

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.

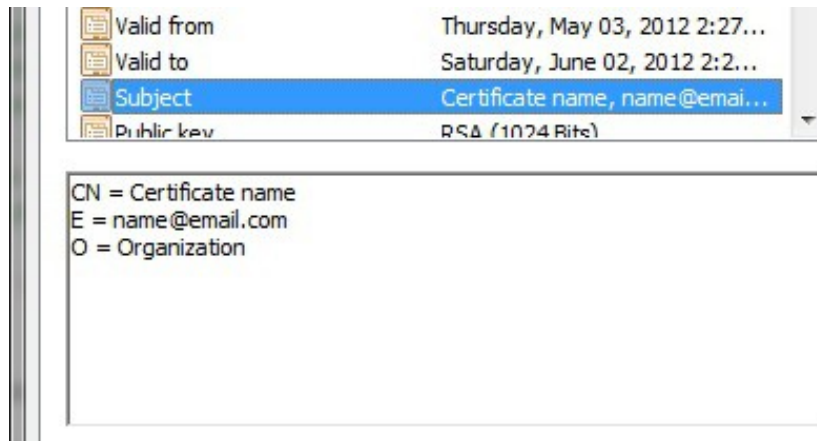
Table of Contents

X.509 Certificate Generator User Manual.....	1
Introduction.....	1
Links.....	1
Warning and Disclaimer.....	1
Trademarks.....	1
Digital Certificate Properties.....	3
Certificate Subject.....	3
Validity Period.....	3
Cryptographic Algorithms.....	4
Key Usage.....	5
Enhanced Key Usage.....	6
PFX Certificate Generator.....	7
Issuing Certificates.....	8
Issuing Certificates Signed by a Root Certificate.....	10
Issue the Root Certificate.....	10
Saving the Root Certificate Public Part.....	11
Issue the Client Certificate Signed by the Root Certificate.....	12
Installing a PFX Certificate.....	14
Issuing Certificates from CSR (SSL Certificates).....	15
Create the CSR for an IIS website.....	16
Signing the CSR Request with the Root Certificate.....	17
Installing the CSR response on the IIS website.....	18
Validating the SSL certificate.....	19
Smart Card Certificate Generator.....	20
Microsoft Certificate Store.....	21
How to Access Microsoft Certificate Store.....	21
Export the Root Certificate from Microsoft Store.....	22
Import the Root Certificate on Microsoft Store.....	22
Observations.....	24
X.509 Certificate Generator and CRL.....	24

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.

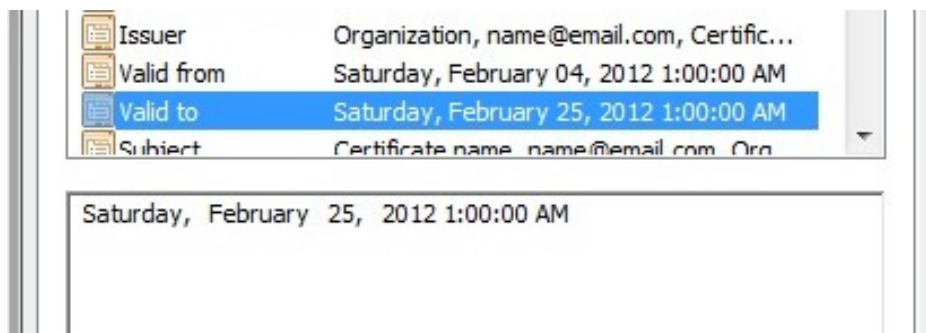


Certificate Subject

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.



Certificate Validity period

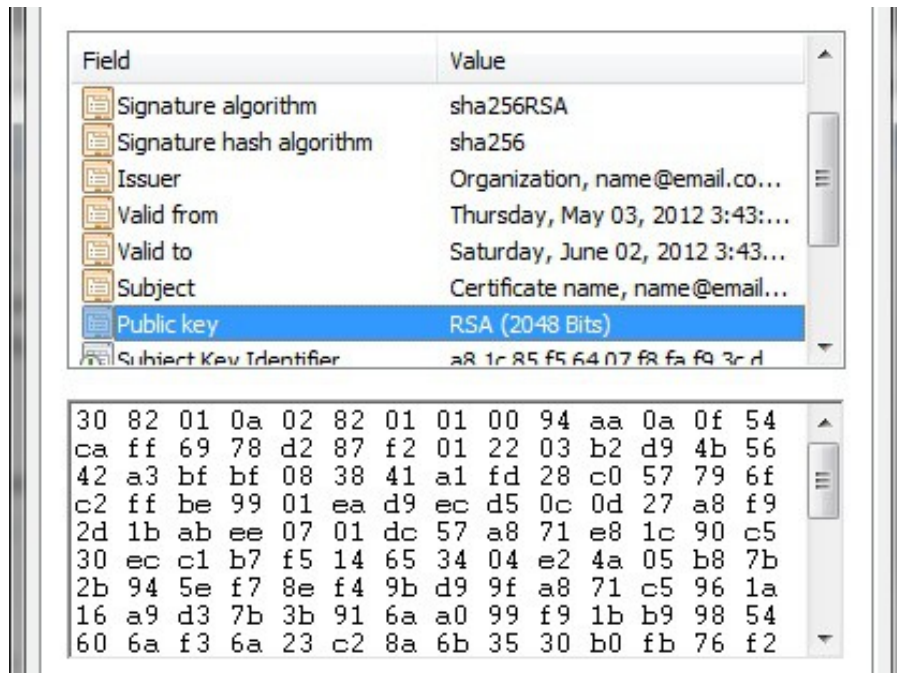
Cryptographic Algorithms

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.



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.

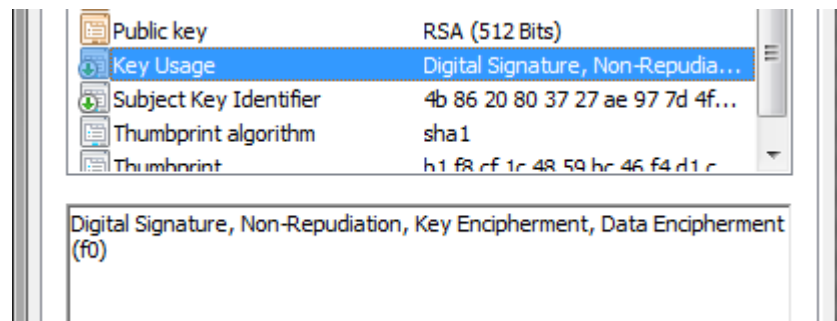
KeyEncipherment - The certificate use the public key for key transport.

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*.



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.

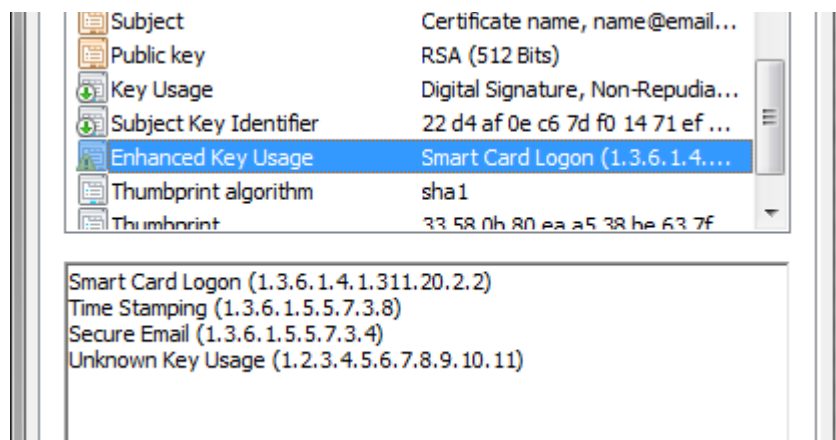
Some of Enhanced Key Usages available by default are:

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.

