X.509 Certificate Generator User Manual

Introduction

X.509 Certificate Generator is a tool that allows you to generate digital certificates in PFX format, on Microsoft Certificate Store or directly on your cryptographic smart card.

X.509 Certificate Generator contains two main applications:

- **PFX Certificate Generator** – this application can be used when it is necessary to issue digital certificates in PFX format.
- **Smart Card Certificate Generator** – this tool is useful when the certificate must be generated directly on your smart card.

Links

X.509 Certificate Generator main page:
http://www.signfiles.com/x509-certificate-generator/

Download X.509 Certificate Generator:
http://www.signfiles.com/apps/X509CertificateGenerator.msi

Warning and Disclaimer

Every effort has been made to make this manual as complete and accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this manual.

Trademarks

.NET, Visual Studio .NET are trademarks of Microsoft Inc.

Adobe, Adobe Reader are trademarks of Adobe Systems Inc.

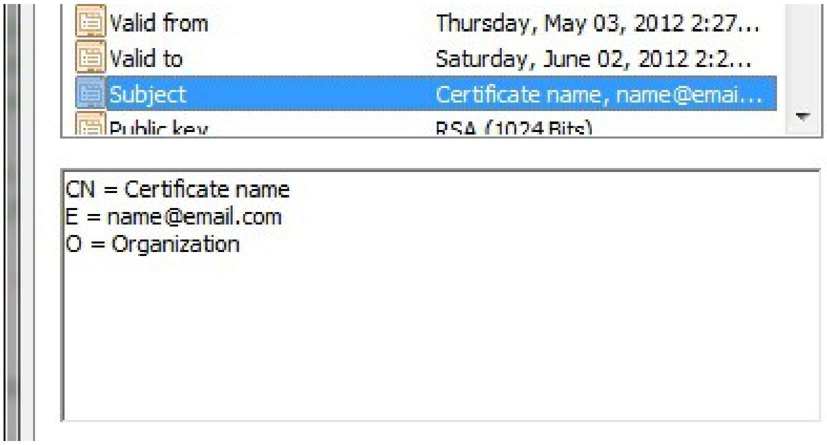
All other trademarks are the property of their respective owners.

Table of Contents

Digital Certificate Properties

Certificate Subject

Every certificate must have a *Subject*. This option can be set on the main interface. The *Subject* can contains Unicode characters like *ä,æ, £, Ñ*.



Valid from	Thursday, May 03, 2012 2:27...
Valid to	Saturday, June 02, 2012 2:2...
Subject	Certificate name, name@emai...
Public key	RSA (1024 Bits)

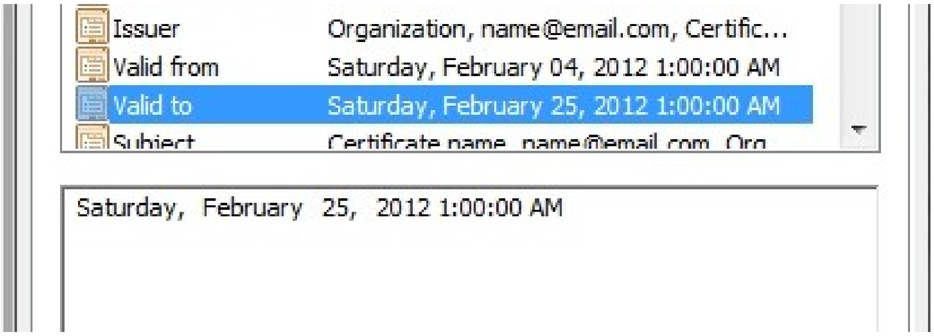
CN = Certificate name
E = name@email.com
O = Organization

Certificate Subject

Validity Period

Every certificate has a validity period. A certificate becomes invalid after it expires.

Observation: On the demo version of the product, the certificate validity cannot exceed 30 days. This is the single limitation of the product on demo mode.



Issuer	Organization, name@email.com, Certific...
Valid from	Saturday, February 04, 2012 1:00:00 AM
Valid to	Saturday, February 25, 2012 1:00:00 AM
Subject	Certificate name, name@email.com, Org

Saturday, February 25, 2012 1:00:00 AM

Certificate Validity period

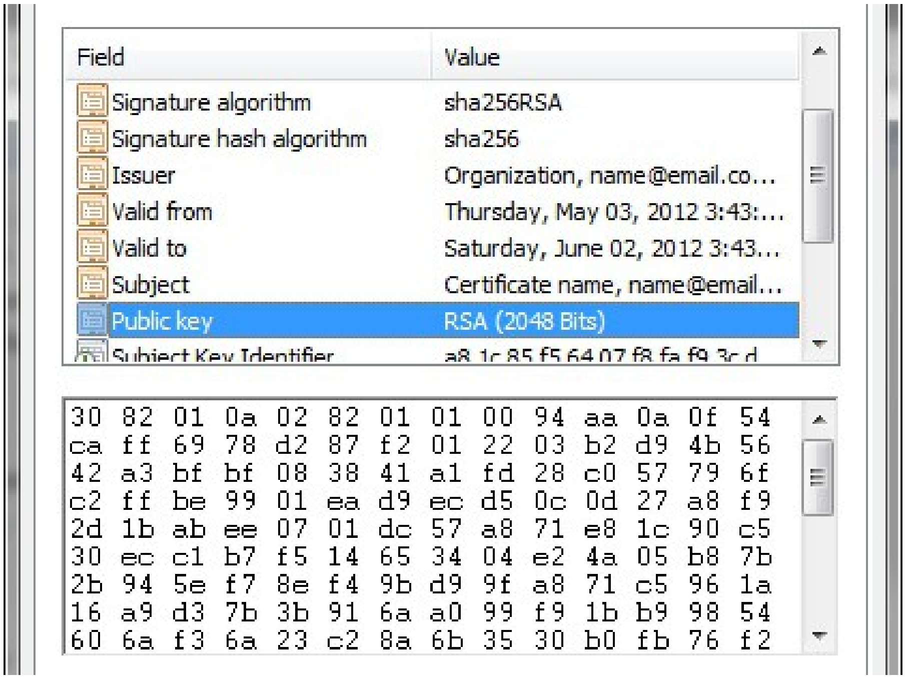
Cryptographic Algorithms

The certificates use RSA algorithm (RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers).

The default value of *RSA Key Length* is *1024 bit* and should be enough for common certificates. For the Root certificates a 2048 key could be used.

The default value of *SignatureAlgorithm* property is *SHA1WithRSA* but it can be set to other values if it is necessary.

Observation: The certificate will requires more time to be generated if a larger key size is used.



Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Organization, name@email.co...
Valid from	Thursday, May 03, 2012 3:43:...
Valid to	Saturday, June 02, 2012 3:43...
Subject	Certificate name, name@email...
Public key	RSA (2048 Bits)
Subject Key Identifier	a8 1c 85 f5 64 07 f8 fa f9 3c d

```
30 82 01 0a 02 82 01 01 00 94 aa 0a 0f 54
ca ff 69 78 d2 87 f2 01 22 03 b2 d9 4b 56
42 a3 bf bf 08 38 41 a1 fd 28 c0 57 79 6f
c2 ff be 99 01 ea d9 ec d5 0c 0d 27 a8 f9
2d 1b ab ee 07 01 dc 57 a8 71 e8 1c 90 c5
30 ec c1 b7 f5 14 65 34 04 e2 4a 05 b8 7b
2b 94 5e f7 8e f4 9b d9 9f a8 71 c5 96 1a
16 a9 d3 7b 3b 91 6a a0 99 f9 1b b9 98 54
60 6a f3 6a 23 c2 8a 6b 35 30 b0 fb 76 f2
```

Certificate public key

Key Usage

A CA, user, computer, network device, or service can have more than one certificate. The Key Usage extension defines the security services for which a certificate can be used. The options can be used in any combination and can include the following:

DataEncipherment - The public key can be used to directly encrypt data, rather than exchanging a symmetric key for data encryption.

DigitalSignature - The certificate use the public key for verifying digital signatures that have purposes other than non-repudiation, certificate signature, and CRL signature.

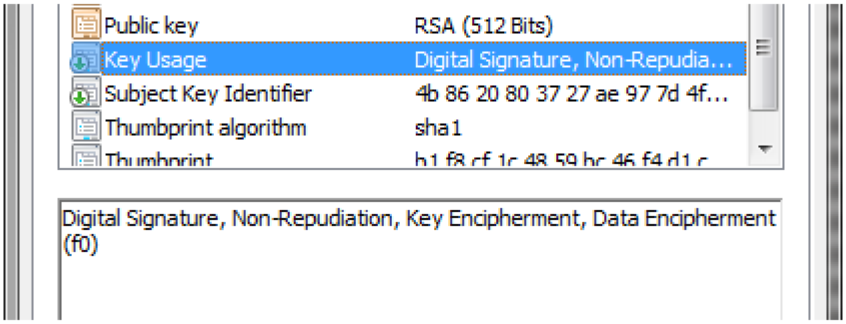
KeyEncipherment - The certificate use the public key for key transport.

CRLSigning - The certificate use the public key for verifying a signature on certificates.

CertificateSigning - The certificate use the public key for key agreement.

For a Regular User certificate, the most used Key Usages are: *DigitalSignature, NonRepudiation, KeyEncipherment* and *DataEncipherment.*

For a Root Certificate (CA certificate), the most used Key Usages are: *CertificateSigning* and *CRLSigning.*



Public key	RSA (512 Bits)
Key Usage	Digital Signature, Non-Repudia...
Subject Key Identifier	4b 86 20 80 37 27 ae 97 7d 4f...
Thumbprint algorithm	sha1
Thumbprint	b1 f8 cf 1c 48 59 bc 46 f4 d1 c

Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)

Certificate Key Usage

Enhanced Key Usage

This extension indicates how a certificate's public key can be used. The Enhanced Key Usage extension provides additional information beyond the general purposes defined in the Key Usage extension. For example, OIDs exist for Client Authentication (1.3.6.1.5.5.7.3.2), Server Authentication (1.3.6.1.5.5.7.3.1), and Secure E-mail (1.3.6.1.5.5.7.3.4).

When a certificate is presented to an application, an application can require the presence of an Enhanced Key Usage OID specific to that application.

X.509 Certificate Generator supports a lot of well known Enhanced Key Usages but also support to specify a custom Enhanced Key Usage extension. The Enhanced Key Usage can be also marked as a Critical extension.

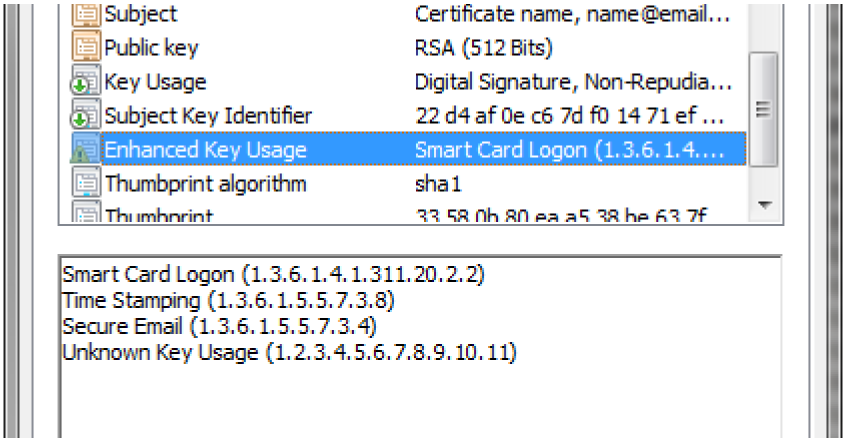
Some of Enhanced Key Usages available by default are:

CodeSigning - The certificate can be used for signing code.

