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:

<i>1</i>		Run		×	
	Typ reso pen: ce	ee the name of a program, folder, d ource, and Windows will open it for rtmgr.msc	ocument, you.	or Internet	
		OK Cancel		<u>B</u> rowse	
Certificates - Current User	Issued 1	Fo State	sued By		Expiration Date
Personal Contification					
All Tasks	۱.	Request New Certificate		1	
Certific View	•	Import			
Enterprise		Advanced Operations	•	Create Custom	n Request
Intermedia Refresh	l			Enroll On Beha	of Of
Active Dire Export List				Manage Enroll	mont Policies
Instructed Help				Manage Enroll	ment Policies
Third-Party Root Certificatio	r	1			
Trusted People					

Select Custom Request.

rtificate Enrollment	
Select Certificate Enrollment Policy	
Certificate enrollment policy enables enrollment for certificate Certificate enrollment policy may already be configured for yo	es based on predefined certificate template
Configured by your administrator	
Active Directory Enrollment Policy	
Configured by you	Add N
Custom Request	
Proceed without enrollment policy	

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.

Certificate Enrollme	nt
Custom request	
Chose an option from	n the list below and configure the certificate options as required.
Template:	(No template) Legacy key 🗸 🗸 🗸
	(No template) CNG key
	(No template) Legacy key
Request format:	
	<u>○ <u>c</u>Mc</u>
Note: Key archival is option is specified in	not available for certificates based on a custom certificate request, even when this the certificate template.
	<u>N</u> ext Cancel

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

			- • ×
🗐 Cer	tificate Enrollment		
(Certificate Information		
(1	Click Next to use the options alr equest, and then click Next.	eady selected for this template, or click Details to custo	mize the certificate
	 Custom request 	③ STATUS: Available	Details 🔺
	The following options deso Key usage: Application policies: Validity period (days):	cribe the uses and validity period that apply to this type	of certificate: <u>Properties</u>
			Next Cancel

(Certificate Properties	×
General Subject Extensions Pr	rivate Key	
The subject of a certificate is the can enter information about the can be used in a certificate.	e user or computer to which the certificate is issued. You e types of subject name and alternative name values tha	J t
Subject of certificate The user or computer that is rec	ceiving the certificate	
Subject name:	-	
<u>Т</u> уре:	CN=certificate on hardware	
Common name 🛛 👻	Add >	
<u>V</u> alue:	< Remove	
Alternative name:		
Туре:		
Directory name 🗸 🗸 🗸		
Val <u>u</u> e:	Add >	
	< Remove	
	OK Cancel Apply	

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

tificate Enrollment
tificate Enrollment
Certificate Information Click Next to use the options already selected for this template, or click Details to customize the certificate and then click Next.
Custom request STATUS: Available The following options describe the uses and validity period that apply to this type of certificate: Key usage: Application policies: Validity period (days): Pro-
Certificate Properties
Select cryptographic service provider (CSP):
Luna Cryptographic Services for Microsoft Windows (Signature) Luna SChannel Cryptographic Services for Microsoft Windows (Encryption)
Microsoft Base DSS and Diffie-Hellman Cryptographic Provider (Signature)
Show all CSPs

General Subject Extensions Private Key		
Cryptographic Service Provider	^	
A CSP is a program that generates a public and private key pair used in many certificate-related processes.		
Select cryptographic service provider (CSP): Smart Card device		
Microsoft Strong Cryptographic Provider (Signature)	~	
EToken Base Cryptographic Provider (Signature)		
Microsoft Base Cryptographic Provider v1.0 (Signature)		
Microsoft Base DSS and Diffie-Hellman Cryptographic Provider (Signature)		
Microsoft Base DSS Cryptographic Provider (Signature)		
Microsoft Base Smart Card Crypto Provider (Signature)		

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.