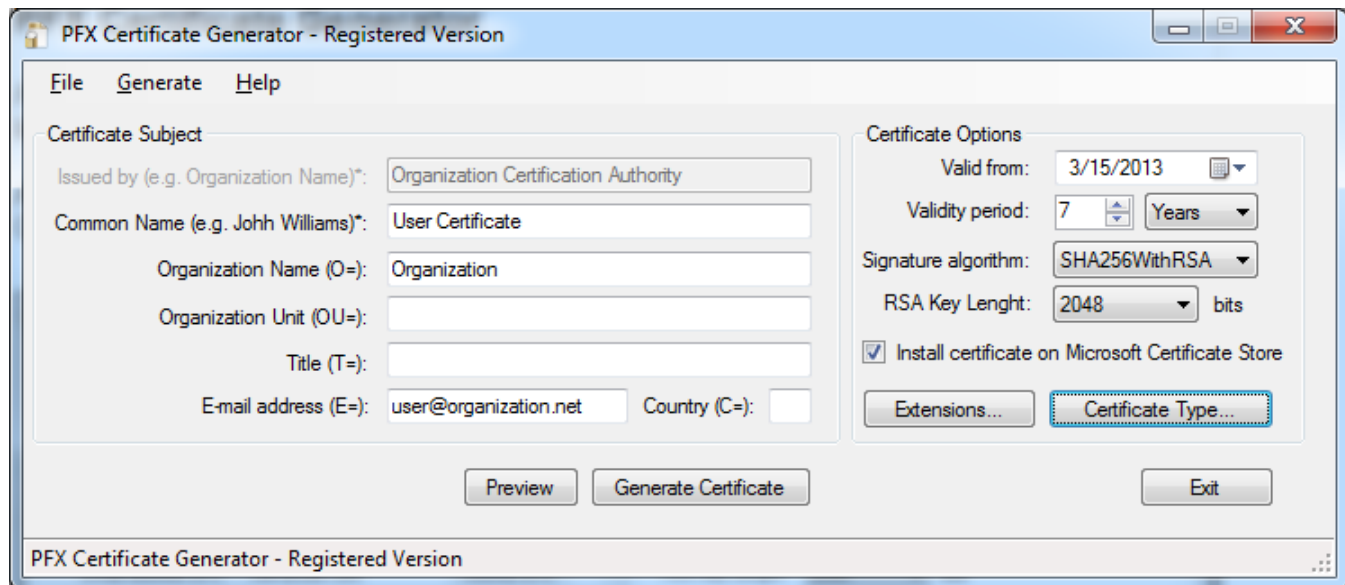


Enhanced Key Usage (marked as Critical Extension)

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.



The screenshot shows the main interface of the PFX Certificate Generator. The window title is "PFX Certificate Generator - Registered Version". It has a menu bar with "File", "Generate", and "Help". The interface is divided into two main sections: "Certificate Subject" on the left and "Certificate Options" on the right. The "Certificate Subject" section contains fields for "Issued by (e.g. Organization Name)*:" (filled with "Organization Certification Authority"), "Common Name (e.g. John Williams)*:" (filled with "User Certificate"), "Organization Name (O=):" (filled with "Organization"), "Organization Unit (OU=):" (empty), "Title (T=):" (empty), "E-mail address (E=):" (filled with "user@organization.net"), and "Country (C=):" (empty). The "Certificate Options" section contains "Valid from:" (filled with "3/15/2013"), "Validity period:" (filled with "7" and "Years"), "Signature algorithm:" (filled with "SHA256WithRSA"), "RSA Key Length:" (filled with "2048" and "bits"), and a checked checkbox for "Install certificate on Microsoft Certificate Store". There are buttons for "Extensions...", "Certificate Type...", "Preview", "Generate Certificate", and "Exit". The status bar at the bottom says "PFX Certificate Generator - Registered Version".

PFX Certificate Generator main interface

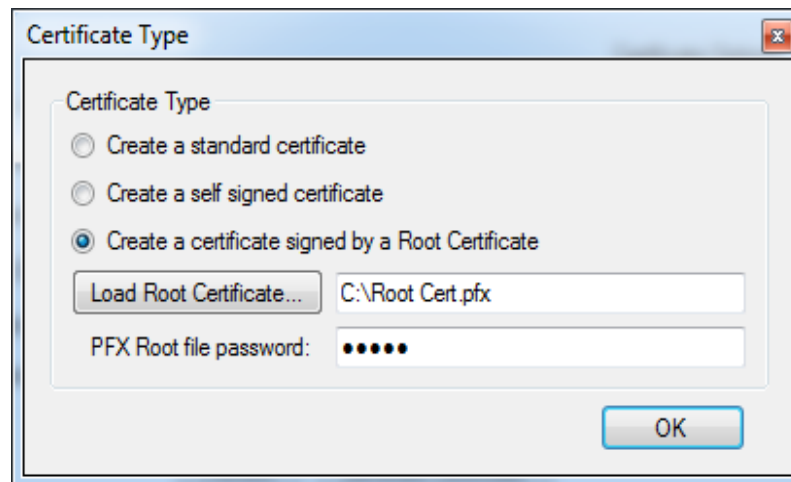
After the PFX certificate is generated, if "Install certificate on local computer (Microsoft Store)" is checked, the certificate can be automatically installed on local computer Certificate Store.

Issuing Certificates

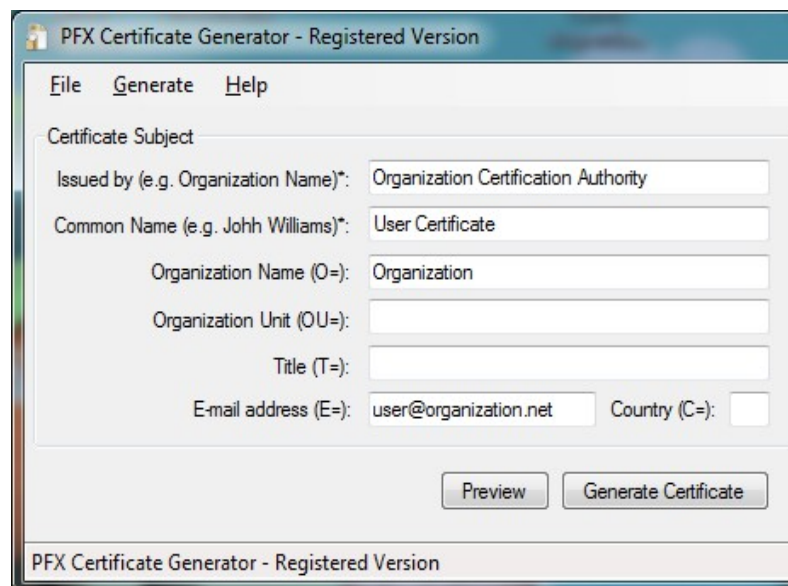
By default, the certificates issued by [PFX Certificate Generator](#) are signed by a Root Certificate created on the fly.

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](#).

