

HOWTO: How to manage X509 certificates with XCA for their correct implementation in Panda GateDefender Integra.



'How-to' guides to configure the management of X509 certificates with XCA

Panda Security wants you to get the most out of GateDefender Integra. For this reason, we offer you all the information you need about the characteristics and configuration of the product. Refer to <http://www.pandasecurity.com/enterprise/solutions/?sitepanda> for more information.

The software described in this document is delivered under the terms and conditions of the end user license agreement and can only be used after accepting the terms and conditions of said agreement.

The anti-spam technology included in this product belongs to Cloudmark. The content filtering technology included in this product belongs to Cobion.

Copyright notice

© Panda Security 2008. All rights reserved. Neither the documents nor the programs that you may access may be copied, reproduced, translated or transferred to any electronic or readable media without prior written permission from Panda Security, c/ Gran Vía Diego López de Haro, 4 48001 Bilbao (Biscay) Spain.

Registered trademarks

Panda Security™. TruPrevent: Registered in U.S.A Patent and Trademark Office. Windows Vista and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries. All other product names may be registered trademarks of their respective owners. D. L. BI-1915-07

© Panda Security 2008. All rights reserved.

Contents

1. INTRODUCTION	5
2. INSTALLATION	5
3. PKI MANAGEMENT	6
3.1. Step 1: Create a database.	6
3.2. Step 2: Create a CA (Certification Authority).....	7
3.3. Step 3: Create a local certificate signed by your CA.....	10
3.4. Local certificate exportation for later use.....	13
4. CSR CERTIFICATE SIGNING REQUEST MANAGEMENT	16
4.1. Step 1: Create the signing request in Integra	16
4.2. Steps to create CSR in Panda GateDefender Integra	16
4.3. Step 2: Sign CSR in XCA	17
5. REVOCATION LIST MANAGEMENT (CRL)	18

Diagrams

Illustration 1- Save the database created -	6
Illustration 2- CA configuration -	7
Illustration 3- Private key configuration -	8
Illustration 4- Create X509 certificate -	8
Illustration 5- Validity period -	9
Illustration 6- Certificates and private keys -	9
Illustration 7- CA signature for local certificate -	10
Illustration 8- Local certificate private key -	11
Illustration 9- Assign names to local certificate -	11
Illustration 10- Local certificate validity period -	12
Illustration 11: Certificate tab	13
Illustration 12: Export the certificate	13
Illustration 13: Name for certificate	14
Illustration 14- CSR to import -	17
Illustration 15- Validity cancellation: Status -	18
Illustration 16- Export CRL -	19

Symbols and icons used in this documentation:



Note. Provides additional information and useful data.



Warning. Highlights the importance of a concept.



Tip. Useful ideas to help you get the most out of the program.



Reference. Other points that offer more information that you might find useful.

Fonts and styles used in this document:

Bold. Names of menus, options, buttons, windows or dialog boxes.

Code: Names of files, extensions, folders, commandline information or configuration files such as, scripts.

Italics: Names of options related to the operating system and programs and files with their own name.

1. Introduction

XCA is a graphic tool for Windows environments for managing the RSA/DSA asymmetric keys and X509 certificates. It provides the means to create the PKI (Public Key Infrastructure) structure, whose components will be used later on in different VPN implementations of Panda GateDefender Integra. It is based on the OpenSSL library, and it has a GPU license.

XCA uses a Berkeley database to store the RSA/DSA keys. The PKI structure components can be imported/exported in different PKCS#7, PKCS#12, PEM or DER-type formats.

XCA lets you create several PKIs on the same server.

2. Installation

The executable file is on the <http://www.sourceforge.org> web page. Version 0.6.4 was used to document this howto.

Once the file is downloaded, double click it to start the installation process. During the installation, all the default options are accepted.

[Content](#)

3. PKI management

3.1. Step 1: Create a database.

Once the XCA application is installed, before starting to manage the keys and certificates, it is necessary to create a database to store the metadata.

The first step is to create a database to store all the PKI components.

To do this, use the **New Database** option in the **File** menu, which will open a new window where you have to enter the name assigned to the database (see image).