			- 🗆 🛛 🕹
📮 Cer	tificate Enrollment		
(Certificate Information		
(1	Click Next to use the options already selected f request, and then click Next.	or this template, or click D	etails to customize the certificate
	✓ Custom request	i) STATUS: Available	Details 🔺
	The following options describe the uses a Key usage: Application policies: Validity period (days):	nd validity period that app	ily to this type of certificate:
	Token Logon	×	Properties
Saf	eNet Authentication Client		
Passwo	ord.		
	eToken		
l:	••••••		Next Cancel
	Current Language: EN		
	c	K Cancel	

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

	-		×
Certificate Enrollment			
Where do you want to save the offline request? If you want to save a copy of your certificate request or want to process the request later, to your hard disk or removable media. Enter the location and name of your certificate rec click Finish.	save the r juest, and	equest then	
File Name: d:\CertReq.csr	Brows	ie	
File format: ● B <u>a</u> se 64 ● Binar <u>y</u>			
Ein	ish	Cance	el

CertReq - Notepad - 🗖	x
<u>File Edit Fo</u> rmat <u>V</u> iew <u>H</u> elp	
BEGIN NEW CERTIFICATE REQUEST	~
MIICaDCCAdECAQAwIjEgMB4GA1UEAwwXY2VydG1maWNhdGUgb24gaGFyZHdhcmUw	
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAIpOUTw0jaYfsq3sm9stfTx4+Gy5	
IEgvmt/0szXzZR/wbBvBTDAKpPTWdISe5a/3JncPk7QkjcM8j1LzAx6C15uzICRi	
rMyux8xNVsHbqQRke8d1fiswBaA3D73ci9/GwiyyeepOtNL4B3+gBQDXzvBwfoxn	
fVfAGeTRNhVsCjhRAgMBAAGgggEEMBoGCisGAQQBgjcNAgMxDBYKNi4zLjk2MDAu	
MjA+BgkqhkiG9w0BCQ4xMTAvMB0GA1UdDgQWBBTagGJaB5G0VnekmsX9wRbj8Gox	
ezAOBgNVHQ8BAf8EBAMCB4AwSAYJKwYBBAGCNxUUMTswOQIBBQwSd21uOC5hbGZh	
dHJ1c3QuaW50DBdBTEZBVFJVU1Rcdm1jdG9yLm1vY2FudQwHTU1DLkVYRTBcBgor	
BgEEAYI3DQICMU4wTAIBAh5EAGUAVABvAGsAZQBuACAAQgBhAHMAZQAgAEMAcgB5	
AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZAB1AHIDAQAwDQYJKoZI	
hvcNAQEFBQADgYEAIz3H1Qk8Z8ApjGdfAZ+hvfapDVpt1bvVBt07sUX6J/0ZsUXf	
c006KwN1GfVfVbvSVX8ykYh1230aTJ7NBgGXPnPAah2cdfQfchWEpfvQUSRHFbOT	
Hca+QXHadDJYgVlzPkgt46ie/FuEXQr4b4bR0v9k50oOCAjtnOgeUBDodsE=	
END NEW CERTIFICATE REQUEST	
	\sim

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



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.

)	Certificate	×			
General Details Certification Path					
Certificate In	nformation	,			
this certificate.	nave enough information to verify				
Issued to:cer	rtificate on hardware				
Issued by: Tes	st CA				
Issued by: Test CA					
Valid from 10/22/2014 to 1/22/2015					
	Install Certificate				
	OK				
S	Token Logon				
GafeNet. Sa	afeNet Authentication Client				
Enter the Token Pass	word.				
Token Name:	eToken				
Token Password:	•••••				
	Current Language: EN				
		ОК			

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 <u>this article</u> or <u>this article</u>).



The certificate appears on the smart card device.

S	SafeNet Authentication	Client Tools
SafeNet A	uthentication Client	© 🕠
 SafeNet Authentication Client Tools Tokens Token EToken User certificates Certificate on Settings Client Settings 	Image: Certificate Data Certificate Data Serial number Issued to Issued by Valid from Valid to Intended purposes	00 99 21 73 39 d7 fd d4 51 73 4e b certificate on hardware Test CA 10/22/2014 01/22/2015 Secure Email,Client Authentication,

The certificate is ready to be used.

	Certificate	×
General Details	; Certification Path	
Certification p	2ath ificate on hardware	

Generate a Certificate using Smart Card Generator

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

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:

R	Certificate	×
General Details	Certification Path	
Certification particular Certification particular CA	ath t Card Certificate	

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.