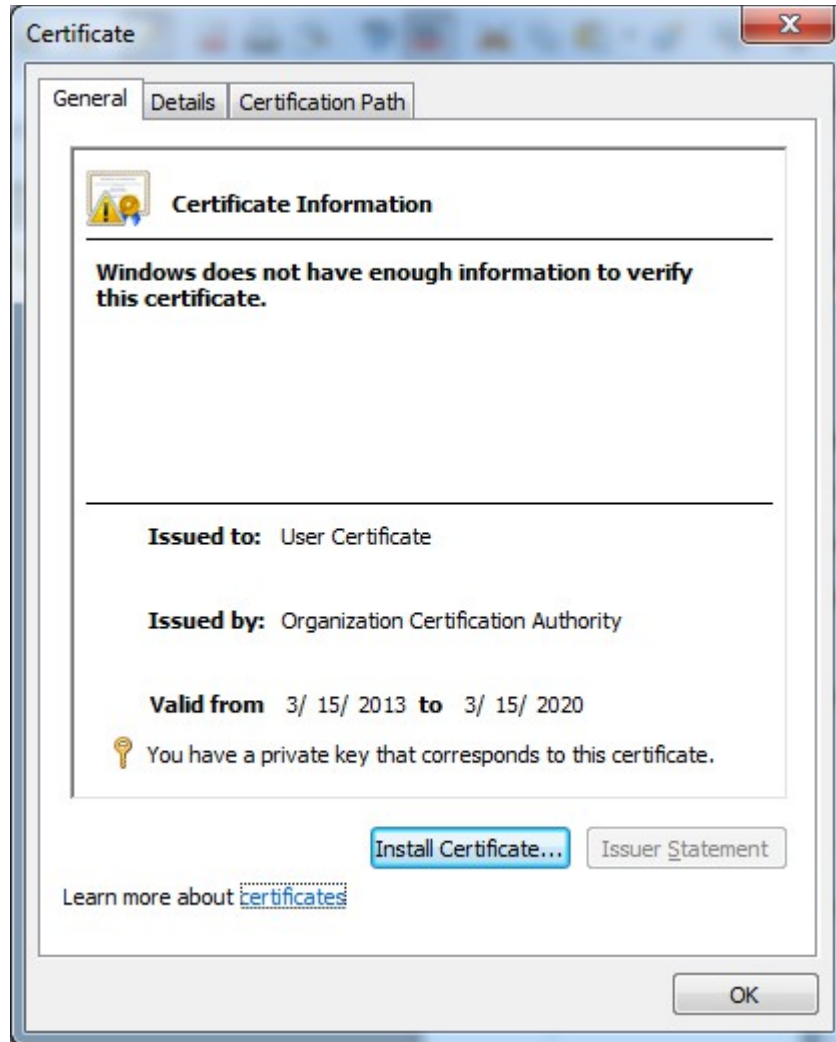


Self-signed certificates



Certificate subject

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



Self-signed certificate

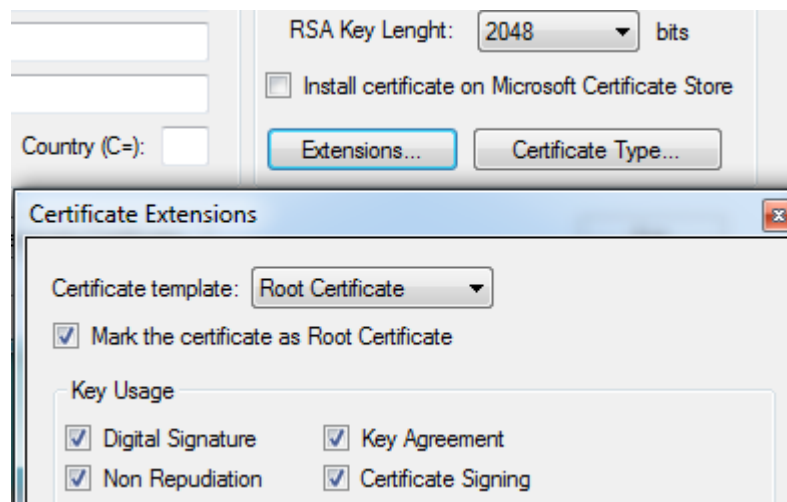
Issuing Certificates Signed by a Root Certificate

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.

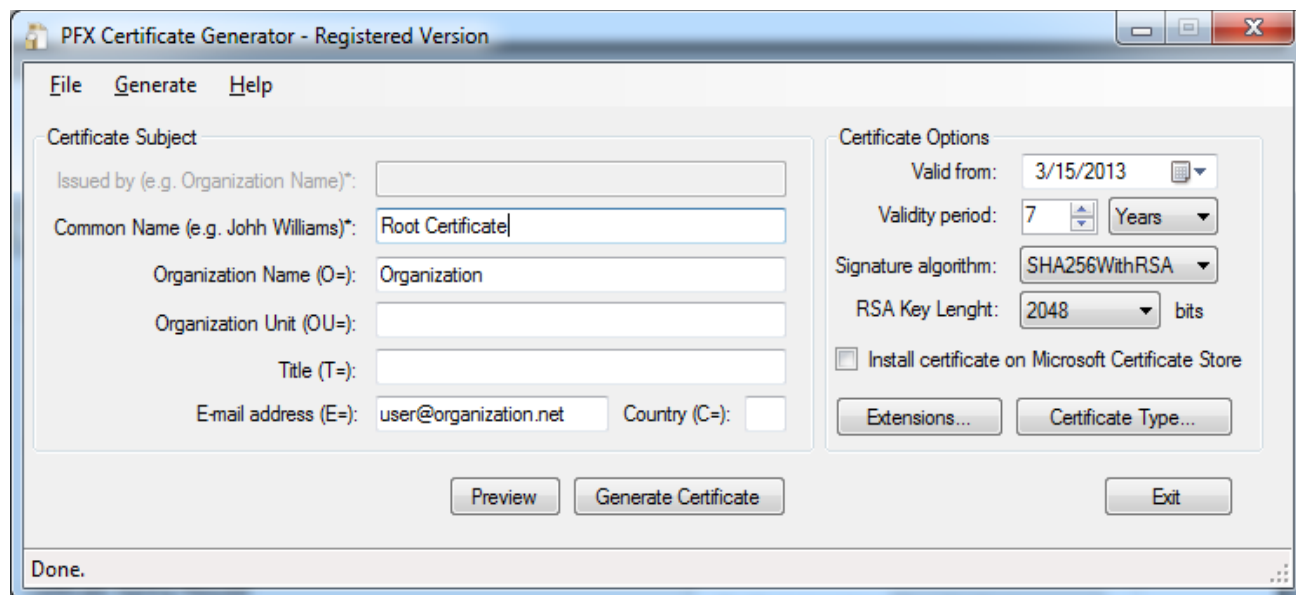
A Root Certificate (CA certificate) is a special type of certificate that can be used to digitally sign other certificates.

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



Root Certificate Template

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



Creating a Root Certificate

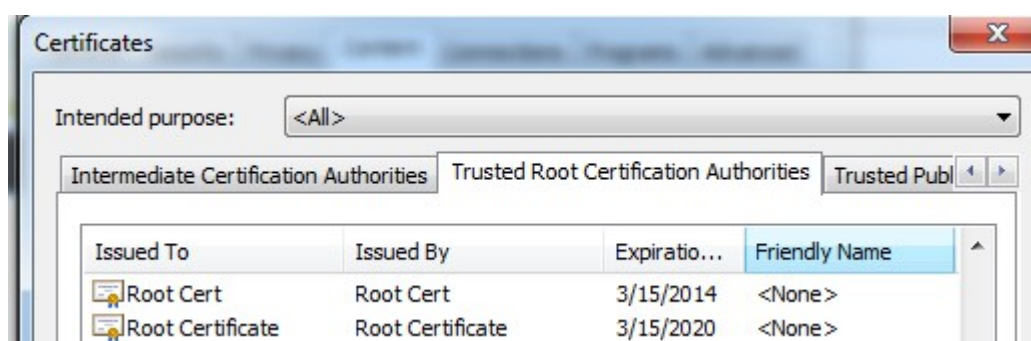
Saving the Root Certificate Public Part

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 be 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 computer first.

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

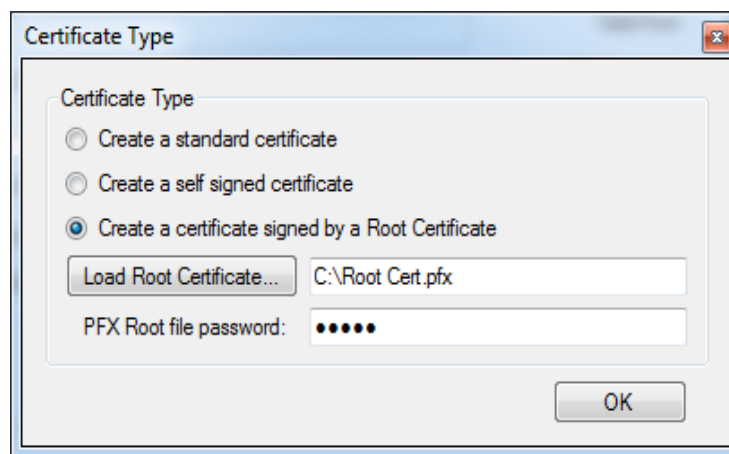


The resulting .CER file must be installed on Microsoft Certificate Store - Trusted Root Certification Authorities Tab (see section: *Microsoft Certificate Store - Import the Root Certificate on Microsoft Store* for more details).