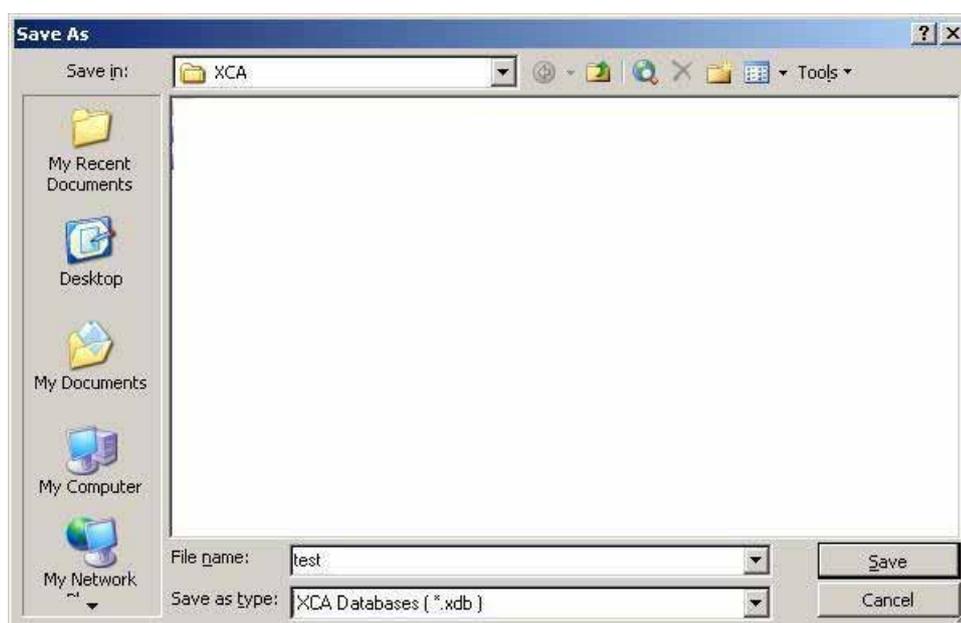


Illustration 1- Save the database created -

After clicking **Save**, a password will be requested again to protect database confidentiality, since it will contain private keys.

3.2. Step 2: Create a CA (Certification Authority)

This step consists in creating a CA used to sign all the PKI certificates:

In the **Certificates** tab in the main window, click **New Certificate**.

In the **Source** tab of the second window, choose protocol **SHA1** for the Signature Algorithm parameter, select CA in **Template for the new certificate** and click **Apply**, do not modify the settings of the rest of the default options (see image):

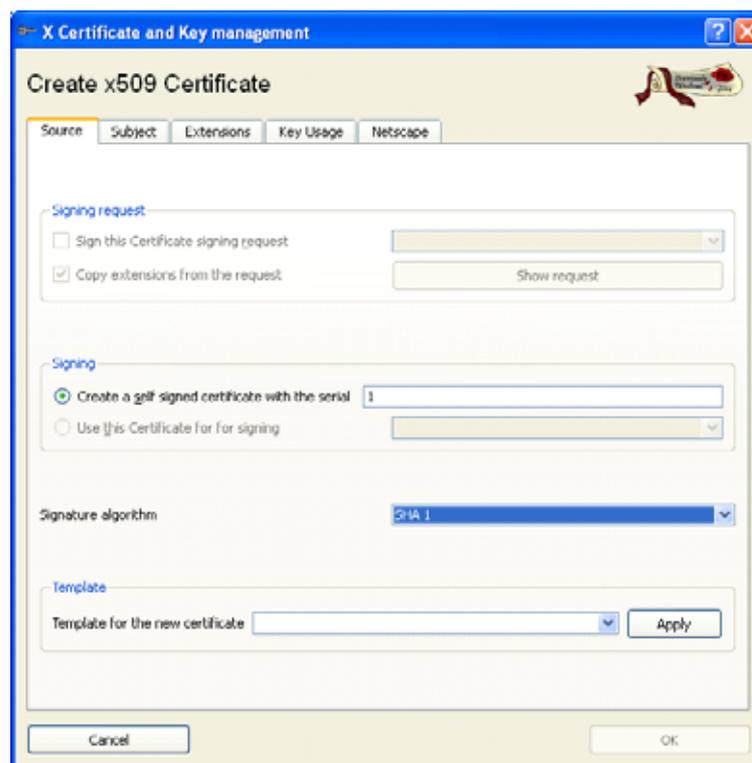


Illustration 2- CA configuration -

In the Private key section of the Subject tab, click Generate a new key.

In the pop-up window, specify the data regarding the CA private key. Maintain the default data and fill in the only empty field, **Name** with an arbitrary name.

Select the **Create** option to end the operation.



Illustration 3- Private key configuration -

In the **Subject** tab, fill in all the relevant fields (apart from the only obligatory field in XCA- **Internal Name**, **Common Name** must also be specified). The value of the Common Name parameter must be unique among all certificates.



You must be consistent when configuring the options in the **Subject** section, so the same fields are completed in all the certificates.

