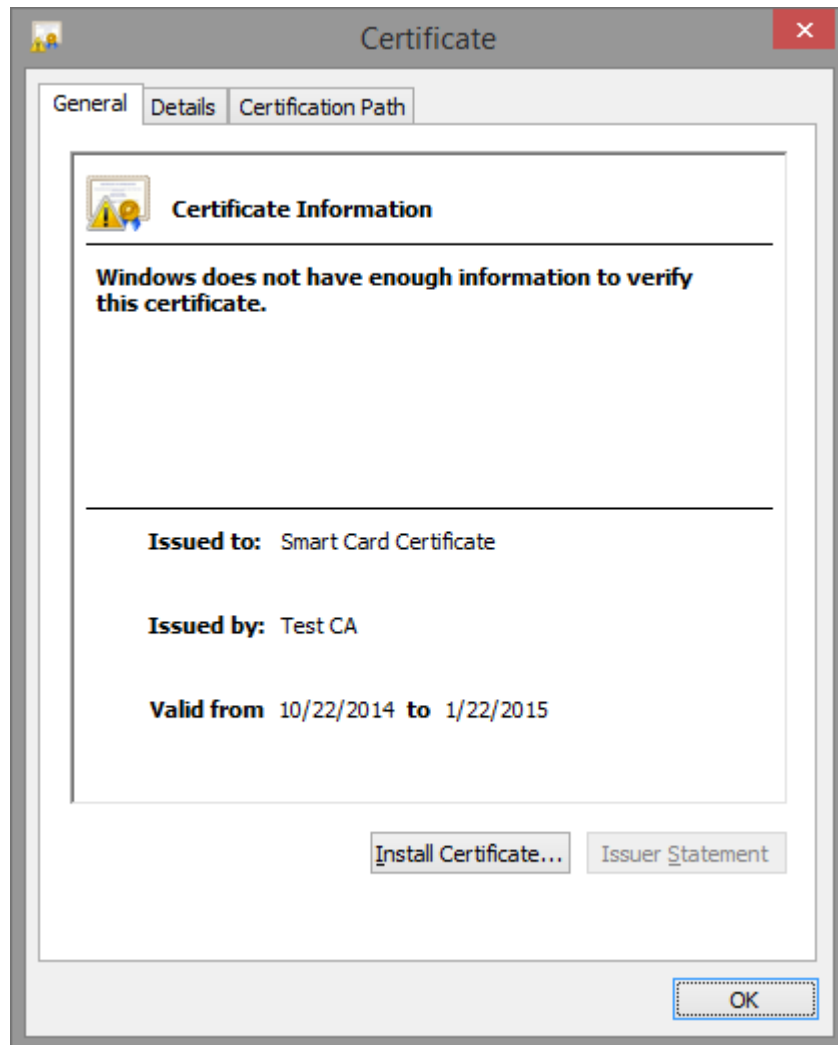
Revocation Password:

This certificate is issued from a CSR (Certificate Signing Request).