Issue the Client Certificate Signed by the Root Certificate

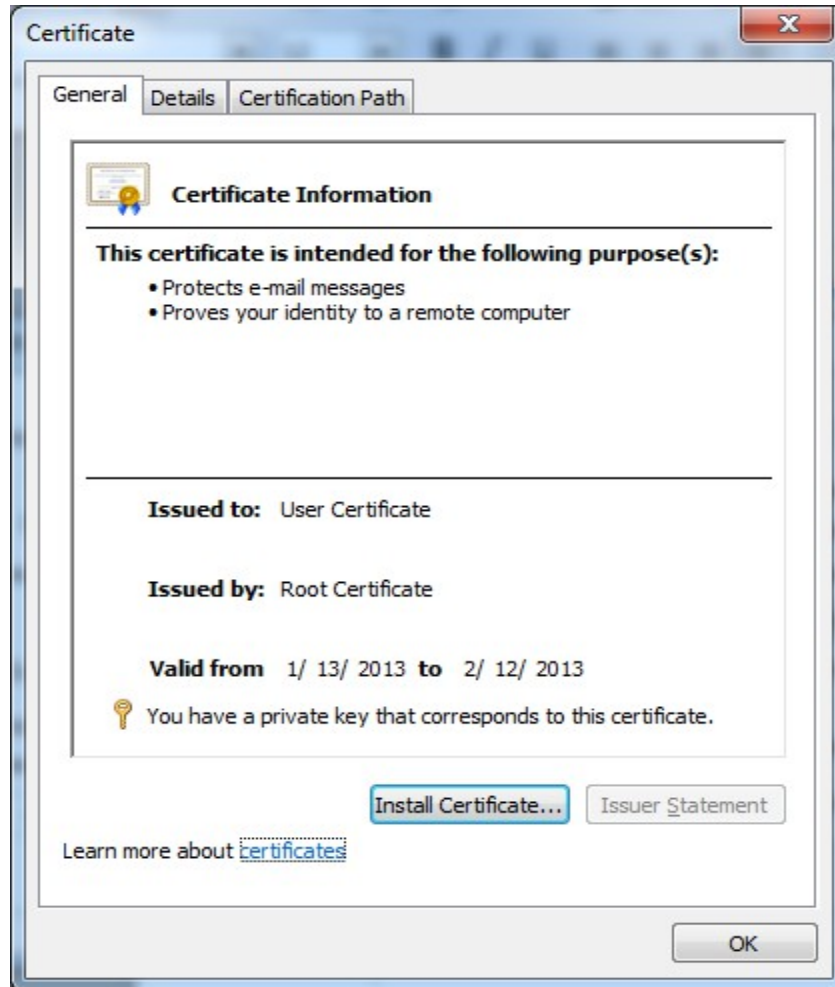
In order to issue certificates signed by this Root Certificate, do the following:

- 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.

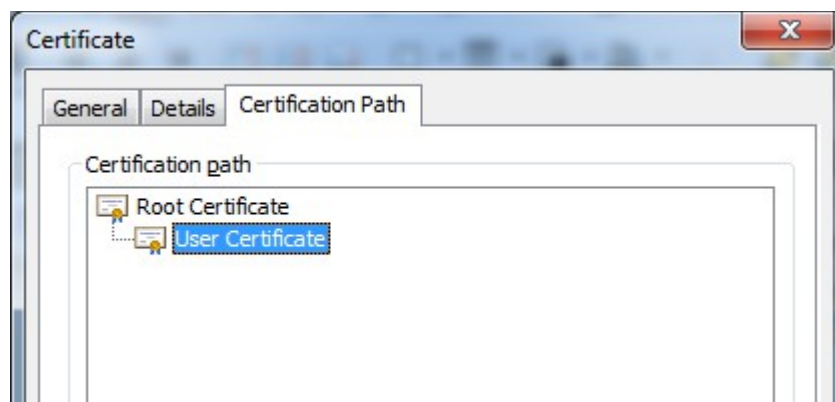


Issue certificates signed by a Root Certificate

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



Certificate signed by a Root Certificate



Certification Path

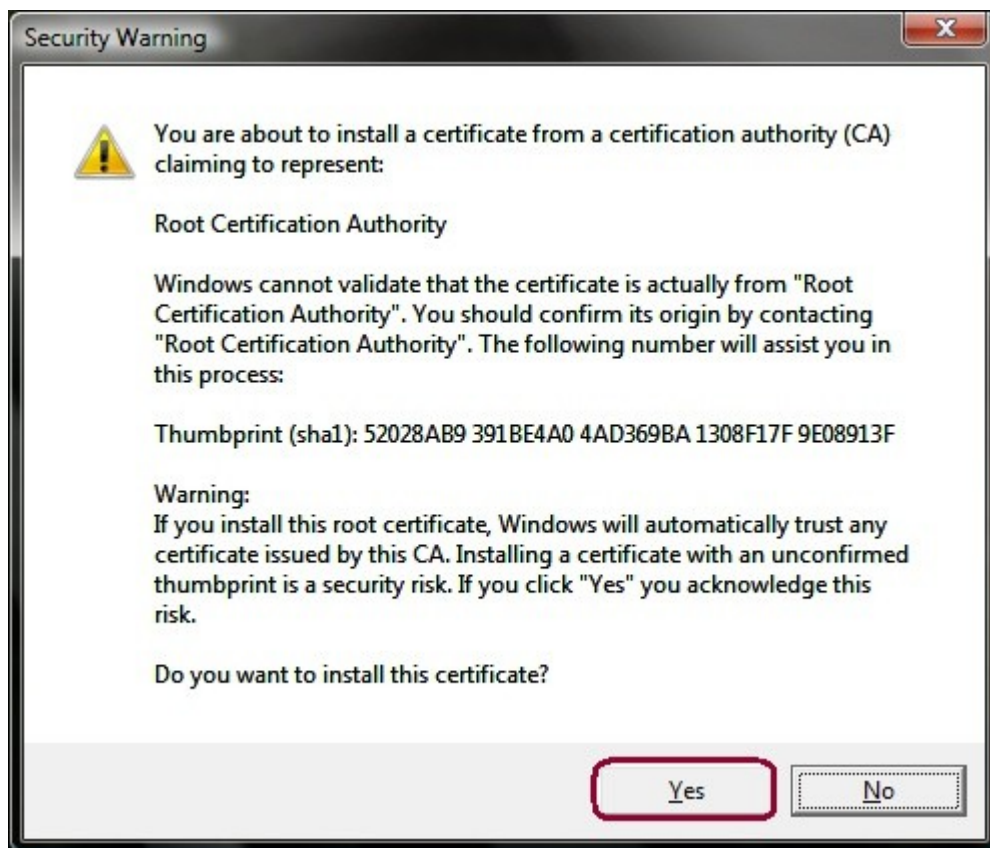
Installing a PFX Certificate

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:



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.