SmartcardLogon - The certificate enables an individual to log on to a computer by using a smart card.

DocumentSigning - The certificate can be used for signing documents.

TimeStamping - The certificate can be used for signing public key infrastructure timestamps according to RFC 3161.



Subject	Certificate name, name@email...
Public key	RSA (512 Bits)
Key Usage	Digital Signature, Non-Repudia...
Subject Key Identifier	22 d4 af 0e c6 7d f0 14 71 ef ...
Enhanced Key Usage	Smart Card Logon (1.3.6.1.4....
Thumbprint algorithm	sha1
Thumbprint	33 58 0b 80 ea a5 38 be 63 7f

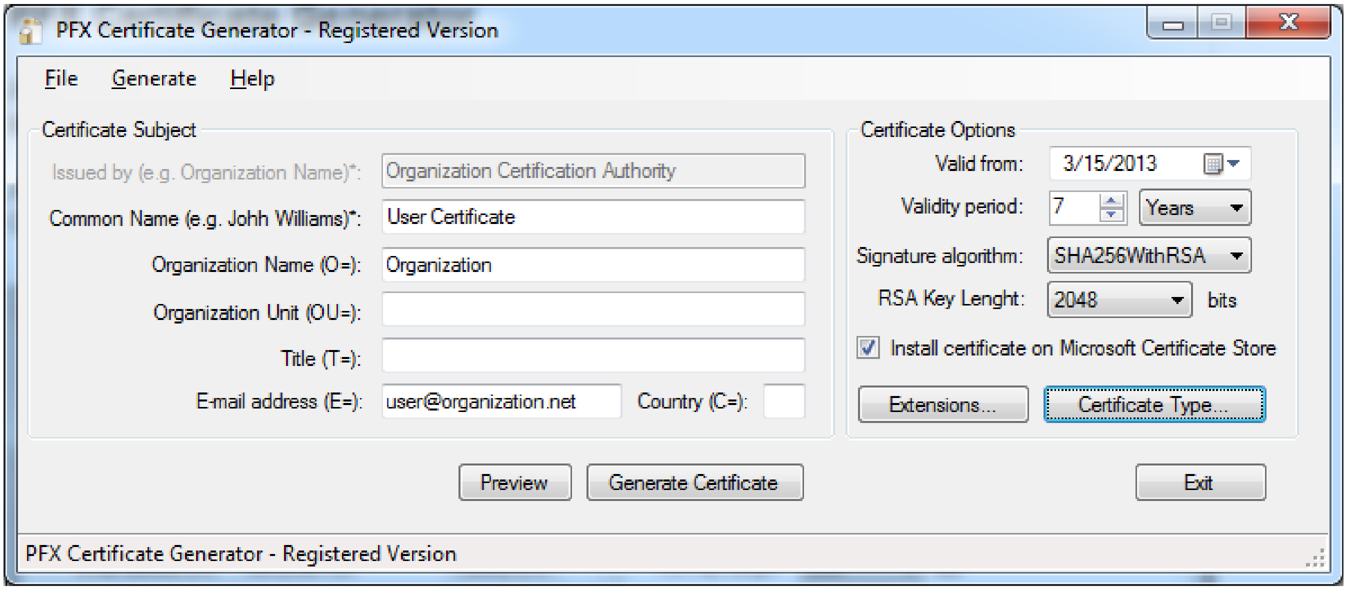
```
Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
Time Stamping (1.3.6.1.5.5.7.3.8)
Secure Email (1.3.6.1.5.5.7.3.4)
Unknown Key Usage (1.2.3.4.5.6.7.8.9.10.11)
```

Enhanced Key Usage (marked as Critical Extension)

PFX Certificate Generator

PFX Certificate Generator is designed to issue custom PFX certificates. All certificate options like Validity period, Signature algorithm, Key length, Key Usage are fully customizable.

Also, the CSR (Certificate Signing Request) can be signed by a previous created Root Certificate. This option is available on *Generate* main menu.



PFX Certificate Generator - Registered Version

Certificate Subject

Issued by (e.g. Organization Name)*: Organization Certification Authority

Common Name (e.g. Johh Williams)*: User Certificate

Organization Name (O=): Organization

Organization Unit (OU=):

Title (T=):

E-mail address (E=): user@organization.net Country (C=):

Certificate Options

Valid from: 3/15/2013

Validity period: 7 Years

Signature algorithm: SHA256WithRSA

RSA Key Lenght: 2048 bits

☑ Install certificate on Microsoft Certificate Store

PFX Certificate Generator - Registered Version

PFX Certificate Generator main interface

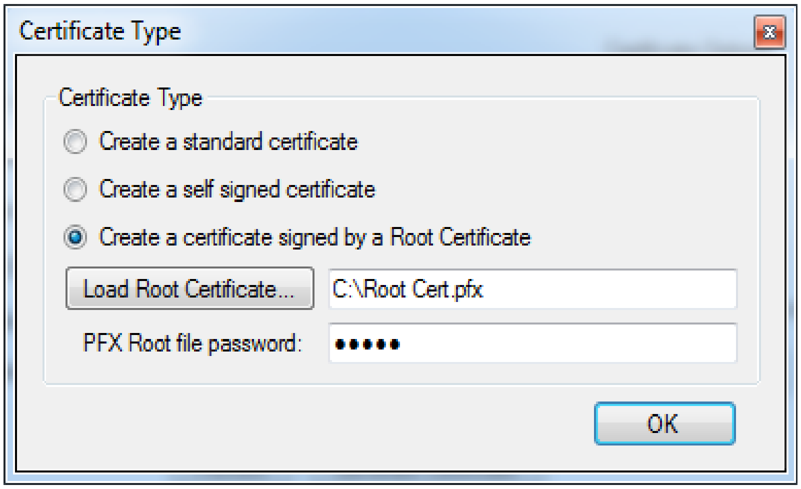
After the PFX certificate is generated, if "Install certificate on local computer (Microsoft Store)" is checked, the certificate can be automatically installed on local computer Certificate Store.

Issuing Certificates

By default, the certificates issued by PFX Certificate Generator are signed by a Root Certificate created on the fly.

Also, the application can issue digital certificates signed by a Root Certificate loaded from a PFX file or self-signed digital certificates.

More details about Self-signed Certificates can be found here.



Certificate Type

○ Create a standard certificate

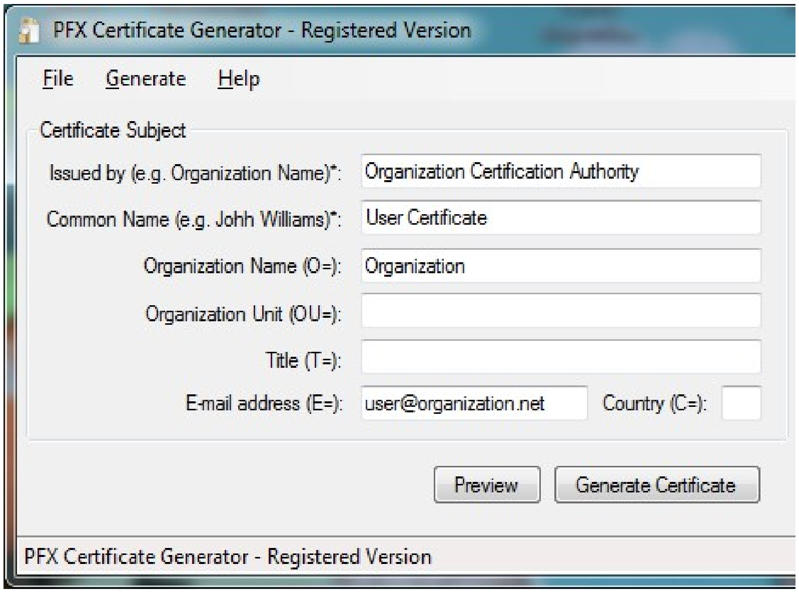
○ Create a self signed certificate

● Create a certificate signed by a Root Certificate

Load Root Certificate...: C:\Root Cert.pfx

PFX Root file password: •••••

Self-signed certificates


PFX Certificate Generator - Registered Version
File
Generate
Help
Preview
Generate Certificate
PFX Certificate Generator - Registered Version

Certificate Subject

Issued by (e.g. Organization Name)*: Organization Certification Authority

Common Name (e.g. Johh Williams)*: User Certificate

Organization Name (O=): Organization

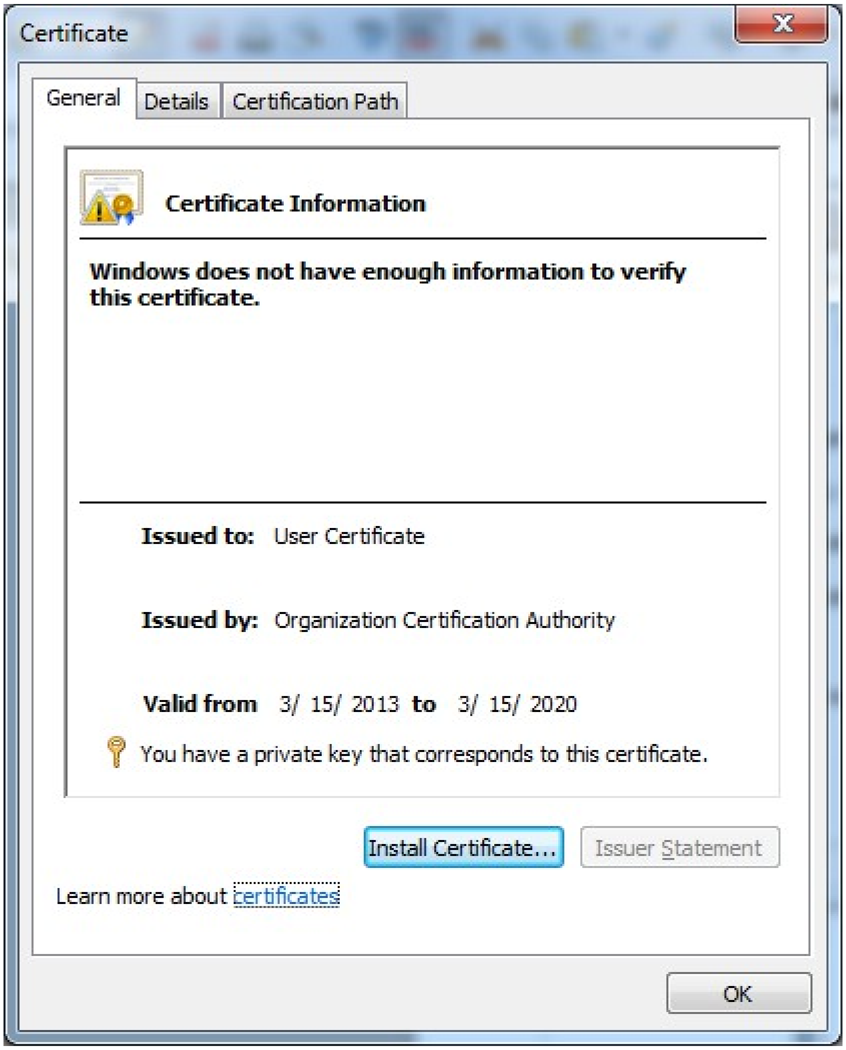
Organization Unit (OU=):

Title (T=):

E-mail address (E=): user@organization.net Country (C=):

Certificate subject

A digital certificate issued by PFX Certificate Generator will look like below:



Certificate Information

Windows does not have enough information to verify this certificate.