👔 Smart Card Certificate Gene	rator - Registered Version 🛛 🗕 🗖 🗙
File Generate Help CSP Smart Card Certificate Service Provider: eToken Base Cryptographic Provider Include Microsoft CSP (software)	Key Usage Igital Signature Key Agreement Non Repudiation Certificate Signing Key Encipherment CRL Signing Data Encipherment CRL Signing
Certificate Subject Issued to (CN=)*: Smart Card Certificate Organization (O=): Organization Unit (OU=): Title (T=): E-mail address (E=): Country (C=):	Enhanced Key Usage ✓ Secure Email Time Stamping IPSEC User ✓ Client Authentication OCSP Signing IPSEC End System Server Authentication Code Signing IPSEC Tunnel ✓ Document Signing Any Purpose Smartcard Logon Add custom Enhanced Key Usage OIDs (comma delimited)
Certificate Options Valid from: 10/22/2014 Validity period: 1 Validit	Template Certificate template: Regular User v Mark the certificate as Root Certificate

Choose Generate PKCS#10 Certificate Re	equest (CSR) option:
----------------------------------------	----------------------

a	Smart Car	d Certificate G	Generator - Registered Version 🛛 🗕 🗖 🗙
File Ger	nerate Help		
CSP	Preview Certificate	Ctrl+E	Key Usage
Smart 🔐	Generate Certificate	Ctrl+G	✓ Digital Signature Key Agreement
eTok	Generate PKCS#10 Certificate Reques	st (CSR)	
	Install PKCS#10 CA Response		✓ Data Enciphement
Certificate S Issu	ubject ed to (CN=)*: Smart Card Certificate		Enhanced Key Usage ✓ Secure Email Time Stamping IPSEC User
Orga	nization (O=):		
Organizatio	n Unit (OU=):		Add custom Enhanced Key Usage OIDs (comma delimited)
	Title (T=):		
E-mail	address (E=):	Country (C=):	Enhanced Key Usage extensions are marked as critical
Certificate C	Options		Template
Valid from:	10/22/2014 Validity period:	1 🔹 Years	✓ Certificate template: Regular User ✓
RSA Key Lenght: 1024 V bits			Mark the certificate as Root Certificate
	Preview Generate Certificate Exit		
Smart Card (Certificate Generator - Registered Versio	on	

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

🖞 Smart	Card Certificate Generat	or - Registered Version	- 🗆 🗙
File Generate Help			
CSP Smart Card Certificate Service Provider: eToken Base Cryptographic Provider Include Microsoft CSP (software)		Key Usage Digital Signature Non Repudiation Key Enciphement Otate Enciphement	
Certificate Subject	E	Inhanced Key Usage	
Issued to (CN=)*: selfsigned on hardward	S	Token Logon	×
Organization (O=): Organization Organization Unit (OU=): Title (T=):	GafeNet. SafeNe	et Authentication Client	
	Enter the Token Password.		
E-mail address (E=):	Token Name:	eToken	
Certificate Options Valid from: 10/22/2014 v Validity pe RSA Key Lenght: 2048 v bits	Token Password:	••••••• Current Language: EN	
Preview		ОК	Cancel

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

 The second second	Smart Card Certificate Gene	erator - Registered Ve	rsion
File Generate Hel	p		
CSP		Key Usage	
Smart Card Certificate Ser	rvice Provider:	 Digital Signature Non Repudiation 	Certificate Sig
e Token Base Cryptograp	onic Provider V	Key Encipherment	CRL Signing
Include Microsoft CSI	P (software)	 Data Encipherment 	
Certificate Subject		Enhanced Key Usage	
Issued to (CN=)*:	Smart Card Certificate	Secure Email	Time Stamping
000	Information	×	
Orga	information		
Organizatio			
	The certificate request was generated successful The investment of the second successful	ully.	ey Usage OIDs (
	Authority and the response must be installed o	n the CSP.	
E-mail			ensions are mark
Certificate (
Valid from:		ОК	jular User
RSA Key Lenght: 1024	✓ bits	Mark the certificate a	s Root Certificate
	Preview Generate Certificate		
The certificate request wa	as saved as: certreq.txt		