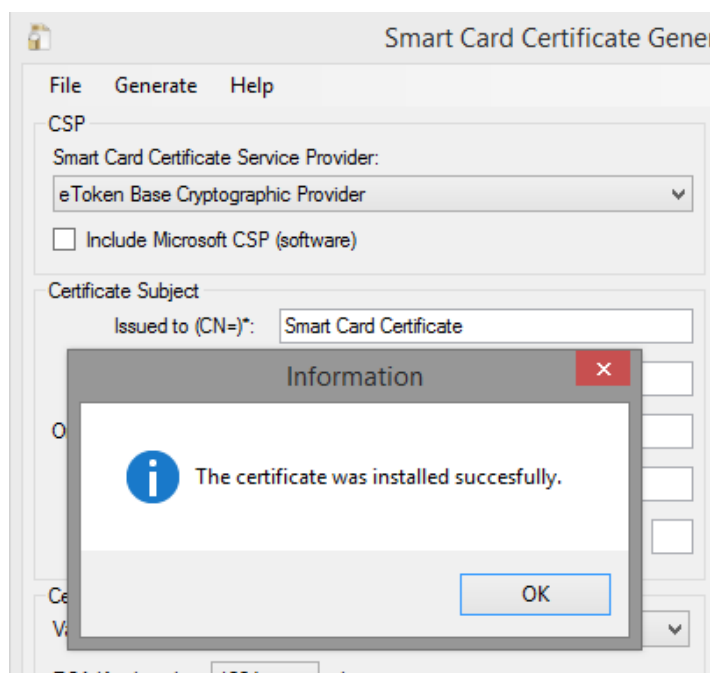
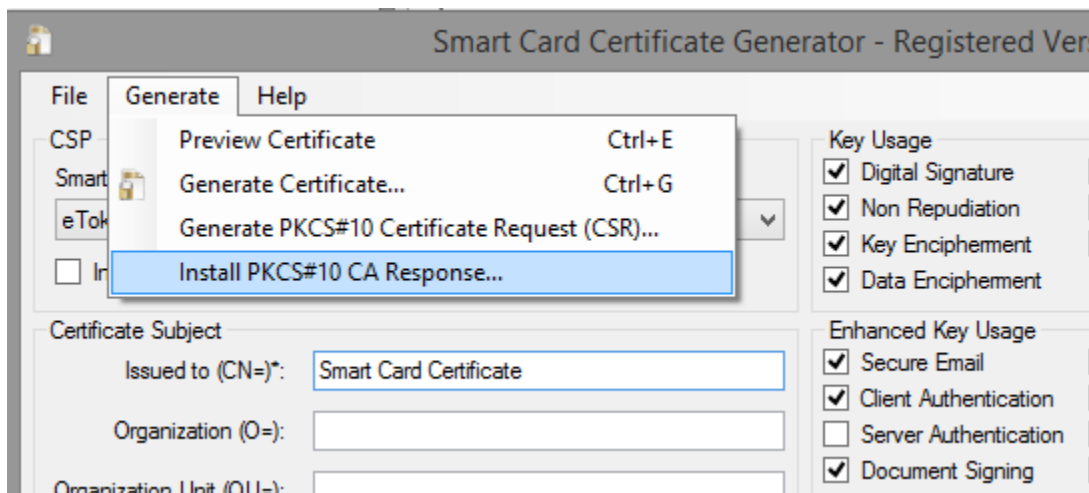
The CA will digitally sign the CSR resulting the .CER file. This .CER file must be copied on the same computer where the CSR was created on the same user account.

If the CSR is created on a smart card device, the device PIN must be entered.

If the CSR is created on a HSM device (like Luna HSM), the HSM credentials must be entered on the PED or console. More details about this can be found on the manuals offered by the HSM vendor.



Install the .CER file using *Install PCS#10 CA Response* option.



After the .CER certificate (public part) is installed on the device, the private key is now binded with the public part of the certificate resulting a fully functional certificate, as below.

If the private key will not correctly bind with the public part (the message “*You have a private key that corresponds to this certificate*” not appear on the certificate window) you must do this manually. More information can be foud on the product manual but a good start is to use *certutil - repairstore* (more details on [this article](#) or [this article](#)).

The certificate appears on the smart card device.

The screenshot displays the SafeNet Authentication Client interface. The top header features the SafeNet logo and the text "SafeNet Authentication Client". Below the header is a navigation pane on the left with the following items: "SafeNet Authentication Client Tools", "Tokens", "eToken", "User certificates", "Smart Card C...", "Settings", and "Client Settings". The "Smart Card C..." item is selected, and its details are shown in a table on the right.