Issued to: User Certificate

Issued by: Organization Certification Authority

Valid from 3/ 15/ 2013 to 3/ 15/ 2020

You have a private key that corresponds to this certificate.

Learn more about certificates

Self-signed certificate

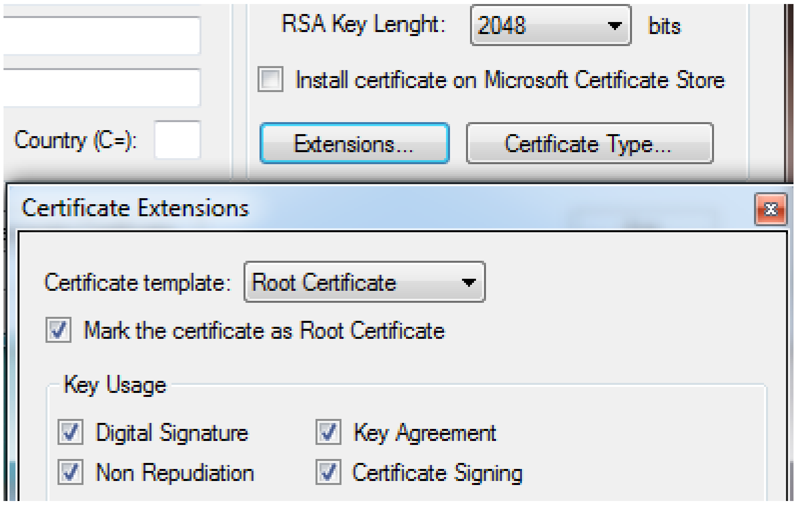
Issuing Certificates Signed by a Root Certificate

Issue the Root Certificate

In some cases, is necessary to issue certificates for an entire organization. On this scenario you can issue a Root Certificate and every certificate issued for an entity will be signed by this Root Certificate.

A Root Certificate (CA certificate) is a special type of certificate that can be used to digitally sign other certificates.

To issue a Root Certificate with X.509 Certificate Generator, simply select *"Root Certificate"* template from *Extensions* dialog and issue the certificate.



Country (C=):

RSA Key Lenght: 2048 bits

□ Install certificate on Microsoft Certificate Store

Certificate template: Root Certificate

☑ Mark the certificate as Root Certificate

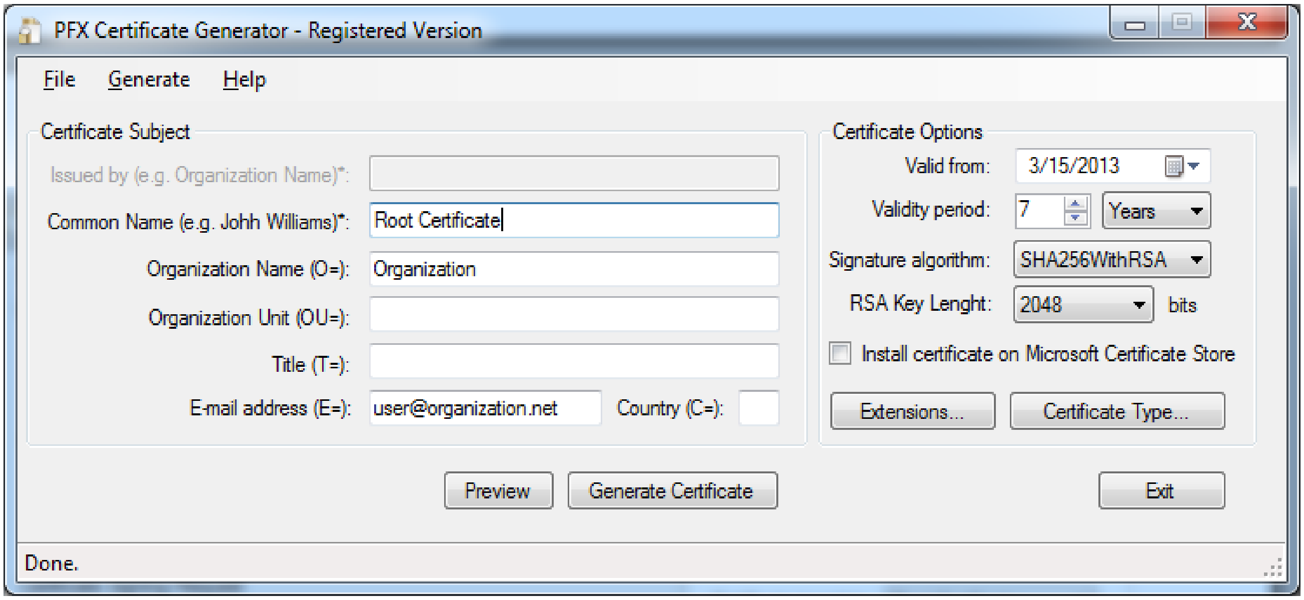
Key Usage

☑ Digital Signature ☑ Key Agreement

☑ Non Repudiation ☑ Certificate Signing

Root Certificate Template

Note to remember the file name and PFX password used to issue this certificate.



Issued by (e.g. Organization Name)*:

Common Name (e.g. Johh Williams)*: Root Certificate

Organization Name (O=): Organization

Organization Unit (OU=):

Title (T=):

E-mail address (E=): user@organization.net Country (C=):

Valid from: 3/15/2013

Validity period: 7 Years

Signature algorithm: SHA256WithRSA

RSA Key Lenght: 2048 bits

☐ Install certificate on Microsoft Certificate Store

Done.

Creating a Root Certificate

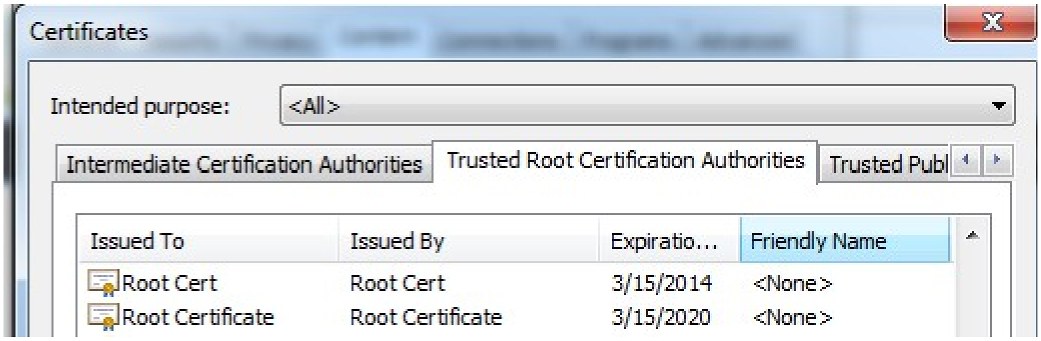
Saving the Root Certificate Public Part

The certificates signed by the Root Certificate, could be considered invalid on some computers.

For example, if a CSR is signed by the Root Certificate, when the SSL certificate is installed, it will considered untrusted by the web browsers.

In order to validate the certificates on other computers, the Root Certificate used to issue Client Certificates (like SSL certificates), must be installed on that computers first.

After the Root Certificate is created and imported, it is available on Microsoft Certificate Store (Personal or Trust Root Certification Authorities Tab)


Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ

Intended purpose: <All>

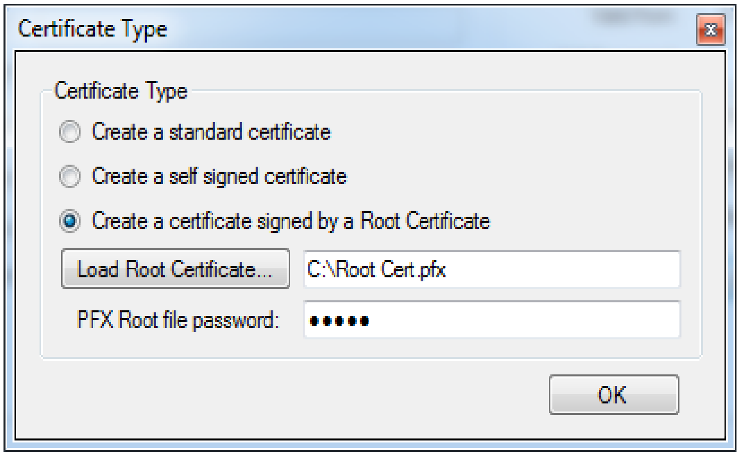
Issued To	Issued By	Expiratio...	Friendly Name
Root Cert	Root Cert	3/15/2014	<None>
Root Certificate	Root Certificate	3/15/2020	<None>

The resulting .CER file must be installed on Microsoft Certificate Store - Trusted Root Certification Authorities Tab (see section: *Microsoft Certificate Store - Import the Root Certificate on Microsoft Store* for more details).

Issue the Client Certificate Signed by the Root Certificate

In order to issue certificates signed by this Root Certificate, do the following:

- on *Extension* tab, select “Standard User” template
- fill the Certificate Subject (Issued to, Organization, E-mail address, etc.) with your data
- on *Certificate Type* tab, select “Create a certificate signed by a Root Certificate” and select the previous created Root certificate.
- Issue and save the PFX certificate.



Certificate Type

Certificate Type

○ Create a standard certificate

○ Create a self signed certificate

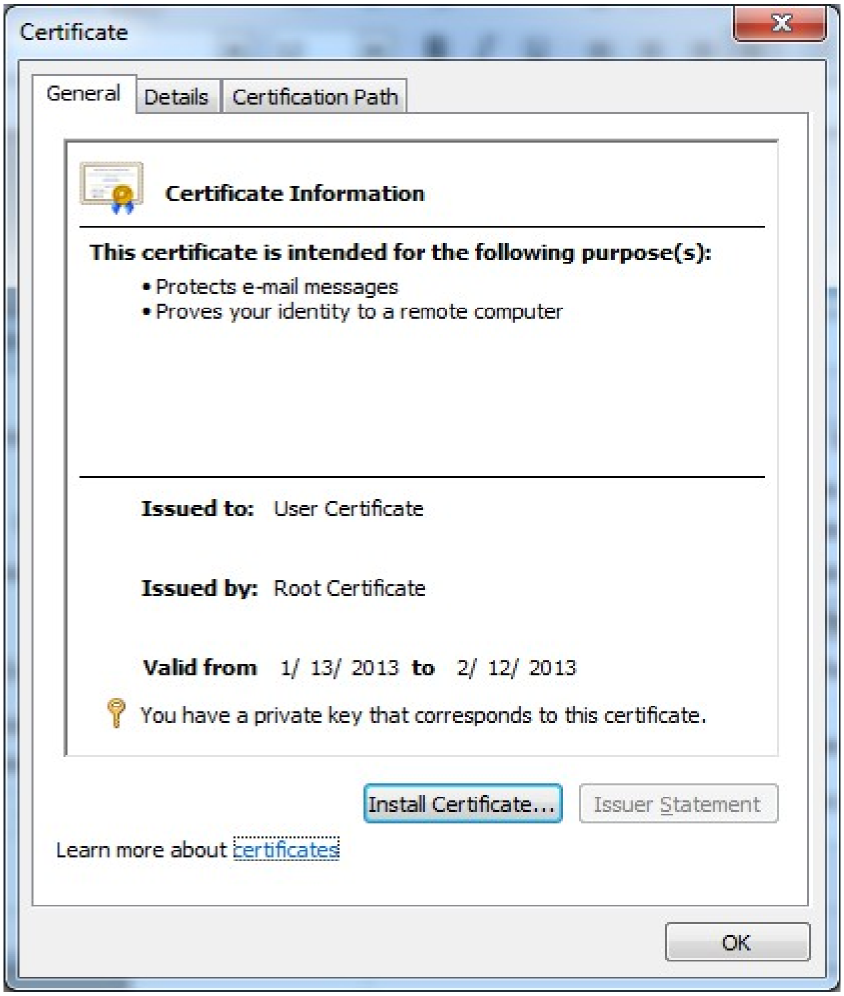
● Create a certificate signed by a Root Certificate