🔲 CertReq - Notepad 🗕 🗖	×
<u>File Edit Format View H</u> elp	
BEGIN NEW CERTIFICATE REQUEST	\sim
MIICaDCCAdECAQAwIjEgMB4GA1UEAwwXY2VydG1maWNhdGUgb24gaGFyZHdhcmUw	
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAIpOUTw0jaYfsq3sm9stfTx4+Gy5	
IEgvmt/0szXzZR/wbBvBTDAKpPTWdISe5a/3JncPk7QkjcM8j1LzAx6Cl5uzICRi	
rMyux8xNVsHbqQRke8d1fiswBaA3D73ci9/GwiyyeepOtNL4B3+gBQDXzvBwfoxn	
fVfAGeTRNhVsCjhRAgMBAAGgggEEMBoGCisGAQQBgjcNAgMxDBYKNi4zLjk2MDAu	
MjA+BgkqhkiG9w0BCQ4xMTAvMB0GA1UdDgQWBBTagGJaB5G0VnekmsX9wRbj8Gox	
ezAOBgNVHQ8BAf8EBAMCB4AwSAYJKwYBBAGCNxUUMTswOQIBBQwSd21uOC5hbGZh	
dHJ1c3QuaW50DBdBTEZBVFJVU1RcdmljdG9yLm1vY2FudQwHTU1DLkVYRTBcBgor	
BgEEAYI3DQICMU4wTAIBAh5EAGUAVABvAGsAZQBuACAAQgBhAHMAZQAgAEMAcgB5	
AHAAdABvAGcAcgBhAHAAaABpAGMAIABQAHIAbwB2AGkAZAB1AHIDAQAwDQYJKoZI	
hvcNAQEFBQADgYEAIz3H1Qk8Z8ApjGdfAZ+hvfapDVpt1bvVBt07sUX6J/0ZsUXf	
c006KwN1GfVfVbvSVX8ykYh1230aTJ7NBgGXPnPAah2cdfQfchWEpfvQUSRHFbOT	
Hca+QXHadDJYgVlzPkgt46ie/FuEXQr4b4bROv9k50oOCAjtnOgeUBDodsE=	
END NEW CERTIFICATE REQUEST	
	\sim