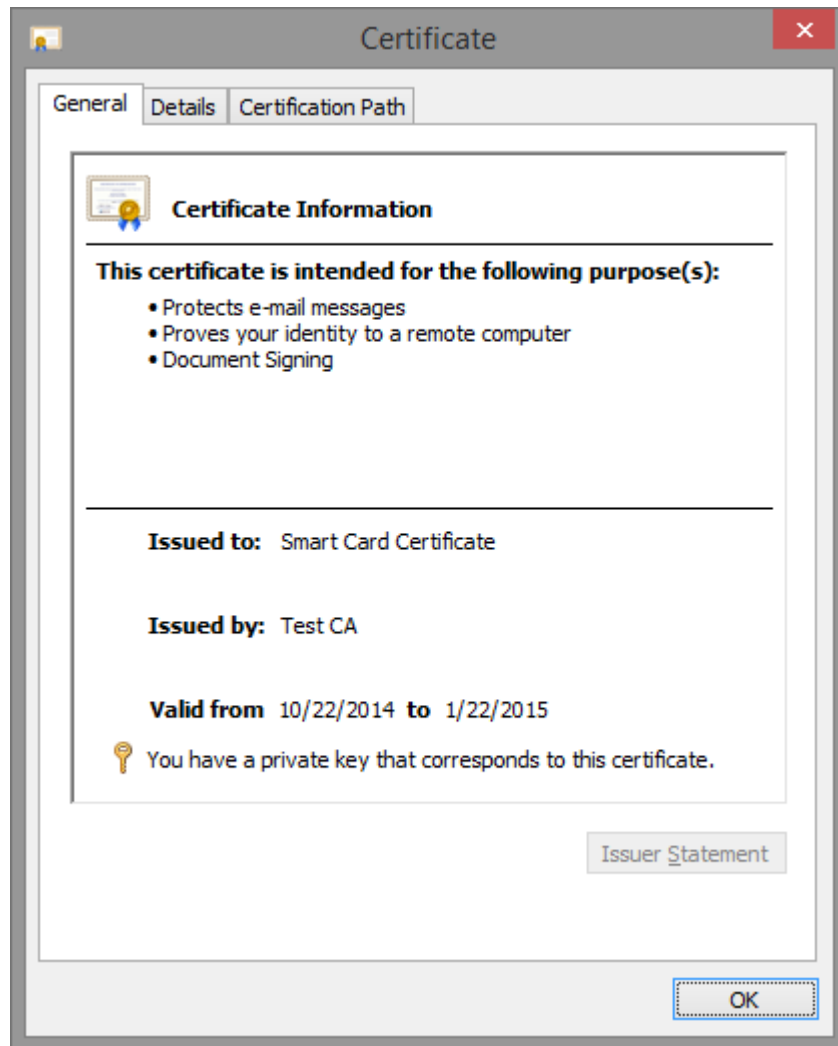
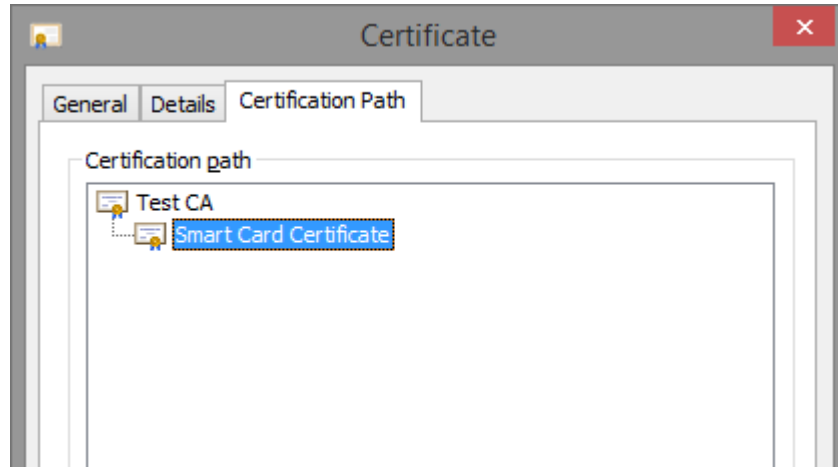
Certificate Data

Serial number	00 b1 93 f8 d8 72 d2 80 21 d1 bb e7 95
Issued to	Smart Card Certificate
Issued by	Test CA
Valid from	10/22/2014
Valid to	01/22/2015
Intended purposes	Secure Email, Client Authentication, Docu

Private Key Data

Key size	1024 bits
Container name	lp-521f4b8c-d9d7-43a7-b4a4-28e49fae
Modulus	82 2e c4 3f fe c0 68 c2 8b e4 d2 b6 db 9
Key specification	AT_KEYEXCHANGE
Default key container	Yes
Exportable	Yes

The certificate is ready to be used.



Generate a Self-Signed Certificate using Smart Card Generator

Download X.509 Digital Certificate Generator from here: <http://www.signfiles.com/x509-certificate-generator/>