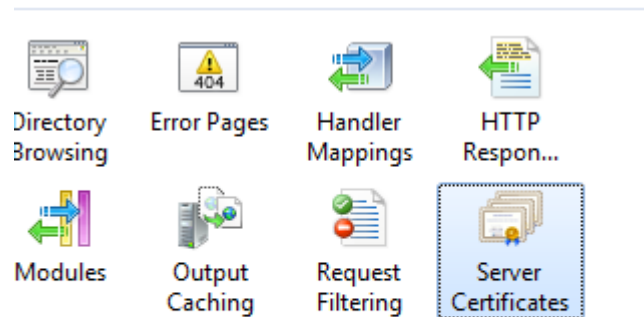
```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDKTCAPICAQAwTjELMAKGA1UEBhMCVVMxMzA1BgNVBAsMAmVlMQswCQYDVQQH
DAJlZTElMAKGA1UECgwCZWUXCzA1BgNVBAsMAmVlMQswCQYDVQDDAJlZTCBnzAN
BgkqhkiG9w0BAQEFAA0BgjQAwgYkCgYEA1C+FhYQiBOSHjTy+g80kP/HlFeuw1cpx
m0ty2kprQpo5RfgPTiCFh+AtUjQsvuCyKiC000+8JdmhHE2s7BvEAX7IedlFUm/v
XdPw8Qpwn3Zj7Uq4zMgFxlHx7dLQeiuVWeTuz1nUWIrKX00owvfw0jFa+OE64wA+
M+n4N/zUmZMAwEAAaCCAZkwGgYKKwYBBAGCNw0CAZEMFgo2LjeUnZYwMC4yMDUG
CS5GAQQBgjcvFDEoMCYCAQUmCHvZXXJtLVBDdA51c2VybS1Q1x1c2VybQwHbW1j
LmV4ZTB5BgorBgEEAYI3DQICMwQwYgIBAR5aAE0AaQ8jAHIAbwBzAG8AZgB0ACAA
UgBTAEEAIABTAEMAaABhAG4AbgB1AGwAIABDAHIAeQ8wAHQAbwBnAHIAyQ8wAGgA
aQ8jACAAUABYAG8AdgBpAGQAZQByAwEAMIHPBgkqhkiG9w0BCQ4xgcEwgb4wDgYD
VR0PAQH/BAQDAgTwMBMGA1UdJQQMMAoGCCsGAQUFBwMBMHgGCsqG5Ib3DQEJDRRr
MGkwDgYIKoZIhvcNAwICAgCAMA4GCCqG5Ib3DQMEAgIAgDALBg1ghkgBZQMEASow
CwYJYIZIAWUDBAETMASGCWCGSAF1AwQBAjALBg1ghkgBZQMEAUwBwYFKw4DAgcw
CgYIKoZIhvcNAwcwHQYDVRO0B8YEFJCT1q/93eBh10+a/qy3Esx2jJBHMA0GCsqG
5Ib3DQEBBQUAA4GBAFAsJK8bnaS7n3i/E4WBJ/15shtEakif8YORpidYo5UyR/U7
khQLws0QyESwOd5BCFtS2JsdvXkTLJYDT0o17ZrnmclN+OwxETlp8rcAVY02MoNg
JfQeoGyg12RGVlcpiodLSmkZ5BE7VPfS5QK0wJ01GHiykyj5YOubHOjVhBj3
-----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*.

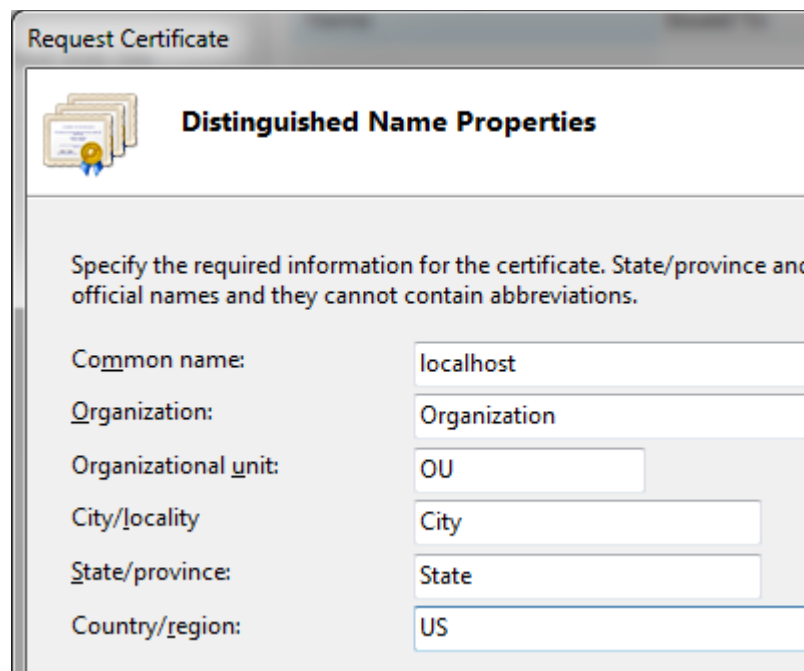
Create the CSR for an IIS website

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).

A screenshot of the 'Request Certificate' dialog box in IIS Manager. The 'Distinguished Name Properties' tab is active, showing a list of fields for specifying certificate information. The fields and their values are: Common name: localhost, Organization: Organization, Organizational unit: OU, City/locality: City, State/province: State, and Country/region: US. A note at the top states: 'Specify the required information for the certificate. State/province and official names and they cannot contain abbreviations.'