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

	gntiles.com/ca/IssueFromCSR.asj
CA Server - Issue Use	er Certificate from CSR
ssue User Certificate from	CSR
BEGIN NEW CERTIFICATE REQU	JEST
MIICaDCCAdECAQAwIjEgMB4GA1UEAww	XY2VydGlmaWNhdGUgb24gaGFyZHdhcmUw
gZ8wDQVJKoZIhvcNAQEBBQADgY0AMIG	JAoGBAIpOUTw0jaYfsq3sm9stfTx4+Gy5
IEgvmt/0szXzZR/wbBvBTDAKpPTwdIS	je5a/3JncPk7QkjcM8j1LzAx6Cl5uzICRi
rMyux8xNVsHbqQRke8d1fiswBaA3D73	sci9/GwiyyeepOtNL4B3+gBQDXzvBwfoxn
fVfAGeTRNhVsCjhRAgMBAAGgggEEMBo	GGL5GAQQBgjcNAgMxDBYKNi4zLjk2MDAu
MjA+BgkqhkiG9w0BCQ4xMTAvMB0GA1U	JdDgQWBBTagGJaB5G0VnekmsX9wRbj8Gox
ezAOBgNVHQ8BAf8EBAMCB4AwSAYJKwY	(BBAGCNxUUMTswOQIBBQwSd21u0C5hbGZh
dHJIc3QuaWS0DBdBTEZBVFJVUIRcdml	LjdG9yLm1vY2FudQwHTUIDLKVYRTBcBgor
BgEEAYI3DQICMU4wTAIBAh5EAGUAVAB	NAGSAZOBuACAOogBbAHMAZOAgAEMacgB5
AHAAdABvAGcAcgBhAHAAaABpAGMAIAB	QAHIAbwB2AGKAZABIAHIDAQAwDQYJKoZI
hvcNAQEFBQADgYEAIz3H1Qk8Z8ApjGd	IfAZ+hyfapDVpt1bvVBt07sUX6J/QZsUXf
c0O6KwNlGfVfVbvSVX8ykYh1230aTJ7	NBgGXPnPAah2cdfQfchwEpfvQUSRHFbOT
Hca+QXHadDJYgVlzPkgt46ie/FuEXQr	4b4bR0v9k50oOCAjtnOgeUBDodsE=
END NEW CERTIFICATE REQUES	5T
AHAAdABvAGcAcgBhAHAAaABpAGMAIAB	QAHIAbwB2AGkAZAB1AHIDAQAwDQYJKoZI
hvcNAQEFBQADgYEAIz3H1Qk8Z8Ap1Gd	IfAZ+hvfapDVpt1bvVBt07sUX6J/Q2sUXf
c006KwNIGfVfVbvSVX8ykYh1230aT37	NBgGXPnPAah2cdfQfchwEpfvQUSRHFbQT
Hca+QXHadDJYgV1zPkgt46ie/FuEXQr	4b4bR0v9k50o0CAjtnOgeUBDodsE=
END NEW CERTIFICATE REQUES	ST
AHAAdABvAGcAcgBhAHAAaABpAGMAIAB	QAHIAbwB2AGkAZABIAHIDAQAwDQYJKoZI
hvcNAQEFBQADgYEAIz3H1Qk8Z8ApiGd	IfAZ+hyfapDVpt1bvVBt07sUX6J/QZsUXf
c006KwNIGfVfVbvSVX8ykYh1230aT37	NBgGXPnPAah2cdfQfchwEpfvQUSRHFbOT
Hca+QXHadD3YgV1zPkgt46ie/FuEXQr	4b4bR0v9k50oOCAjtnOgeUBDodsE=
END NEW CERTIFICATE REQUES	iT
Certificate Template:	User Certificate
Certificate Validity Period:	3 Months T
AHAAdABVAGCAcgBhAHAAaABPAGMATAB hvcNAQEFBQADgYEAIz3H1Qk8Z8Ap1Gd c006KwN1GfVfVbvSVX8ykYh1230aT37 Hca+QXHadD3YgV1zPkgt46ie/FuEXQr END NEW CERTIFICATE REQUES Certificate Template: Certificate Validity Period: Hashing Algorithm:	QAHIAbwB2AGkAZABIAHIDAQAwDQYJKoZI IfAZ+hvfapDVptlbvVBt07sUX6J/QZsUXf NBgGXPnPAah2cdfQfchWEpfvQUSRHFbOT Ab4bR0v9k50oOCAjtnOgeUBDodsE= ST 3 Months T SHA1 T

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.

	Certificate	×
General Details (Certification Path	_
Certifi	cate Information	
Windows doe this certificat	s not have enough information to verify e.	
Issued to	: Smart Card Certificate	
Issued b	y: Test CA	
Valid fro	m 10/22/2014 to 1/22/2015	
	Install Certificate Issuer Statement	
	OK	

a	Smart Card Certificate Generator - Registered Ver
File Ger	erate Help
-CSP -	Preview Certificate Ctrl+E Key Usage
Smart 🚰	Generate Certificate Ctrl+G Digital Signature
eTok	Generate PKCS#10 Certificate Request (CSR)
	Install PKCS#10 CA Response
Certificate S	ubject Enhanced Key Usage
Issu	ed to (CN=)*: Smart Card Certificate
0.000	✓ Client Authentication
Olga	
Organizatio	Init (OII=)
	Smart Card Certificate General File Generate Help CSP Smart Card Certificate Service Provider:
	e Token Base Cryptographic Provider 🗸 🗸
	Include Microsoft CSP (software)
	Certificate Subject
	Issued to (CN=)*: Smart Card Certificate
	Information
	O The certificate was installed succesfully.

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 certuil - repairstore (more details on this article or this article).

The certificate appears on the smart card device.

Client Settings



Private Key Data

Intended purposes

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
Accellance losses and alterna	M

Secure Email, Client Authentication, Docu

The certificate is ready to be used.

	Certi	ficate	×
General Details	Certification Path		
Certification <u>p</u> a	ith		- 1
Test CA	Card Certificate		

	Certificate	×
General	Details Certification Path	
	Certificate Information	
Thi	 s certificate is intended for the following purpose(s): Protects e-mail messages Proves your identity to a remote computer Document Signing 	
-	Issued to: Smart Card Certificate	
	Issued by: Test CA	
	Valid from 10/22/2014 to 1/22/2015	
9	You have a private key that corresponds to this certificate.	
	Issuer <u>S</u> tatement	
	ОК	

Generate a Self-Signed Certificate using Smart Card Generator

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

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.