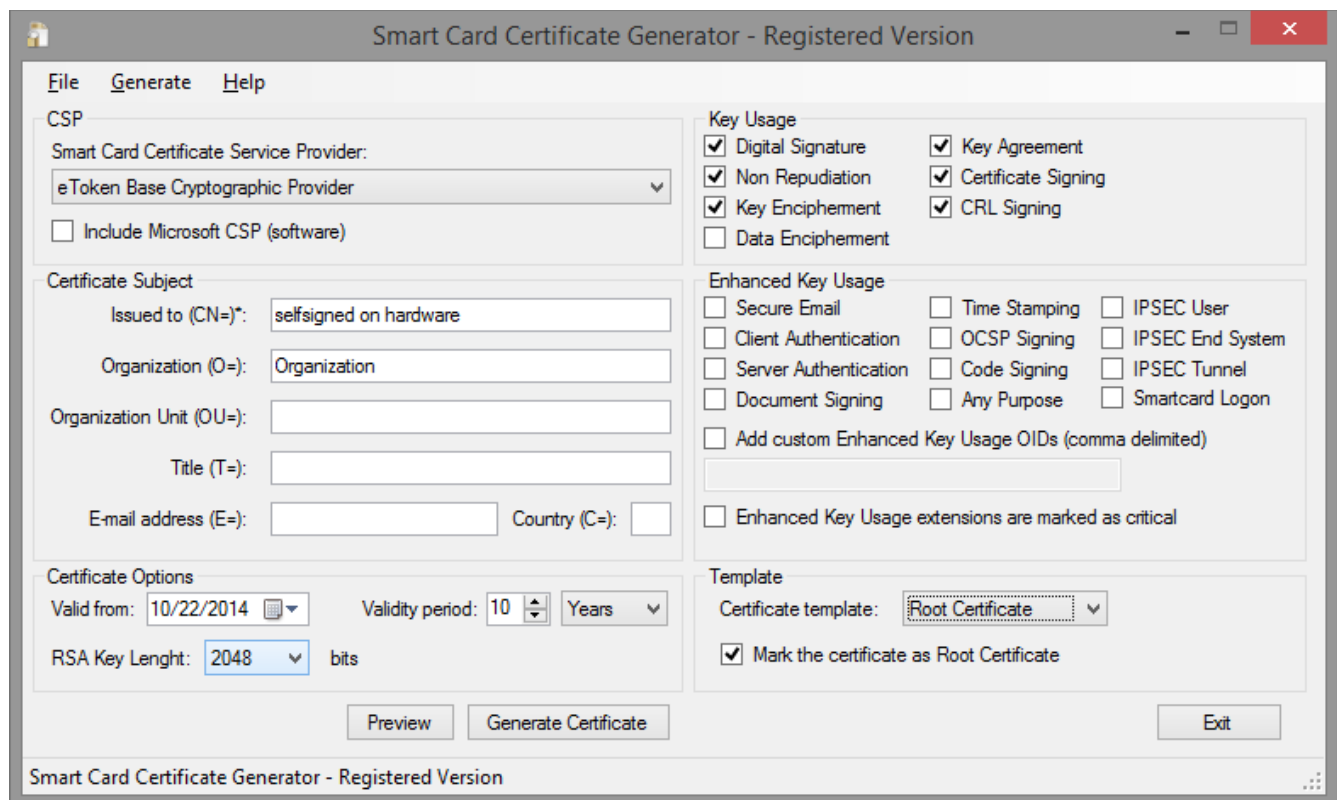
Start Smart Card Generator and make all necessary customizations.

This section is useful when you want to generate a Root CA Certificate directly on a hardware device.