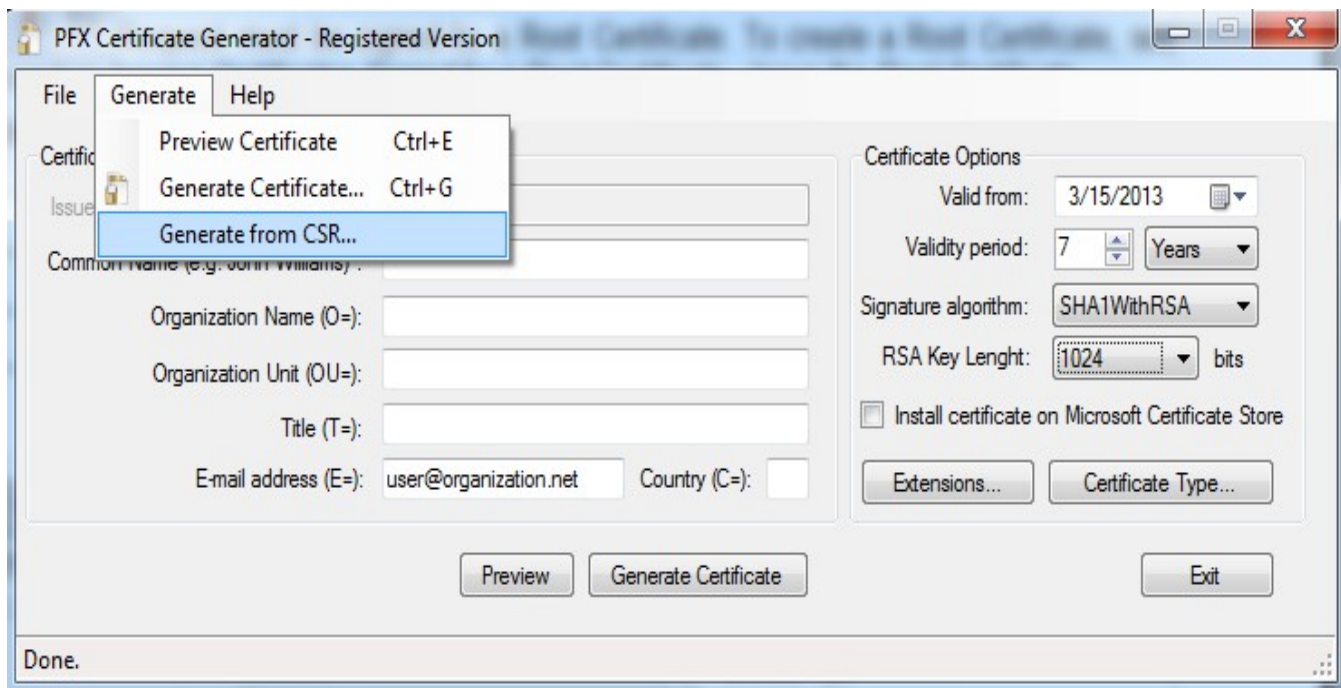
Creating the CSR Request

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:

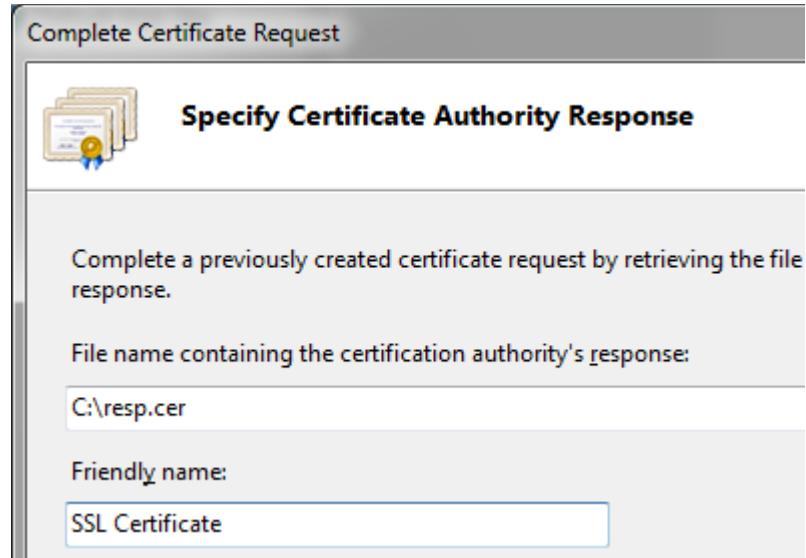
- select *SSL Certificate* template from the *Certificate Type* tab.
- Load the Root Certificate previously created
- Load the CSR by pressing *Generate from CSR...* menu item
- Save the resulting .CER file (e.g. c:\resp.cer)



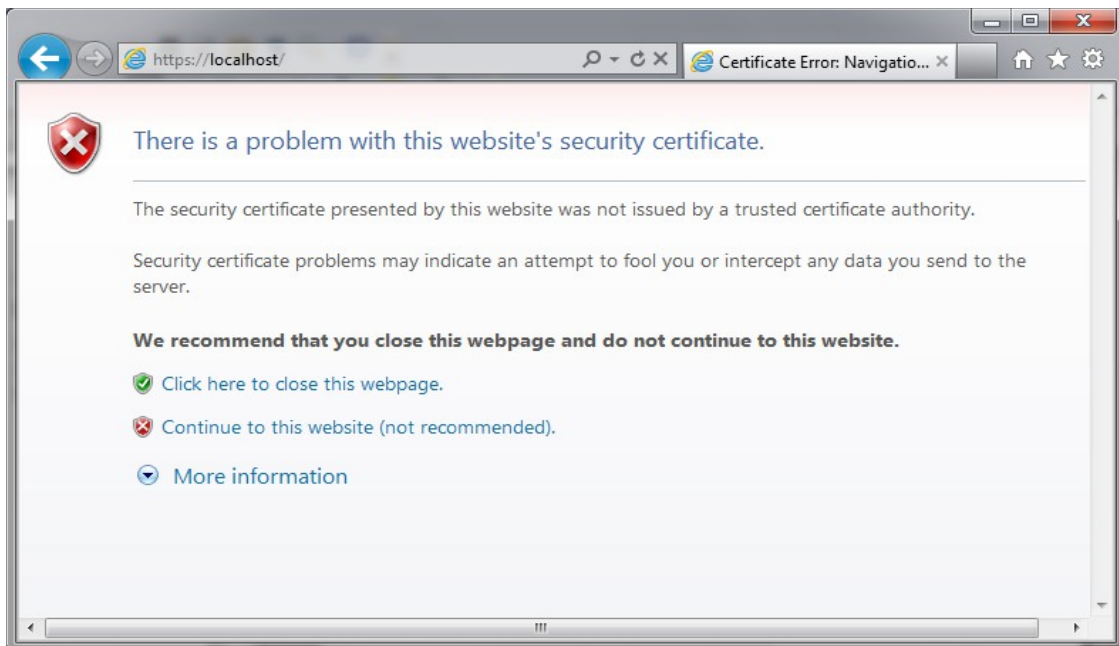
Signing the CSR with a Root Certificate

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.



Right now, the certificate is installed. To test the SSL website, go to <https://localhost>.



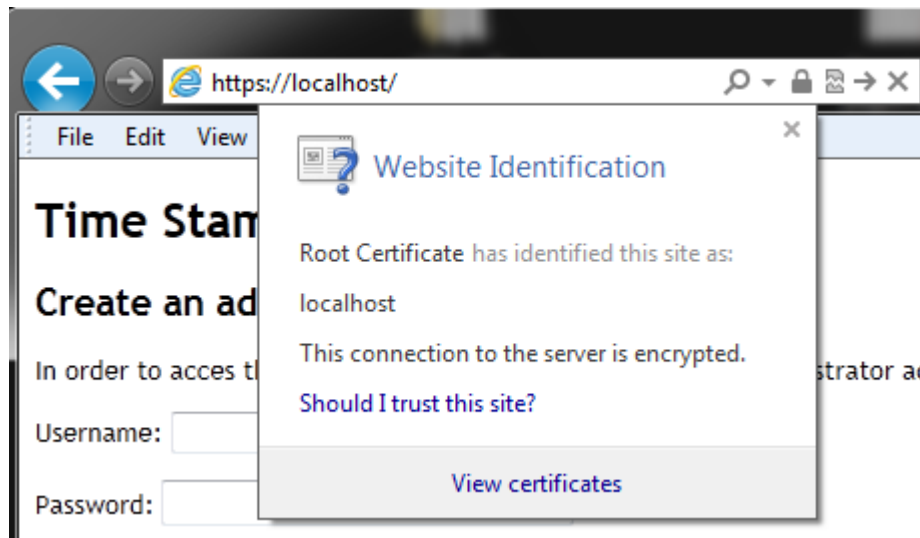
Untrusted certificate

Validating the SSL certificate

If the SSL certificate is considered untrusted by your web browser, you must install the Root Certificate public 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:



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 public 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.

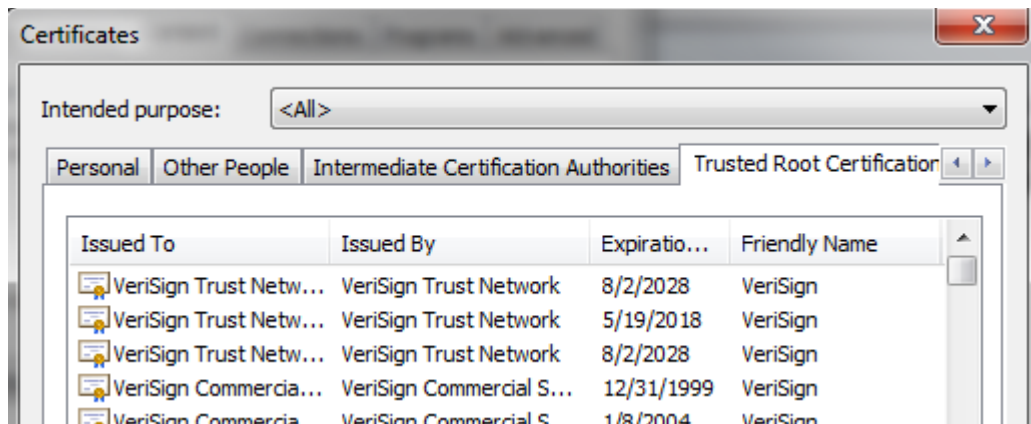
The screenshot shows the 'Smart Card Certificate Generator - Registered Version' application window. The interface includes a menu bar with 'File', 'Generate', and 'Help'. The main area is divided into several sections:

- CSP:** A dropdown menu for 'Smart Card Certificate Service Provider' is set to 'eToken Base Cryptographic Provider'. There is an unchecked checkbox for 'Include Microsoft CSP (software)'.
- Key Usage:** A group box containing checkboxes for 'Digital Signature' (checked), 'Non Repudiation' (checked), 'Key Encipherment' (checked), 'Data Encipherment' (checked), 'Key Agreement' (unchecked), 'Certificate Signing' (unchecked), and 'CRL Signing' (unchecked).