Load Root Certificate... C:\Root Cert.pfx

PFX Root file password: •••••

Issue certificates signed by a Root Certificate

A certificate signed by a Root Certificate will look like below:



Certificate

General | Details | Certification Path

Certificate Information

This certificate is intended for the following purpose(s):
- Protects e-mail messages
- Proves your identity to a remote computer

Issued to: User Certificate

Issued by: Root Certificate

Valid from 1/ 13/ 2013 to 2/ 12/ 2013

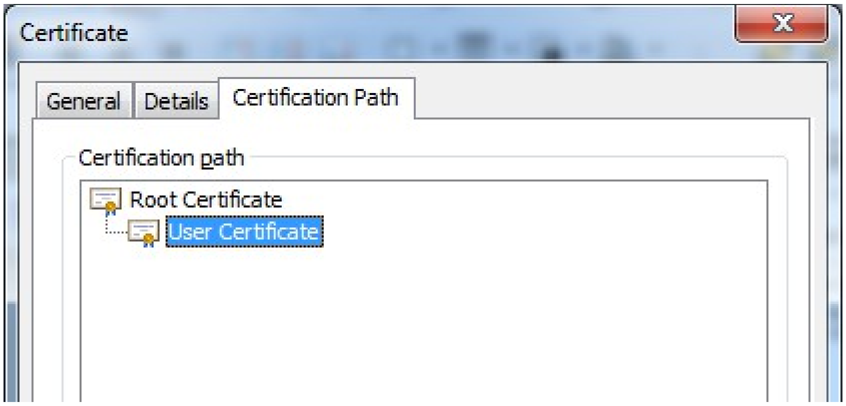
You have a private key that corresponds to this certificate.

Install Certificate... | Issuer Statement

Learn more about certificates

OK

Certificate signed by a Root Certificate



Certificate

General | Details | Certification Path

Certification path

Root Certificate
User Certificate

Certification Path

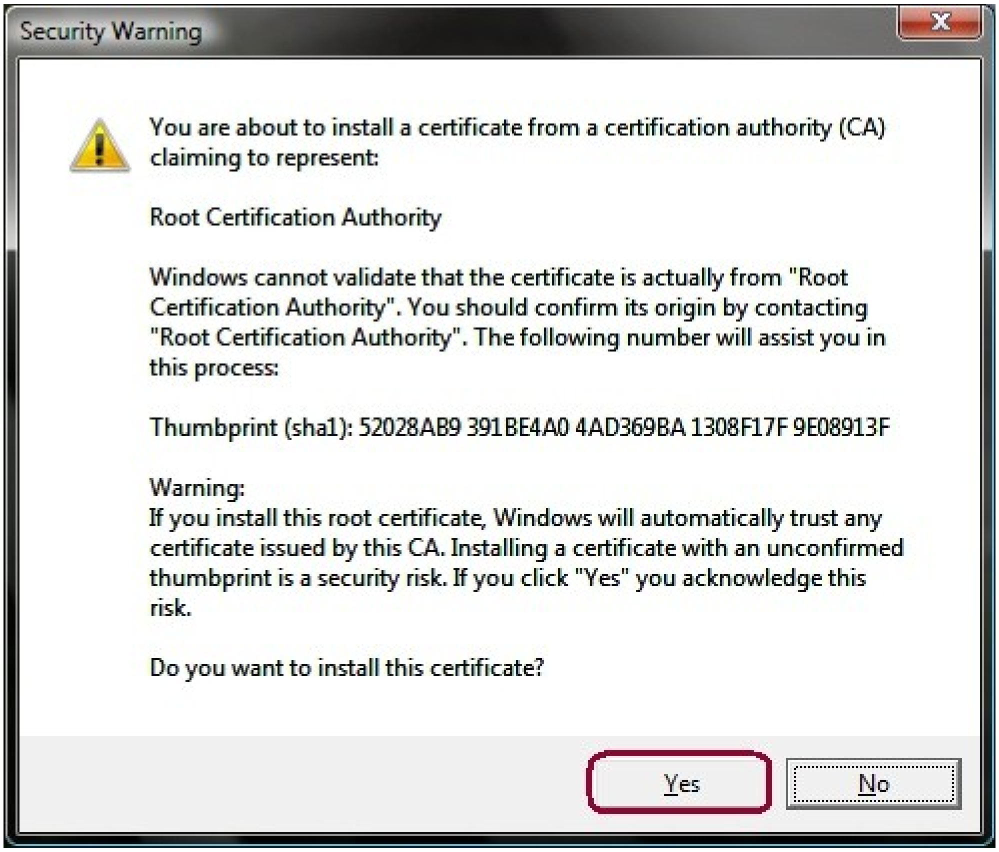
Installing a PFX Certificate

If you already have a PFX digital certificate and you want to be validated by your system, follow these steps:

- double click the PFX file (just press *Next* without change anything)
- enter the PFX protection password
- press Yes when the message below appears.

When a user certificate is issued by a Root Certificate, in order to trust the user certificate, the Root Certificate must be imported on *Microsoft Store – Trusted Root Certification Authorities*.

When the PFX user certificate is imported on Microsoft Store, the Root Certificate can be also imported as follow:



You are about to install a certificate from a certification authority (CA) claiming to represent:

Root Certification Authority

Windows cannot validate that the certificate is actually from "Root Certification Authority". You should confirm its origin by contacting "Root Certification Authority". The following number will assist you in this process:

Thumbprint (sha1): 52028AB9 391BE4A0 4AD369BA 1308F17F 9E08913F

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

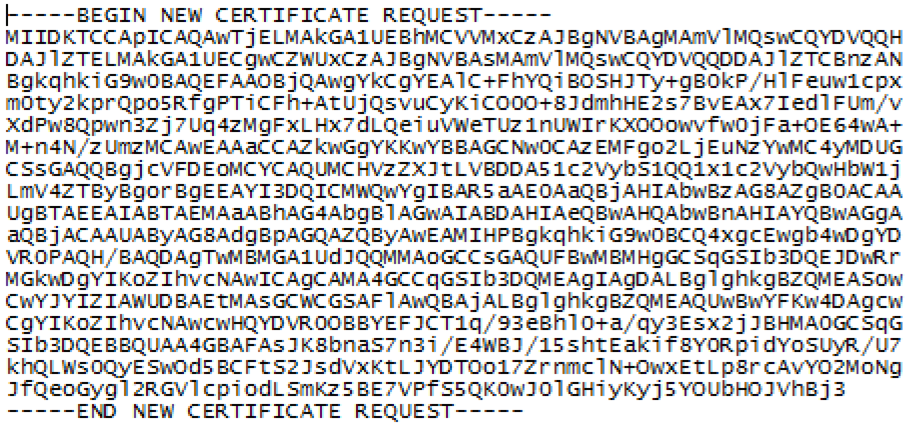
Do you want to install this certificate?

Installing Root Certificate on Microsoft Store

At this step, the Root Certificate is imported and every certificate issued by this Root is considered trusted.

Issuing Certificates from CSR (SSL Certificates)

A *Certificate Signing Request* (also CSR or certification request) is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate. The most common format for CSRs is the PKCS#10 specification.