🕆 Smart Card Certificate Gene	rator - Registered Version 🛛 🗕 🗖 🗙
<u>F</u> ile <u>G</u> enerate <u>H</u> elp	
CSP Smart Card Certificate Service Provider: e Token Base Cryptographic Provider v	Key Usage Digital Signature Non Repudiation Key Enciphement CRL Signing
Include Microsoft CSP (software)	Data Encipherment
Certificate Subject Issued to (CN=)*: selfsigned on hardware	Enhanced Key Usage Secure Email Client Authentication OCSP Signing UPSEC End System
Organization (O=): Organization	Server Authentication Code Signing IPSEC Tunnel Document Signing Any Purpose Smartcard Logon
Title (T=):	Add custom Enhanced Key Usage OIDs (comma delimited)
E-mail address (E=): Country (C=):	Enhanced Key Usage extensions are marked as critical
Certificate Options	Template
Valid from: 10/22/2014 🔍 Validity period: 10 🖨 Years 🗸	Certificate template: Root Certificate
RSA Key Lenght: 2048 v bits	✓ Mark the certificate as Root Certificate
Preview Generate Certificate	Exit
Smart Card Certificate Generator - Registered Version	

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

Smart S	Card Certificate Gene	rator - Registered Version	- 🗆 🗙
File Generate Help			
CSP Smart Card Certificate Service Provider: eToken Base Cryptographic Provider Include Microsoft CSP (software)	~	Key Usage Digital Signature Non Repudiation Key Agreement Key Encipherment Data Encipherment	
Certificate Subject		Enhanced Key Usage	
Issued to (CN=)*: selfsigned on hardwa	S	Token Logon	×
Organization (O=): Organization Organization Unit (OU=):	GafeNet. Safe	Net Authentication Client	
Title (T=):	Enter the Token Passwor	d.	
	Token Name:	eToken	
Certificate Options Valid from: 10/22/2014 ₪▼ Validity p∉ RSA Key Lenght: 2048 ∨ bits	Token Password:	Current Language: EN	
Preview Please wait		ОК	Cancel

Smart Card Certificate Gene	erator - Registered Version 🛛 🗕 🗆 🗙
File Generate Help	
CSP Smart Card Certificate Service Provider:	Key Usage ✓ Digital Signature ✓ Non Repudiation ✓ Non Repudiation
Include Microsoft CSP (software)	Key Encipherment CRL Signing Data Encipherment
Certificate Subject	Information
Issued to (CN=)*: selfsigned on hardware Organization (O=): Organization Organization Unit (OU=): Title (T=):	The certificate was generated successfully.
E-mail address (E=): Country (C=):	ОК
Certificate Options	Template
Valid from: 10/22/2014	Certificate template: Root Certificate V
RSA Key Lenght: 2048 V bits	✓ Mark the certificate as Root Certificate
Preview Generate Certificate	Exit
Done.	

The certificate is successfully created and ready to be used.

	Certificate	×	
Gene	ral Details Certification Path		
	Certificate Information		
	This certificate is intended for the following purpose(s): All issuance policies All application policies 		
-	Issued to: selfsigned on hardware		
	Issued by: selfsigned on hardware		
ш.	Valid from 10/22/2014 to 10/22/2024		
	You have a private key that corresponds to this certificate.		
	Issuer <u>S</u> tatement		
	ОК		

🔽 Ce	ertificate	×		
General Details Certification Par	th			
Show: <all></all>	~			
Field	Value	•		
Subject Public key Subject Key Identifier	selfsigned on hardware, Orga RSA (2048 Bits) 1f 64 80 37 89 a7 10 9a cb 09			
Key Usage	Digital Signature, Non-Repudia			
Basic Constraints	Subject Type=CA, Path Lengt sha1			
Thumbprint	0a c5 28 26 79 00 08 f1 c7 e1 🗸	,		
Digital Signature, Non-Repudiation, Key Encipherment, Key Agreement, Certificate Signing, Off-line CRL Signing, CRL Signing (ee)				
	ОК			