- Certificate Subject:** Fields for 'Issued to (CN=):', 'Organization (O=)', 'Organization Unit (OU=)', 'Title (T=)', 'E-mail address (E=)', and 'Country (C=)'. The values are 'Smart Card User Certificate', 'Client Organization', 'Accounting', an empty field, 'user@organization.com', and an empty field respectively.
- Enhanced Key Usage:** A group box with checkboxes for 'Secure Email' (checked), 'Client Authentication' (checked), 'Document Signing' (checked), 'Add custom Enhanced Key Usage OIDs (comma delimited)' (checked), 'Time Stamping' (unchecked), 'OCSP Signing' (unchecked), 'Any Purpose' (unchecked), 'IPSEC User' (unchecked), 'IPSEC End System' (unchecked), 'IPSEC Tunnel' (unchecked), and 'Smartcard Logon' (unchecked). Below these is a text field containing '1.2.3.3.3.1.2,1.3.2.2.1.3.4|'. There is also an unchecked checkbox for 'Enhanced Key Usage extensions are marked as critical'.
- Certificate Options:** Fields for 'Valid from:' (1/25/2013), 'Validity period:' (1), and 'RSA Key Length:' (2048 bits). The 'Valid from' field has a calendar icon.
- Template:** A dropdown menu for 'Certificate template:' is set to 'Regular User'. There is an unchecked checkbox for 'Mark the certificate as Root Certificate'.

At the bottom, there are buttons for 'Preview', 'Generate certificate', and 'Exit'. The status bar at the very bottom reads 'Smart Card Certificate Generator - Registered Version'.

Microsoft Certificate Store

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

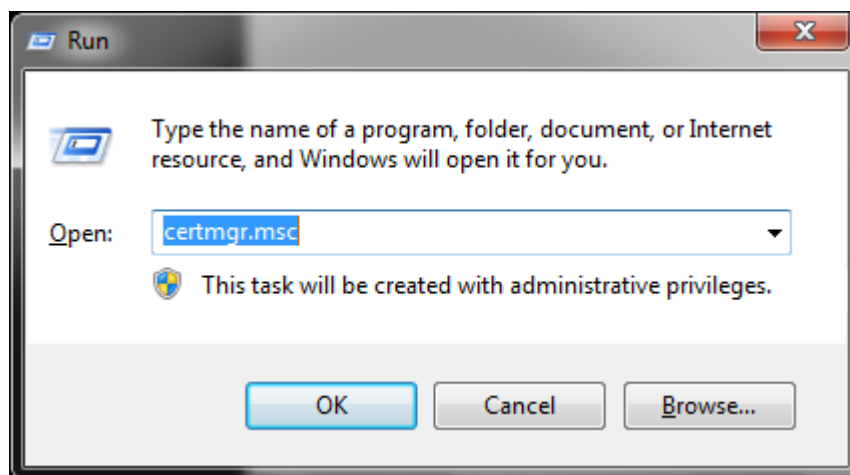


Microsoft Certificate Store

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.



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 filename 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, an warning message can appear.