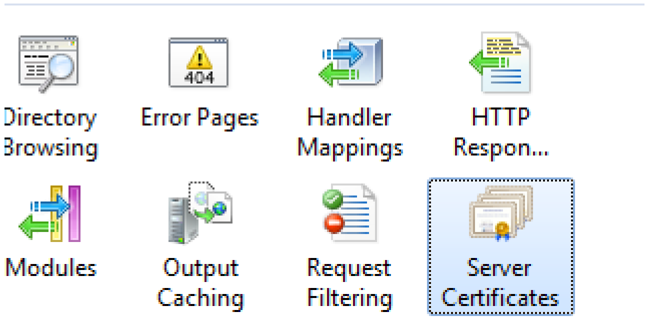
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDKTCCApICAQAwTjELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAmVlMQswCQYDVQQH
DAJlZTELMAkGA1UECgwCZWUxCzAJBgNVBAsMAmVlMQswCQYDVQQDDAJlZTCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAlC+FhYQiBOSHJTy+gBOkP/HlFeuw1cpx
m0ty2kprQpo5RfgPTiCFh+AtUjQsvuCyKiCOOO+8JdmhHE2s7BvEAx7IedlFUm/v
XdPw8Qpwn3Zj7Uq4zMgFxLHx7dLQeiuVWeTUz1nUWIrKXOOowvfw0jFa+OE64wA+
M+n4N/zUmzMCAwEAAaCCAZkwGgYKKwYBBAGCNw0CAzEMFgo2LjEuNzYwMC4yMDUG
CSsGAQQBgjcVFDEoMCYCAQUMCHVzZXJtLVBDDA51c2VybS1QQ1x1c2VybQwHbW1j
LmV4ZTByBgorBgEEAYI3DQICMWQwYgIBAR5aAE0AaQBjAHIAbwBzAG8AZgB0ACAA
UgBTAEEAIABTAEMAaABhAG4AbgBlAGwAIABDAHIAeQBwAHQAbwBnAHIAYQBwAGgA
aQBjACAAUAByAG8AdgBpAGQAZQByAwEAMIHPBgkqhkiG9w0BCQ4xgcEwgb4wDgYD
VR0PAQH/BAQDAgTwMBMGA1UdJQQMMAoGCCsGAQUFBwMBMHgGCSqGSIb3DQEJDwRr
MGkwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQMEAgIAgDALBglghkgBZQMEASow
CwYJYIZIAWUDBAEtMAsGCWCGSAFlAwQBAjALBglghkgBZQMEAQUwBwYFKw4DAgcw
CgYIKoZIhvcNAwcwHQYDVR0OBBYEFJCT1q/93eBhl0+a/qy3Esx2jJBHMA0GCSqG
SIb3DQEBBQUAA4GBAFAsJK8bnaS7n3i/E4WBJ/15shtEakif8YORpidYoSUyR/U7
khQLWs0QyESwOd5BCFtS2JsdVxKtLJYDTOo17ZrnmclN+OwxEtLp8rcAvYO2MoNg
JfQeoGygl2RGVlcpiodLSmKz5BE7VPfS5QKOwJOlGHiyKyj5YOUbHOJVhBj3
-----END NEW CERTIFICATE REQUEST-----
```

Certificate Signing Request (CSR)

PFX Certificate Generator can digitally sign CSR request using a Root Certificate. To create a Root Certificate see the section *Issuing Certificates Signed by a Root Certificate - Issue the Root Certificate*.

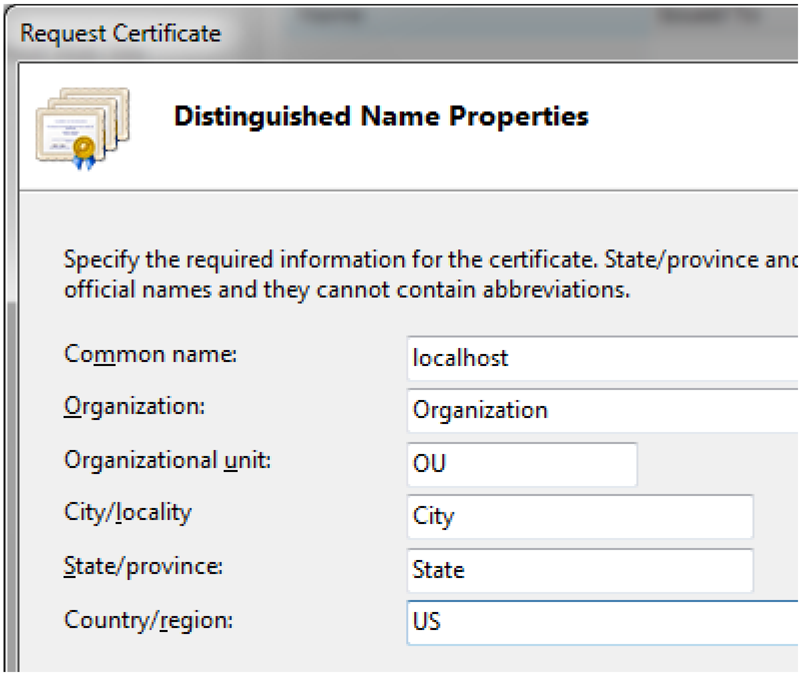
Create the CSR for an IIS website

To generate a CSR for your website, access IIS - Computer – Manage – Service and Applications – IIS Manager – Server Certificates, like below:



IIS Configuration

– select *Create Certificate Request* and fill the form with your information, click Finish, click Next and save the CSR file on a local file (e.g. *c:\CSR.txt*).



Request Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province anc
official names and they cannot contain abbreviations.

Common name:	localhost
Organization:	Organization
Organizational unit:	OU
City/locality	City
State/province:	State
Country/region:	US

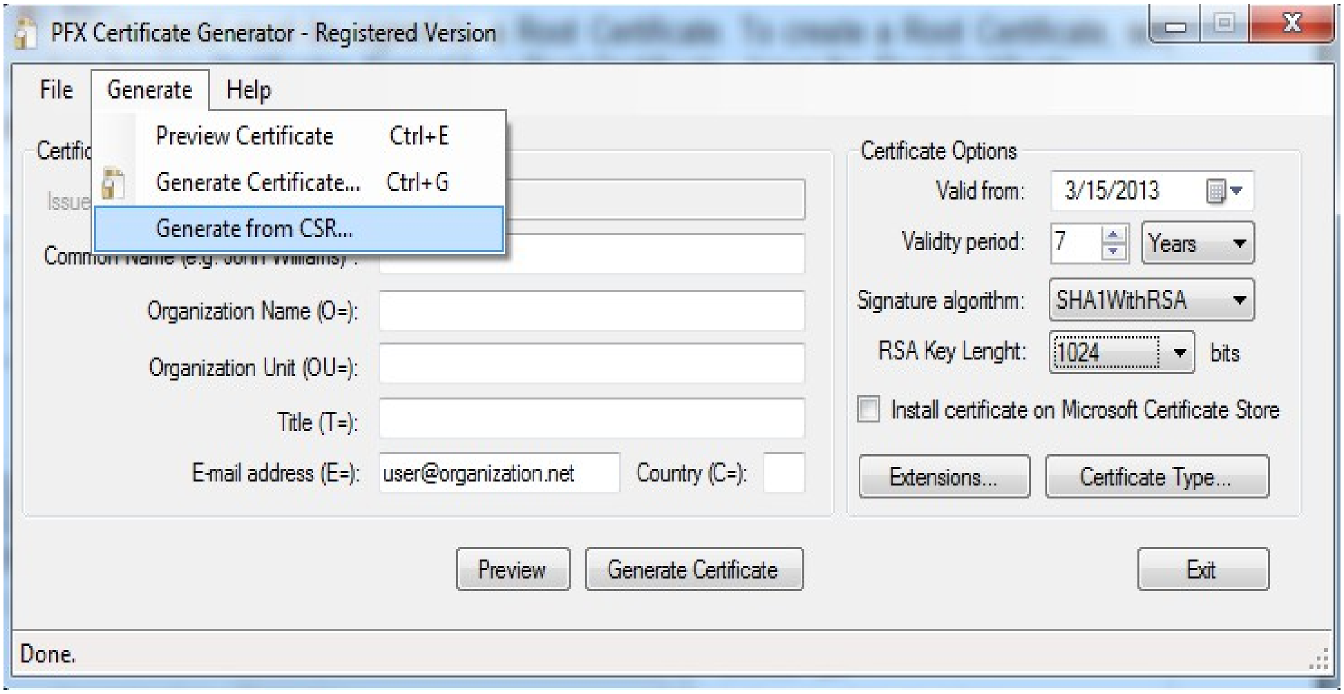
Creating the CSR Request

Signing the CSR Request with the Root Certificate

Every CSR Request must be signed by a Root Certificate. To create a Root Certificate, see the section *Issuing Certificates Signed by a Root Certificate - Issue the Root Certificate*.

To digitally sign the CSR Request, follow the steps below:

- select *SSL Certificate* template from the *Certificate Type* tab.
- Load the Root Certificate previously created
- Load the CSR by pressing *Generate from CSR...* menu item
- Save the resulting .CER file (e.g. c:\resp.cer)


PFX Certificate Generator - Registered Version
File
Generate
Help
Preview Certificate Ctrl+E
Generate Certificate... Ctrl+G
Generate from CSR...
Extensions...
Certificate Type...
Preview
Generate Certificate
Exit

Certific

Issue

Common Name (e.g. John Williams) :

Organization Name (O=):

Organization Unit (OU=):

Title (T=):

E-mail address (E=): user@organization.net

Country (C=):

Certificate Options

Valid from: 3/15/2013

Validity period: 7 Years

Signature algorithm: SHA1WithRSA

RSA Key Lenght: 1024 bits

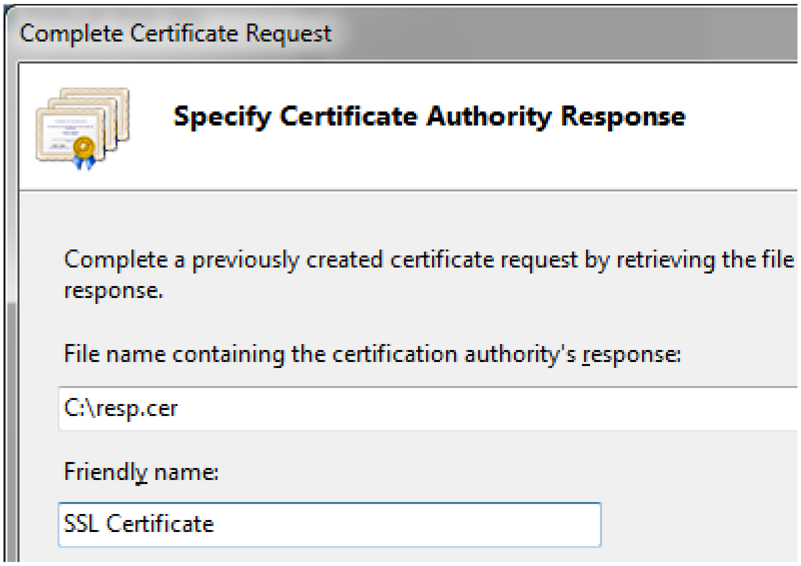
☐ Install certificate on Microsoft Certificate Store

Done.

Signing the CSR with a Root Certificate

Installing the CSR response on the IIS website

Go to IIS - Computer – Manage – Service and Applications – IIS Manager – Server Certificates – *Complete Certificate Request*. Select the resulting .CER file previously signed by the Root Certificate (c:\resp.cer) and click OK.