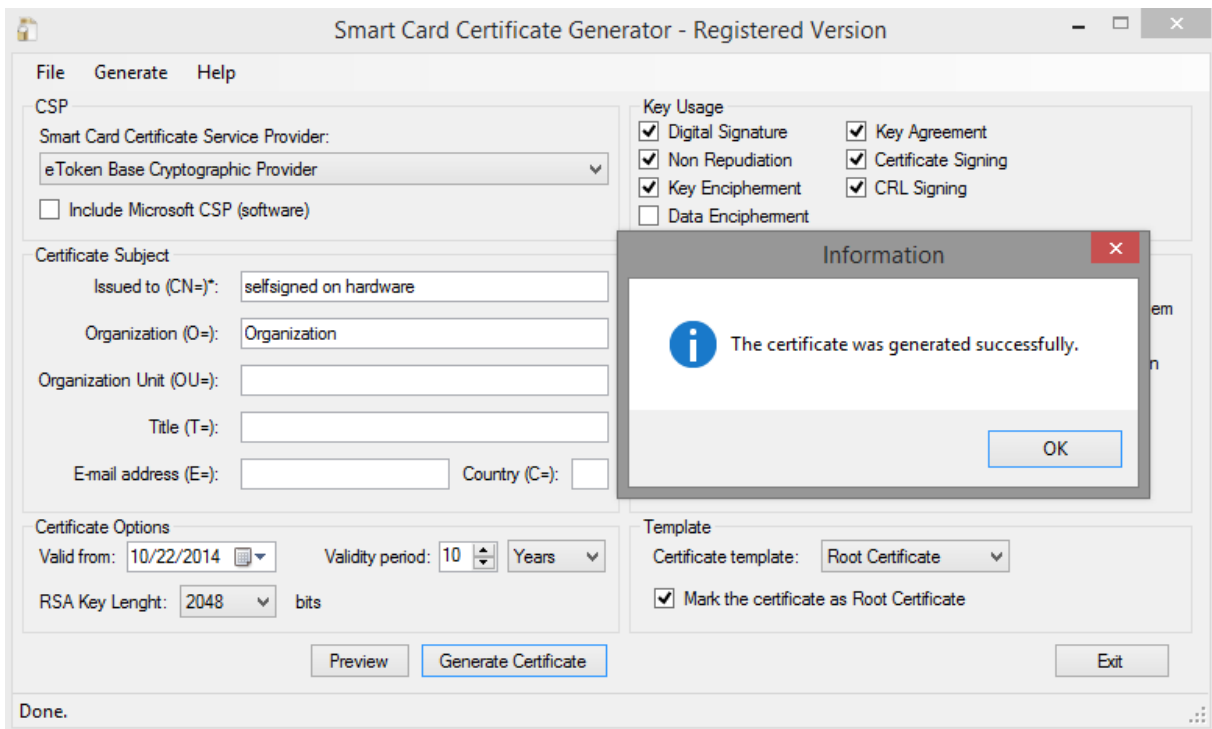
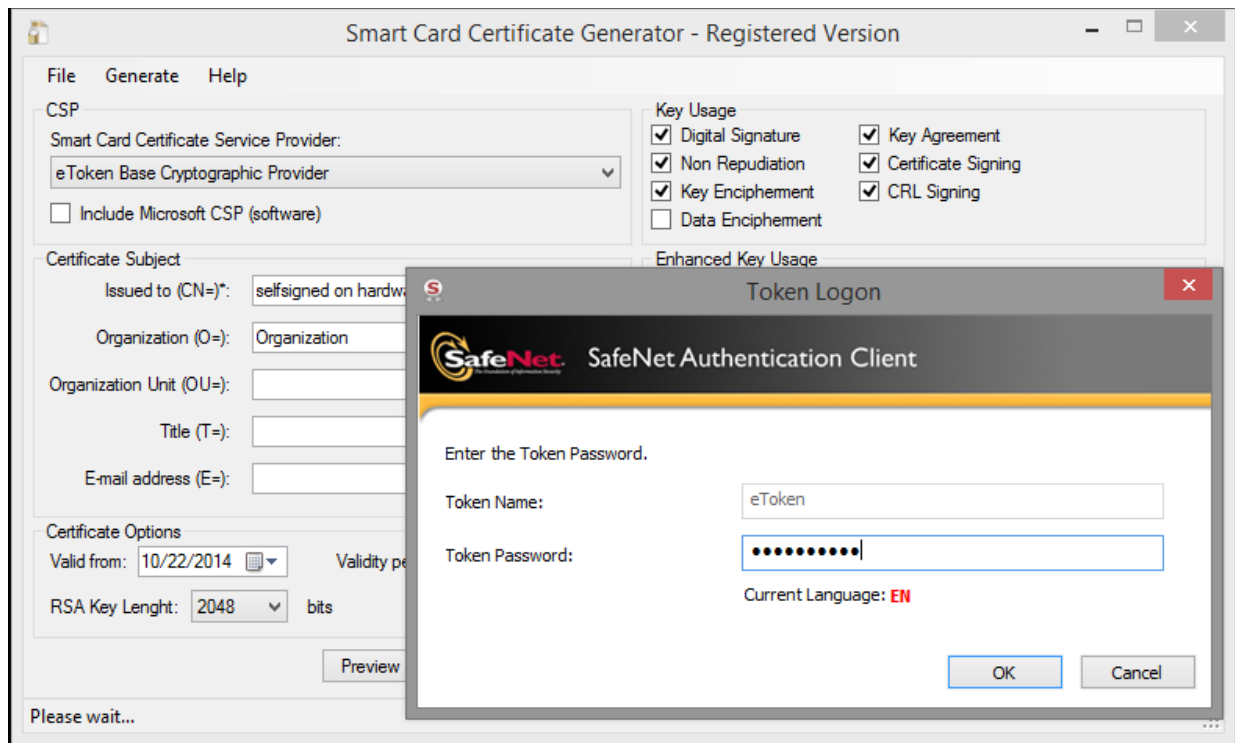
If the certificate is created on a smart card device, the device PIN must be entered.

If the certificate is created on a HSM device (like Luna HSM), the HSM credentials must be entered on the PED or console. More details about this can be found on the manuals offered by the HSM vendor.

Note that this product will not work for all types of hardware devices and HSM's.



If the certificate is created on a smart card device, the device PIN must be entered, as below:



The certificate is successfully created and ready to be used.