If you digitally sign a PDF file and want to validate Adobe PDF digital signatures, read this document:

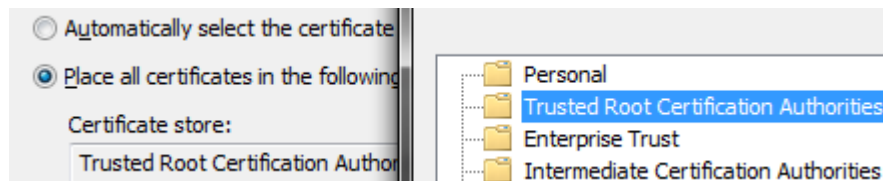
<http://www.signfiles.com/manuals/ValidatingDigitalSignaturesInAdobe.pdf>

Import the Root Certificate on Microsoft Store

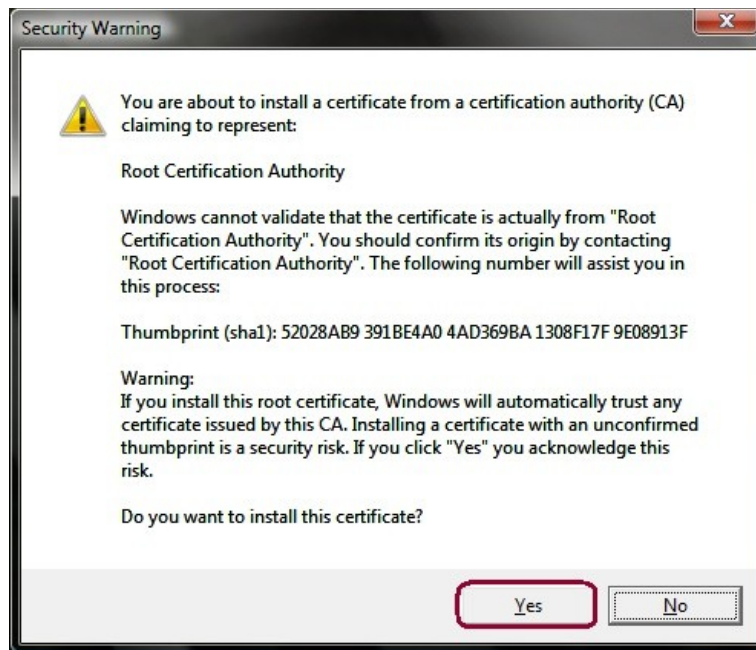
- Copy the exported .cer file obtained above (*Export the Root Certificate from Microsoft Store*) on the target computer
- Right click on the imported .cer file and select *Install Certificate*



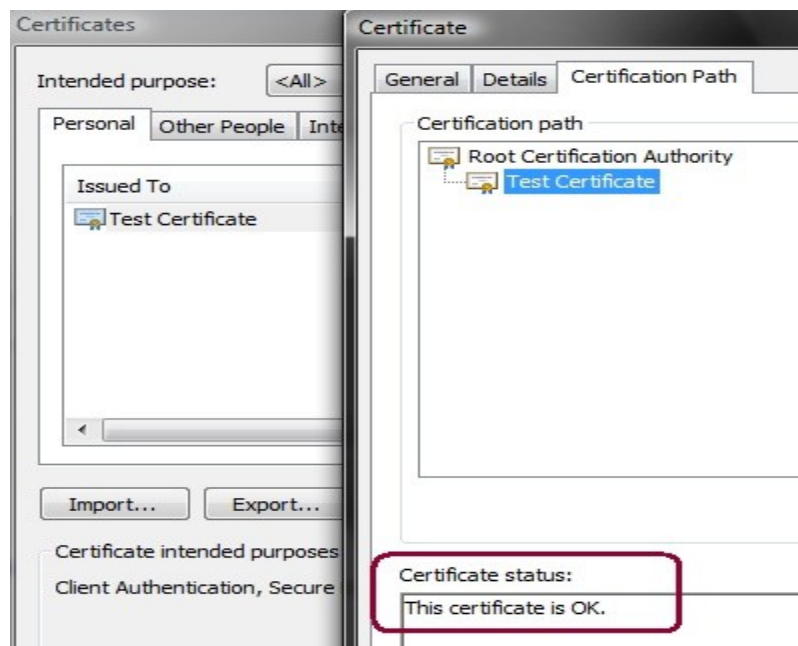
- Click *Next* and select *Place all certificates in the following store*
- Click *Browse* and select *Trusted Root Certification Authorities*



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



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.



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.

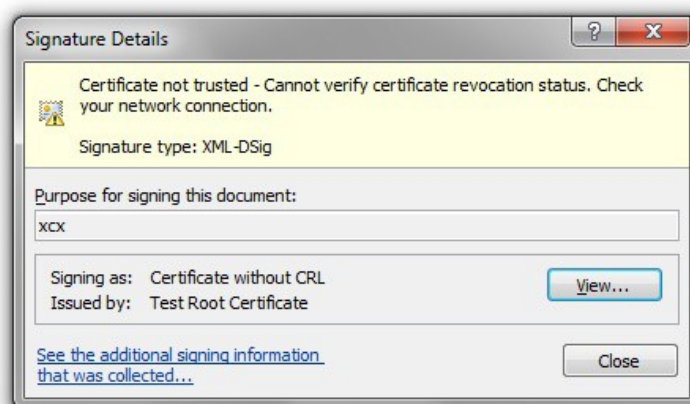
According to the X.509 standard, the CRL field is optional and should be ignored if it not exists but in Office 2010 digital signatures this field is mandatory.

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

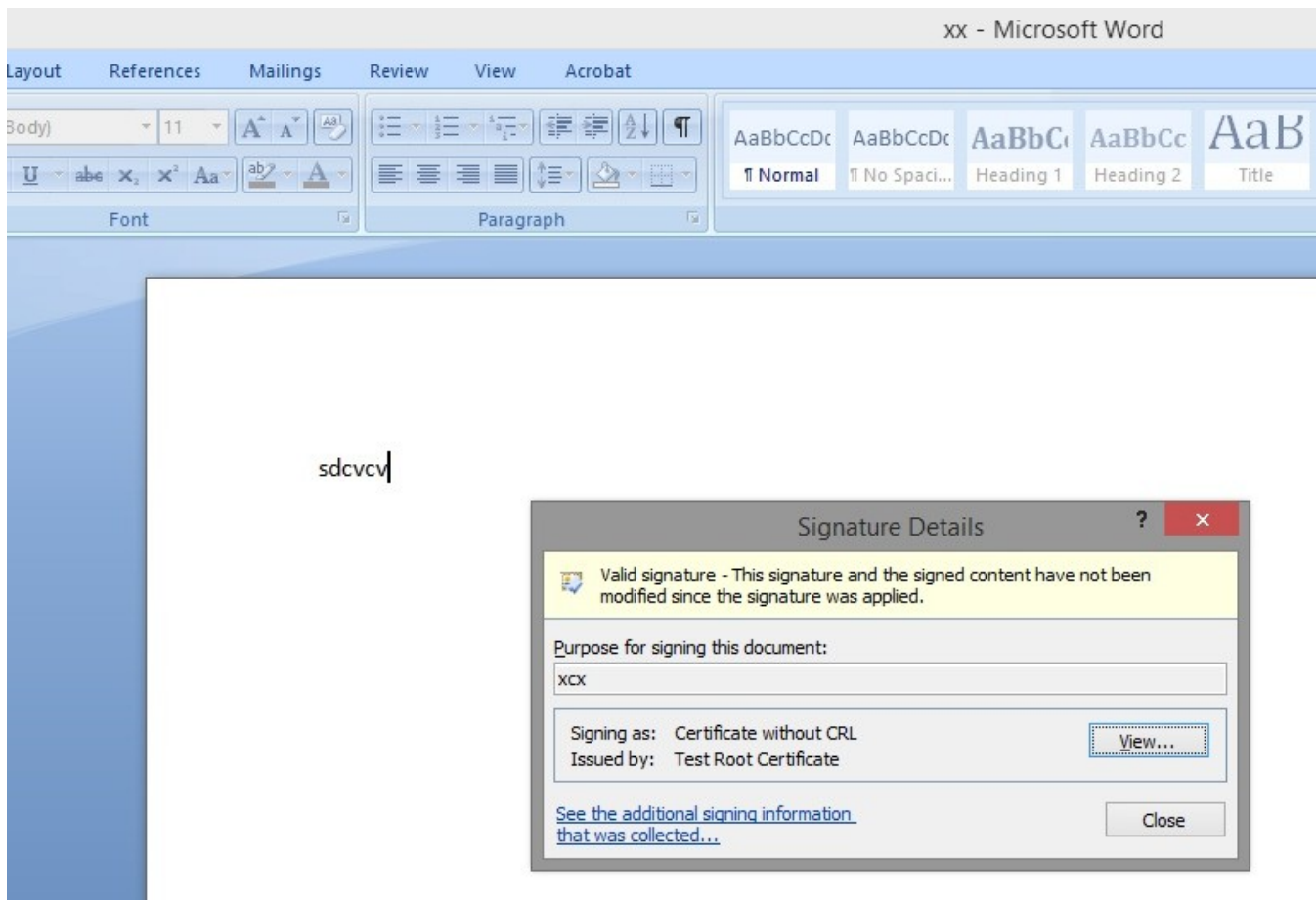
The CRL file MUST be published on the web (e.g. <http://rapidssl-crl.geotrust.com/crls/rapidssl.crl>) but X.509 Certificate Generator is a desktop product and cannot generate a CRL file and publish it on the web. This is the reason why the CRL attribute is not set on the certificates issued by X.509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



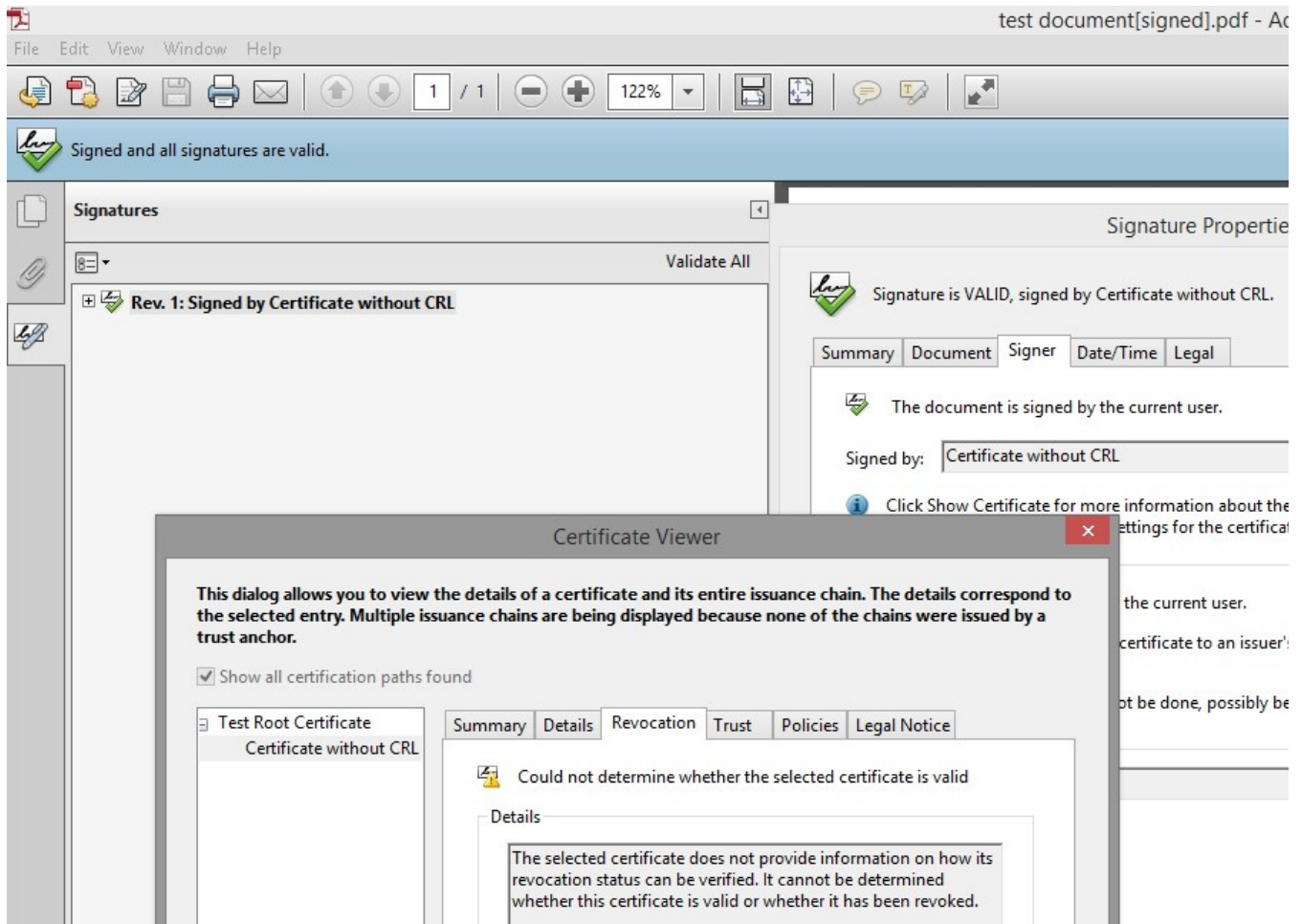
sdvcv



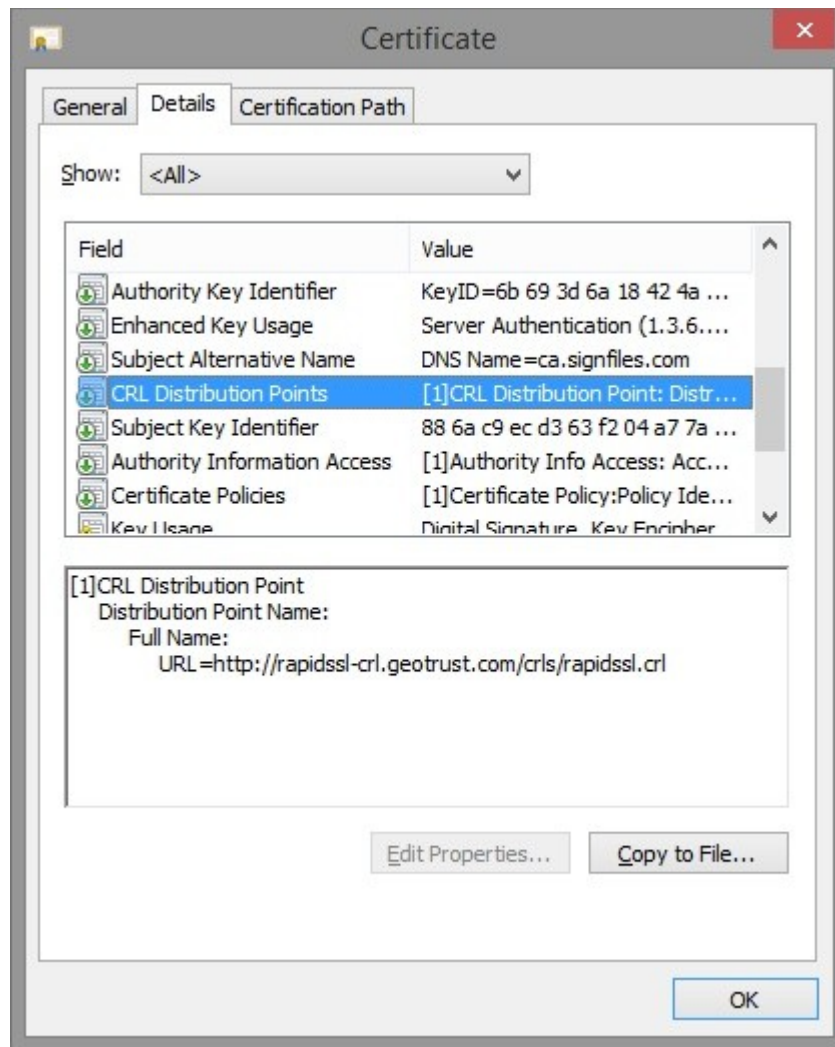
Office 2010 - Digital signature made by a certificate without CRL – signature is considered invalid



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



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



A digital certificate with CRL