Complete Certificate Request

Specify Certificate Authority Response

Complete a previously created certificate request by retrieving the file response.

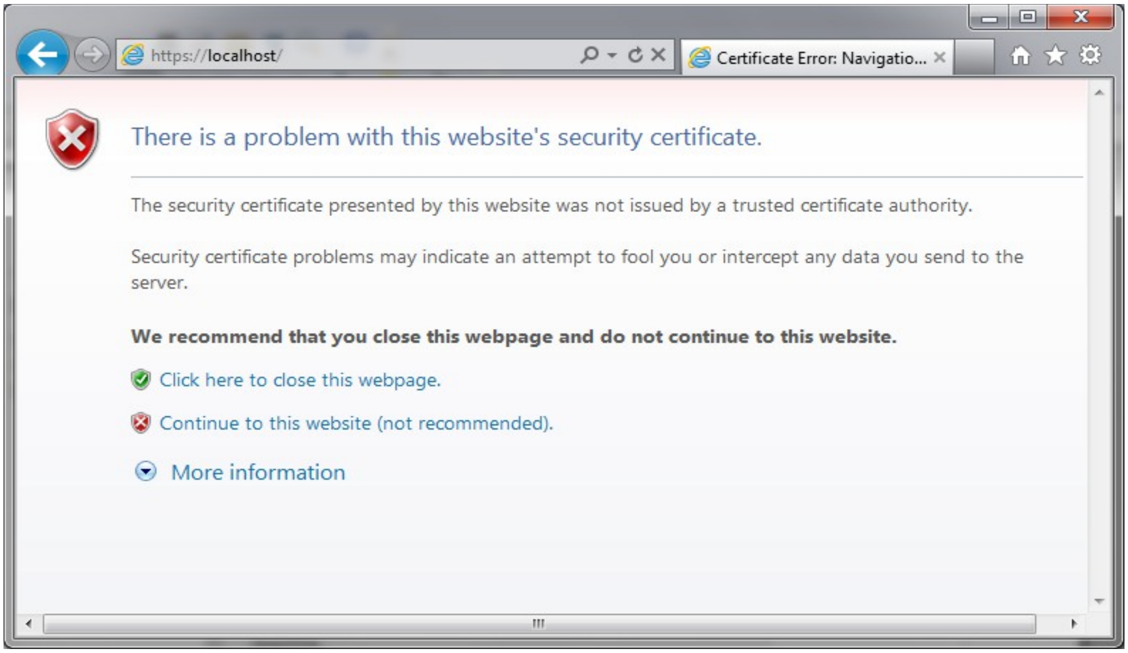
File name containing the certification authority's response:

C:\resp.cer

Friendly name:

SSL Certificate

Right now, the certificate is installed. To test the SSL website, go to *https://loclahost*.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

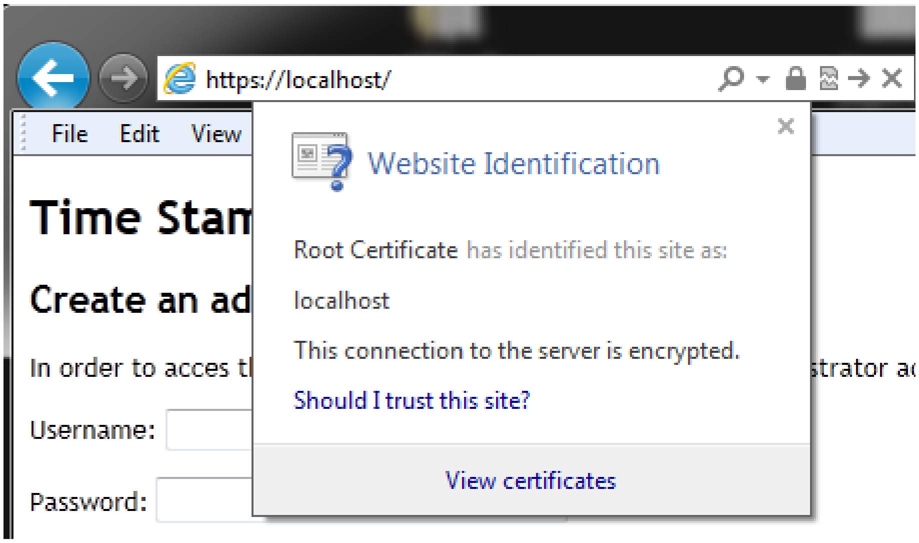
Untrusted certificate

Validating the SSL certificate

If the SSL certificate is considered untrusted by your web browser, you must install the Root Certificate pubic part used to digitally sign the CSR on Microsoft Certificate Store – Trusted Root Certification Authorities.

More details about this issue are available on this section: *Saving the Root Certificate Public Part*.

After the Root Certificate is imported, the website will look like below:



Root Certificate has identified this site as:

localhost

This connection to the server is encrypted.

Should I trust this site?

Trusted SSL certificate

Steps to validate the SSL certificate:

- Issue the Root certificate
- Install the certificate and extract the Root Certificate public part from Microsoft Store.
- Create and sign the CSR request with the Root Certificate
- Install the CSR Response on the webserver
- Install the Root Certificate pubic part on *Microsoft Certificate Store – Trusted Root Certification Authorities*. **This step must be done on every computer that access your website.**

Smart Card Certificate Generator

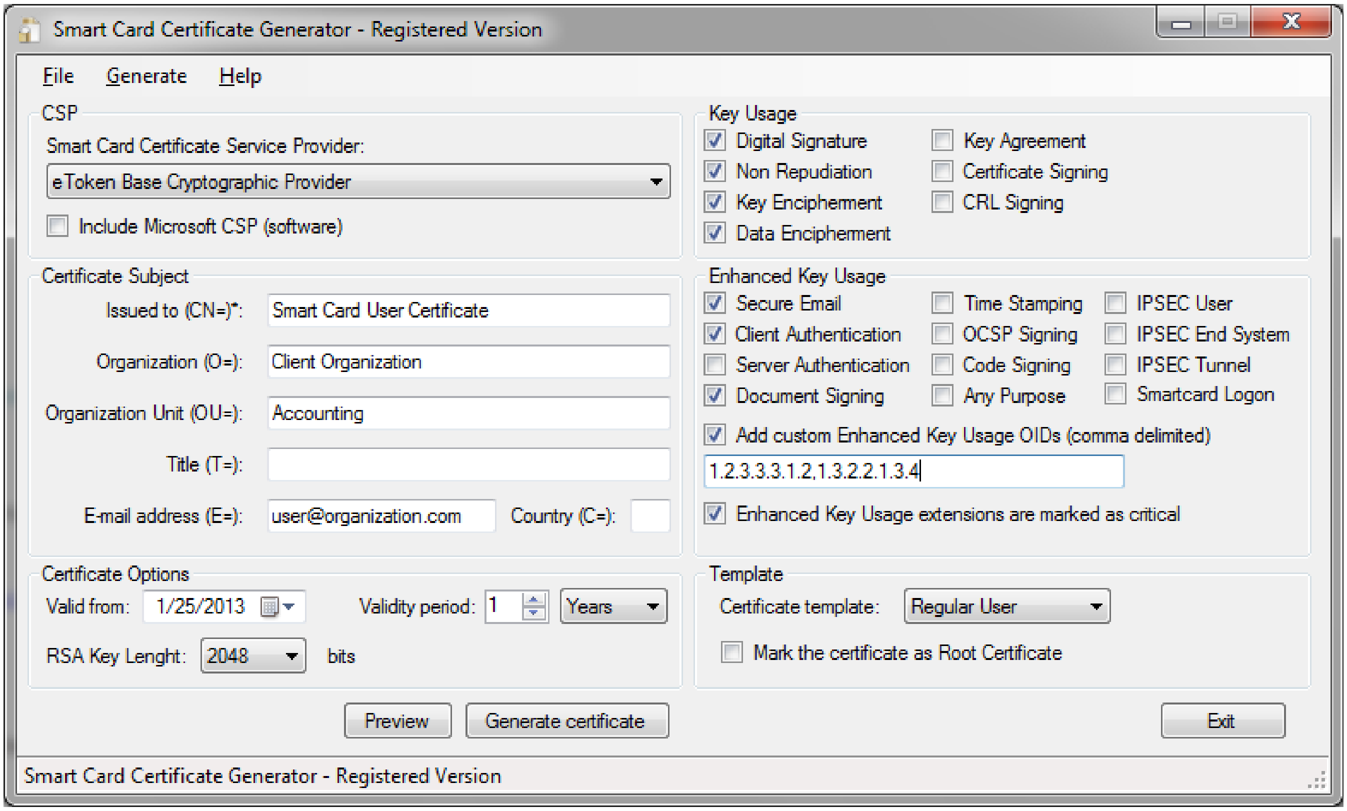
Observation: This product will work only on Windows Vista or higher.

Smart Card Certificate Generator is designed to issue self-signed digital certificates directly on cryptographic Smart Cards.

To issue the certificate on your smart card, follow the steps below:

- plug in your smart card on the USB port
- select the CSP smart card from the top left section
- be sure that you have enough space on the smart card
- set the proper settings from the product interface (certificate subject, validity period, extensions, etc).
- Generate your certificate.

If you like to generate the certificate directly on the Microsoft Certificate Store, check *Include Microsoft CSP (software)* checkbox, and select *Microsoft Enhanced Cryptographic Provider v1.0* or other CSP.



Smart Card Certificate Generator - Registered Version

CSP

Smart Card Certificate Service Provider: eToken Base Cryptographic Provider

☐ Include Microsoft CSP (software)

Certificate Subject

Issued to (CN=)*: Smart Card User Certificate

Organization (O=): Client Organization

Organization Unit (OU=): Accounting

Title (T=):

E-mail address (E=): user@organization.com

Country (C=):

Certificate Options

Valid from: 1/25/2013

Validity period: 1 Years

RSA Key Lenght: 2048 bits

Key Usage

☑ Digital Signature
☑ Non Repudiation
☑ Key Encipherment
☑ Data Encipherment
☐ Key Agreement
☐ Certificate Signing
☐ CRL Signing

Enhanced Key Usage

☑ Secure Email
☑ Client Authentication
☐ Server Authentication
☑ Document Signing
☐ Time Stamping
☐ OCSP Signing
☐ Code Signing
☐ Any Purpose
☐ IPSEC User
☐ IPSEC End System
☐ IPSEC Tunnel
☐ Smartcard Logon

☑ Add custom Enhanced Key Usage OIDs (comma delimited)

1.2.3.3.3.1.2,1.3.2.2.1.3.4

☑ Enhanced Key Usage extensions are marked as critical

Template

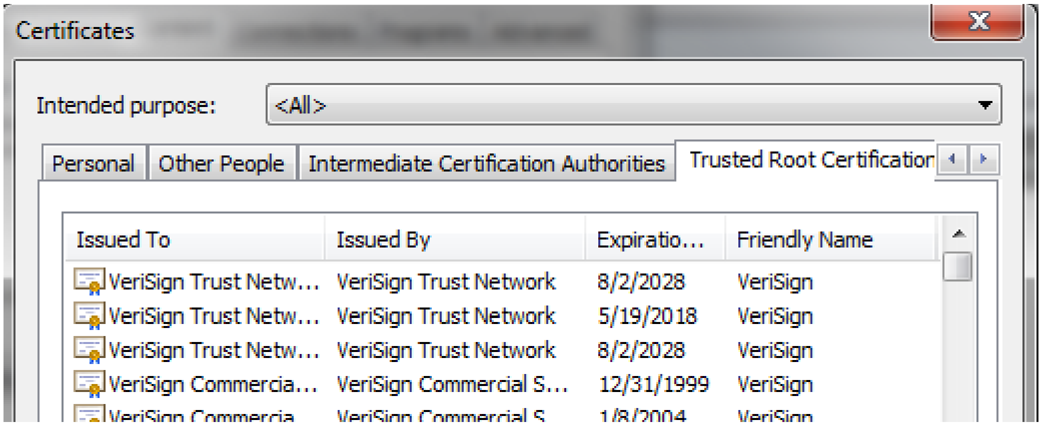
Certificate template: Regular User

☐ Mark the certificate as Root Certificate

Smart Card Certificate Generator - Registered Version

Microsoft Certificate Store

All digital certificates installed on the system appears in Microsoft Certificate Store.


Certificates
Intended purpose:
Personal
Other People
Intermediate Certification Authorities
Trusted Root Certification

Intended purpose: <All>

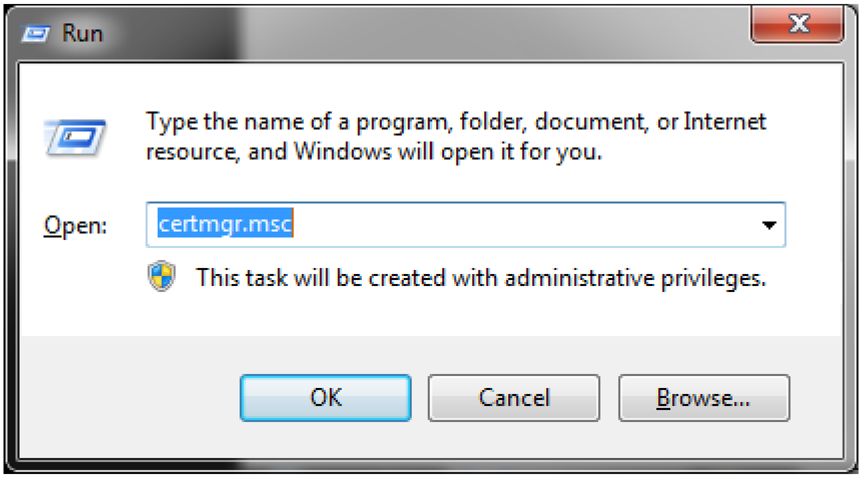
Issued To	Issued By	Expiratio...	Friendly Name
VeriSign Trust Netw...	VeriSign Trust Network	8/2/2028	VeriSign
VeriSign Trust Netw...	VeriSign Trust Network	5/19/2018	VeriSign
VeriSign Trust Netw...	VeriSign Trust Network	8/2/2028	VeriSign
VeriSign Commercia...	VeriSign Commercial S...	12/31/1999	VeriSign
VeriSign Commercia	VeriSign Commercial S	1/8/2004	VeriSign

Microsoft Certificate Store

How to Access Microsoft Certificate Store

- start Internet Explorer
- go to *Tools* menu – *Internet Options* – *Content* tab – *Certificates* button
- on *Certificates* window your personal certificates appears in *Personal* tab.
- The Root certificates appears in *Trusted Root Certification Authorities* tab.

Also, the Microsoft Store can be accessed by running *certmgr.msc* on Run Command.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: certmgr.msc

This task will be created with administrative privileges.

Accessing Microsoft Certificate Store

Export the Root Certificate from Microsoft Store

- Go to Microsoft Store
- Select *Trusted Root Certification Authorities* tab
- Select the Root Certificate that you want to export
- Click *Export* button and *Next*
- Select the path and file name for your exported certificate
- Click *Finish*.

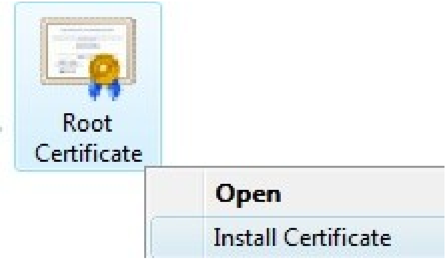
The Root Certificate is exported as *.cer* file. This file can be imported on the computers where you want to validate your certificate.

Note that if you digitally sign a file or send a digitally sign an email message to a computer that not have the Root Certificate installed, a warning message can appear.

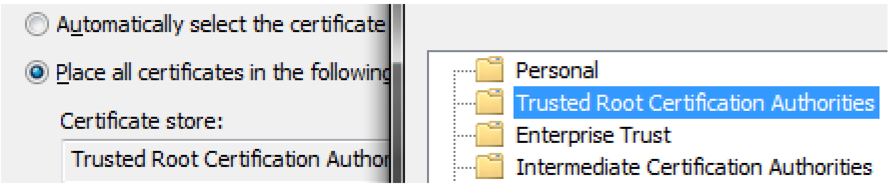
If you digitally sign a PDF file and want to validate Adobe PDF digital signatures, read this document:
http://www.signfiles.com/manuals/ValidatingDigitalSignaturesInAdobe.pdf

Import the Root Certificate on Microsoft Store

- Copy the exported .cer file obtained above (*Export the Root Certificate from Microsoft Store*) on the target computer
- Right click on the imported .cer file and select *Install Certificate*



- Click *Next* and select *Place all certificates in the following store*
- Click *Browse* and select *Trusted Root Certification Authorities*


○ Automatically select the certificate

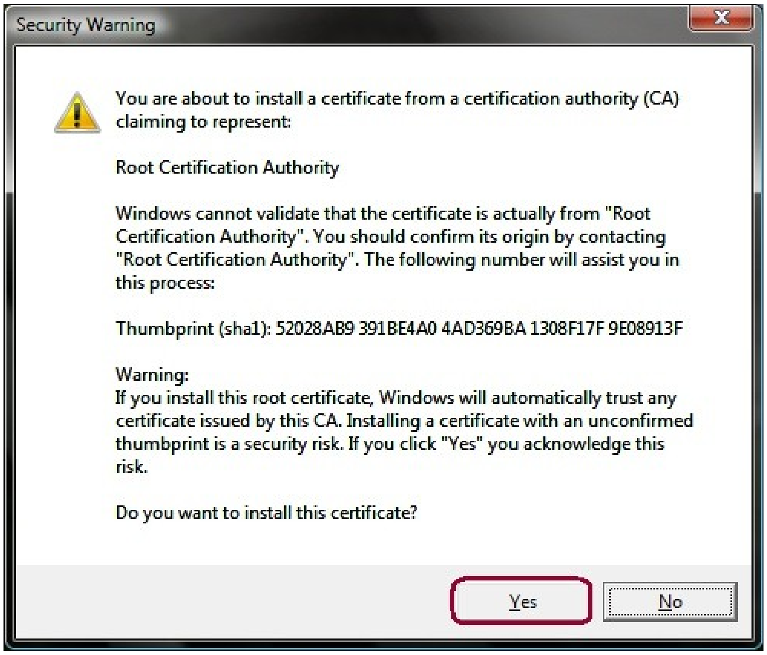
● Place all certificates in the following

Certificate store:

Trusted Root Certification Author

Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities

- Click *Finish*
- press Yes when the message below appears.



You are about to install a certificate from a certification authority (CA) claiming to represent:

Root Certification Authority

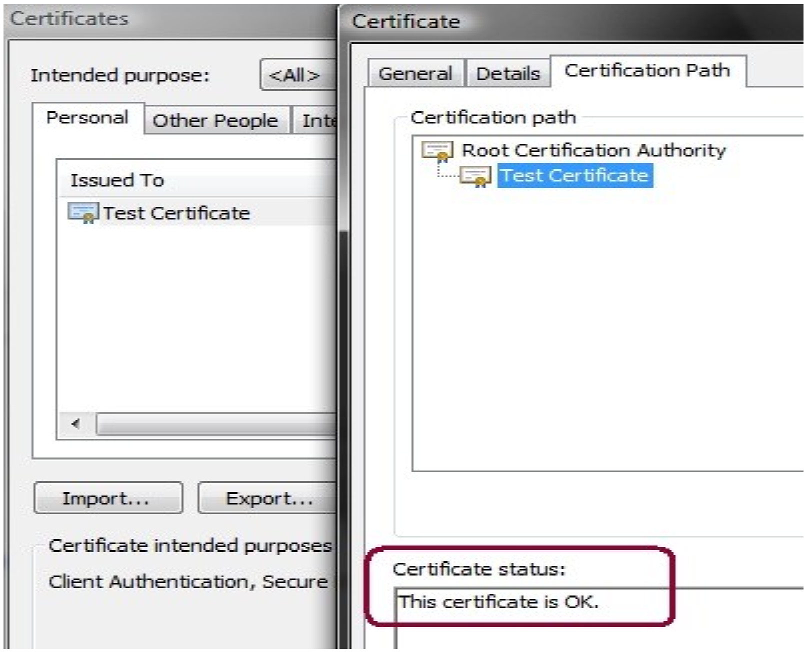
Windows cannot validate that the certificate is actually from "Root Certification Authority". You should confirm its origin by contacting "Root Certification Authority". The following number will assist you in this process:

Thumbprint (sha1): 52028AB9 391BE4A0 4AD369BA 1308F17F 9E08913F

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

After the Root Certificate is imported in Microsoft Store, the certificates issued by that Root Certification Authority will be considered valid on the machine where the Root Certificate was imported.



Certificate status:
This certificate is OK.

Observations

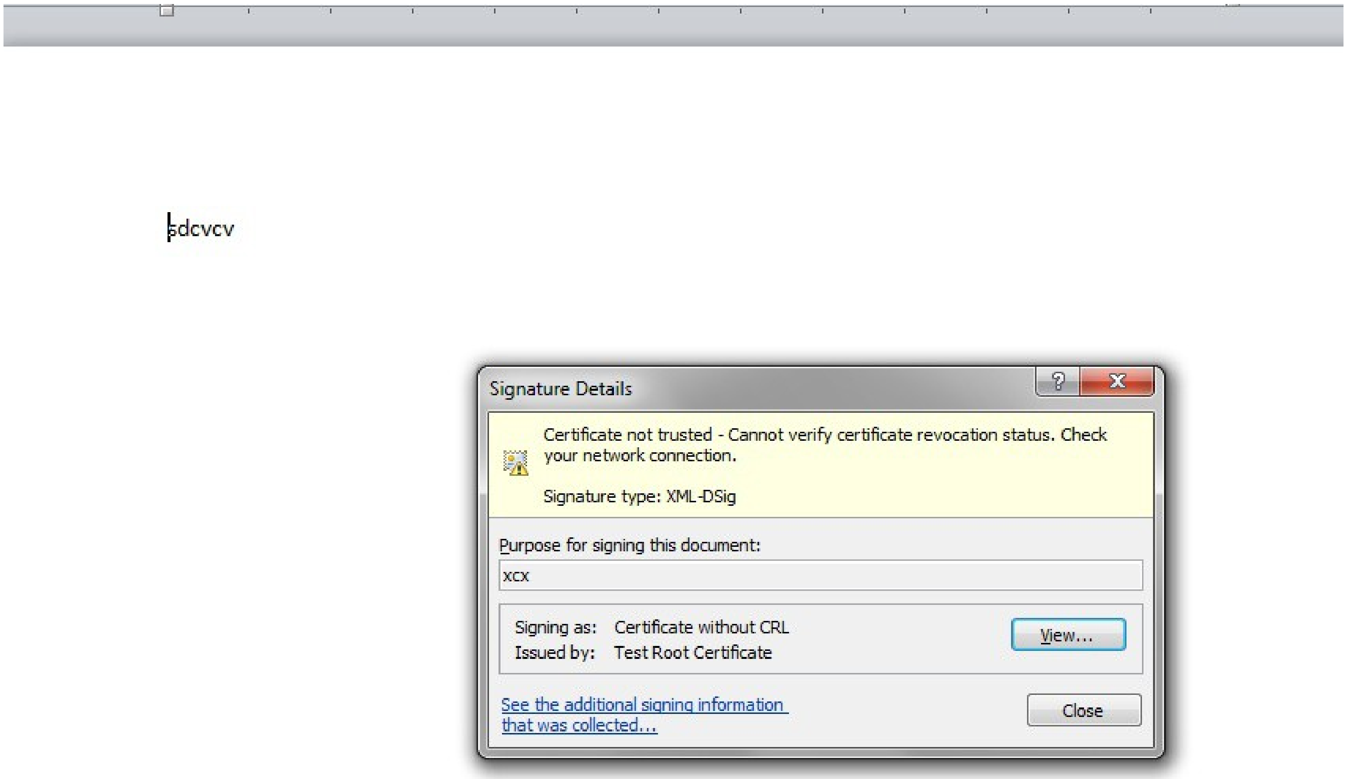
X.509 Certificate Generator and CRL

A CRL file is a web resource that is a list with all invalid certificates (e.g. http://rapidssl-crl.geotrust.com/crls/rapidssl.crl). The certificate can be revoked by the issuer in some circumstances (e.g. the person leaves the company) and the certificate serial number of that person is appended to the CRL when the revocation is made.

According the the X.509 standard, the CRL field is optional and should be ignored if it not exists but in Office 2010 digital signatures this field is mandatory.

If CRL field not appears on the certificate, the Office 2010 digital signature is considered invalid.

The CRL file MUST be published on the web (e.g. http://rapidssl-crl.geotrust.com/crls/rapidssl.crl) but X.509 Certificate Generator is a desktop product and cannot generates a CRL file and publish it on the web. This is the reason why the CRL attribute is not set on the certificates issued by X.509 Certificate Generator.



sdcvcv

Signature Details

Certificate not trusted - Cannot verify certificate revocation status. Check your network connection.

Signature type: XML-DSig

Purpose for signing this document:

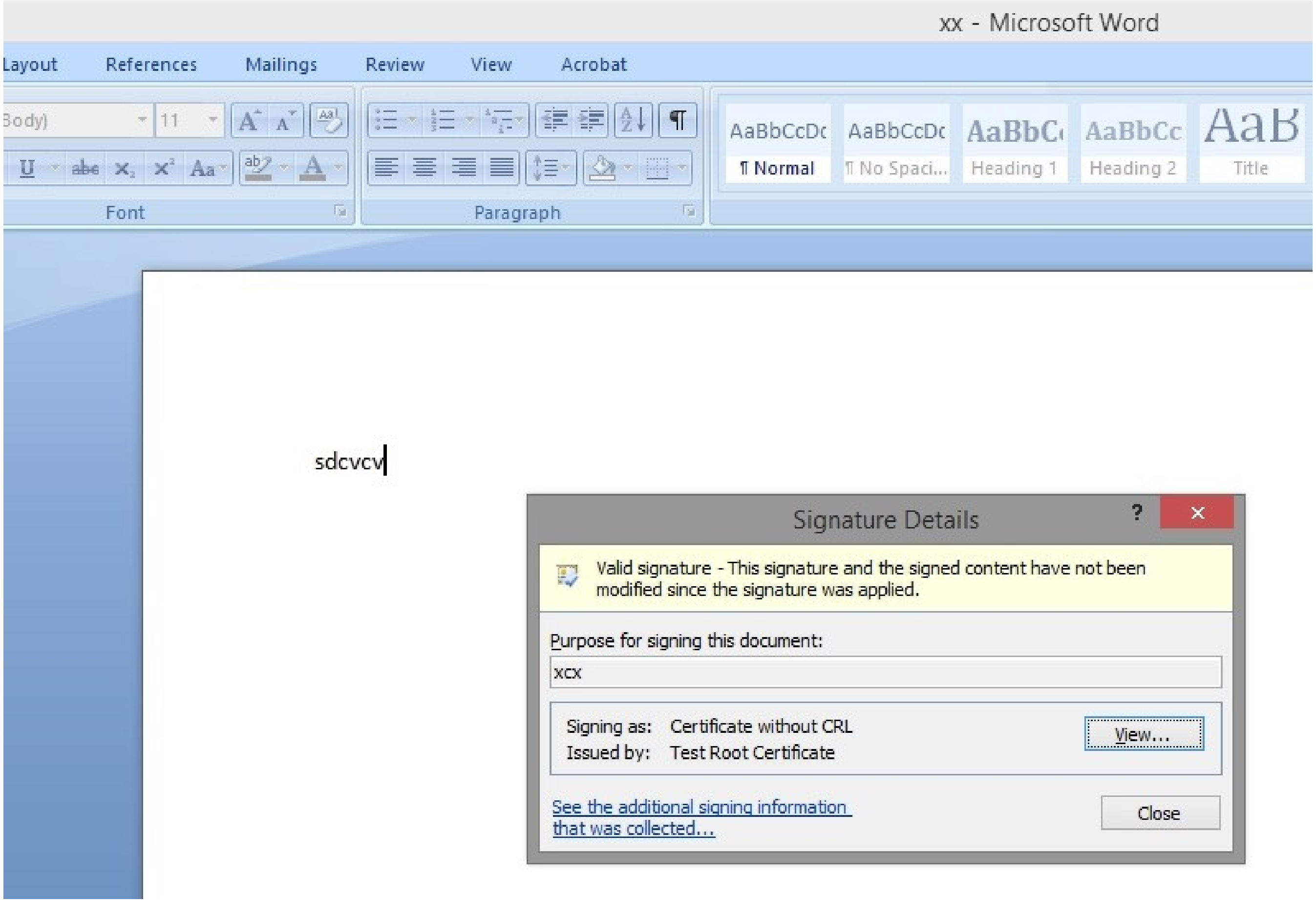
xcx

Signing as: Certificate without CRL

Issued by: Test Root Certificate

See the additional signing information that was collected...

Office 2010 - Digital signature made by a certificate without CRL – signature is considered invalid



Valid signature - This signature and the signed content have not been modified since the signature was applied.

Purpose for signing this document:

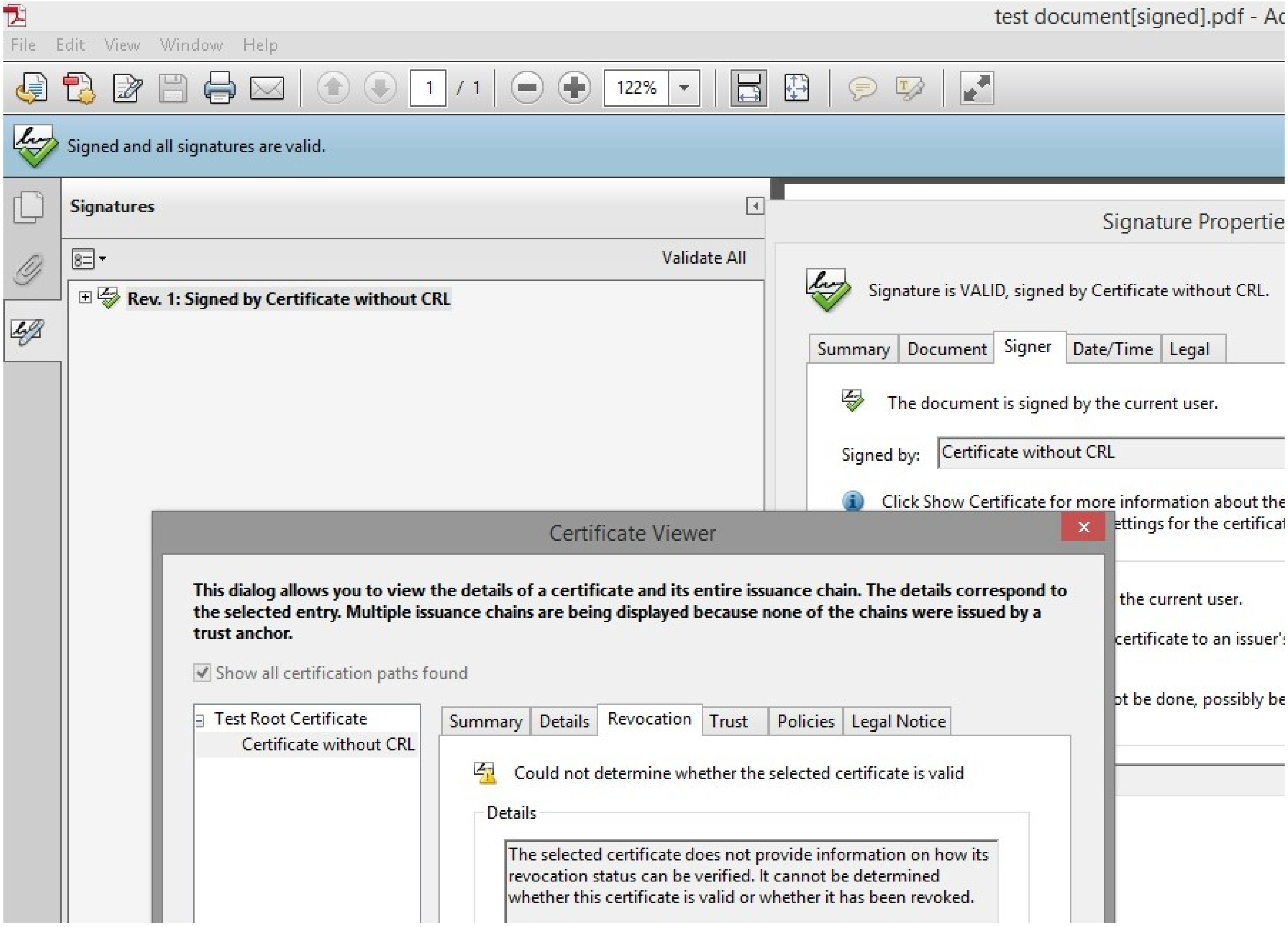
xcx

Signing as: Certificate without CRL

Issued by: Test Root Certificate

See the additional signing information that was collected...

Office 2007 - Digital signature made by a certificate without CRL – signature is considered valid


test document[signed].pdf - Ac
File Edit View Window Help
1 / 1
122%
Signatures
Validate All
Signature Propertie
Summary Document Signer Date/Time Legal
Certificate Viewer
Summary Details Revocation Trust Policies Legal Notice
Details
ettings for the certificat
the current user.
certificate to an issuer's
ot be done, possibly be

Signed and all signatures are valid.

Rev. 1: Signed by Certificate without CRL

Signature is VALID, signed by Certificate without CRL.

The document is signed by the current user.

Signed by: Certificate without CRL

Click Show Certificate for more information about the

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry. Multiple issuance chains are being displayed because none of the chains were issued by a trust anchor.

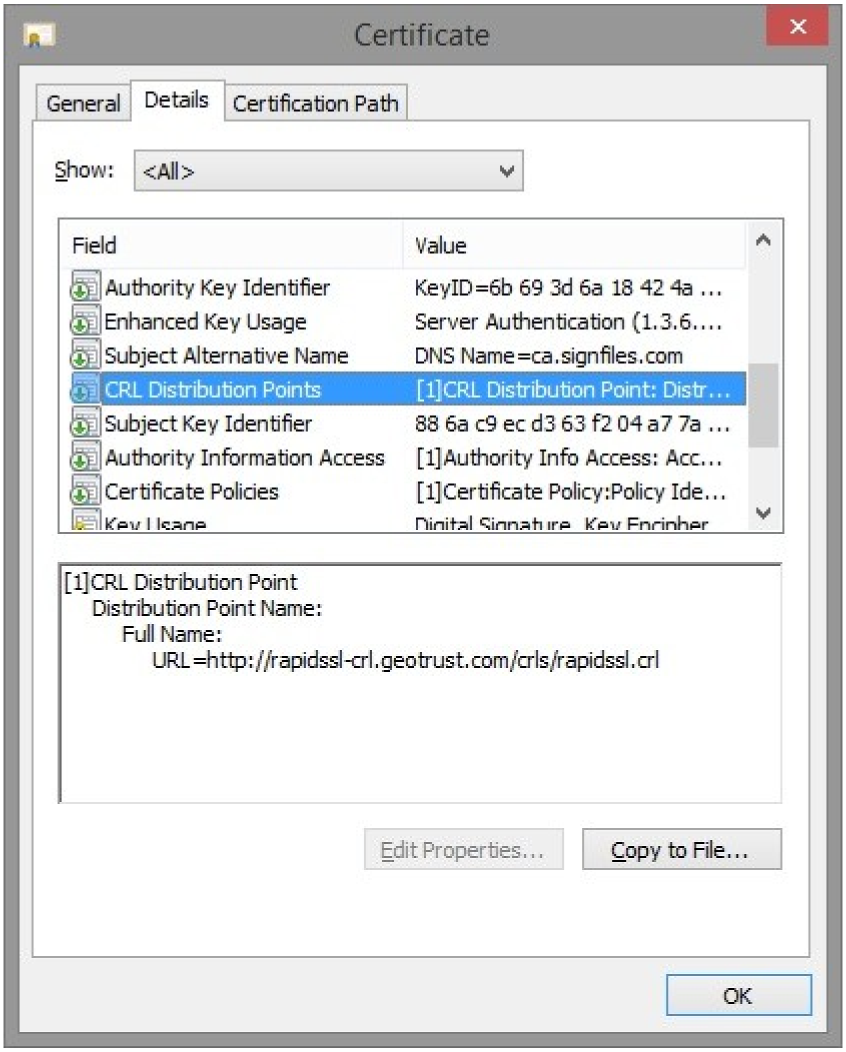
☑ Show all certification paths found

Test Root Certificate
Certificate without CRL

Could not determine whether the selected certificate is valid

The selected certificate does not provide information on how its revocation status can be verified. It cannot be determined whether this certificate is valid or whether it has been revoked.

Adobe Reader - Digital signature made by a certificate without CRL – signature is considered valid



Show: <All>

Field	Value
Authority Key Identifier	KeyID=6b 69 3d 6a 18 42 4a ...
Enhanced Key Usage	Server Authentication (1.3.6....
Subject Alternative Name	DNS Name=ca.signfiles.com
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Subject Key Identifier	88 6a c9 ec d3 63 f2 04 a7 7a ...
Authority Information Access	[1]Authority Info Access: Acc...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Key Usage	Digital Signature, Key Encipher

```
[1]CRL Distribution Point
     Distribution Point Name:
          Full Name:
               URL=http://rapidssl-crl.geotrust.com/crls/rapidssl.crl
```

A digital certificate with CRL