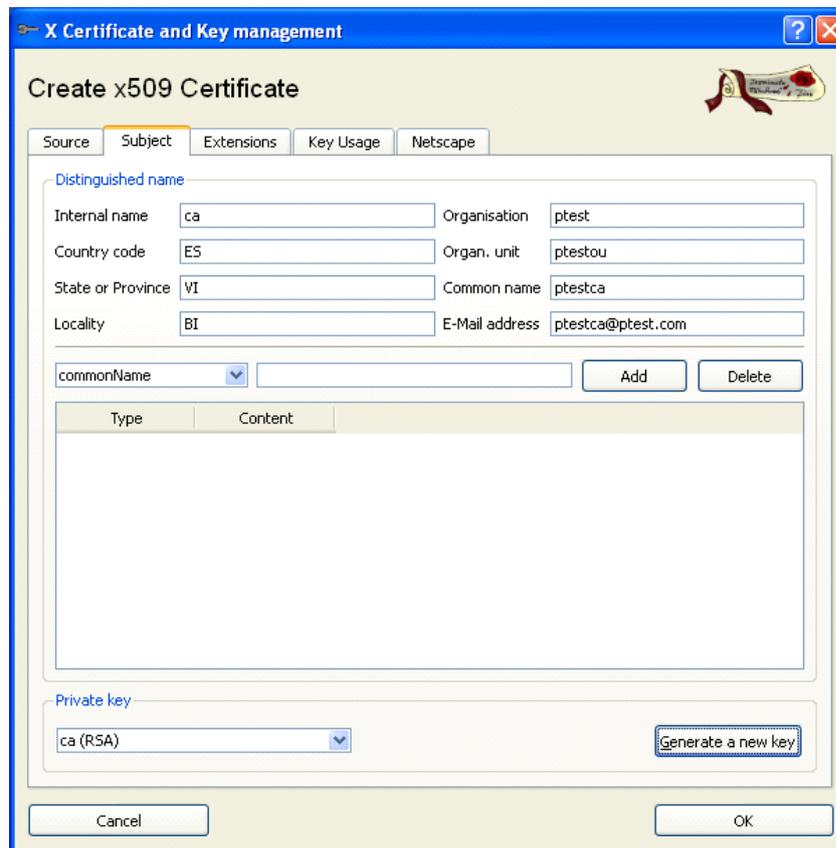


Illustration 4- Create X509 certificate -

Finally, in the **Extension -> Basic Constrains** tab, choose the type of certificate. In this case it is the **Certification Authority** type.

The default XCA values can be changed in the **Validity** section of this tab. These values indicate the CA validity interval. The CA validity must not end before the validity of the certificates signed by it. The one year default value is adequate, even though this value usually ranges between 2 and 10 years, depending on the security policy implemented in the organization/entity.

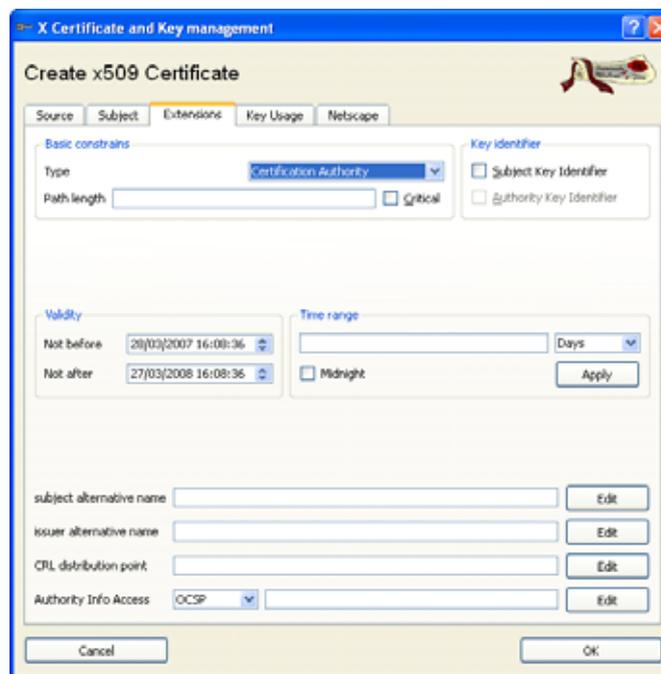


Illustration 5- Validity period -

Click **OK** at the bottom right to complete the CA creation.

In the **Certificates** and **Private keys** tabs, you can see the registries created regarding the CA certificate and its private key.



Illustration 6- Certificates and private keys -

3.3. Step 3: Create a local certificate signed by your CA

Once the CA is created, you have to create certificates for servers and clients to authenticate themselves during the initial VPN tunnel creation phase.

In the **Certificates** tab in the main window, click **New Certificate**.

In this case, select the **Use this Certificate for signing** option in the **Source** tab, and select the CA certificate created in the previous step. Select **HTTPS_server** or **HTTPS_client** in **Template for the new certificate** depending on whether the certificate is for a server or a client, and click **Apply**.

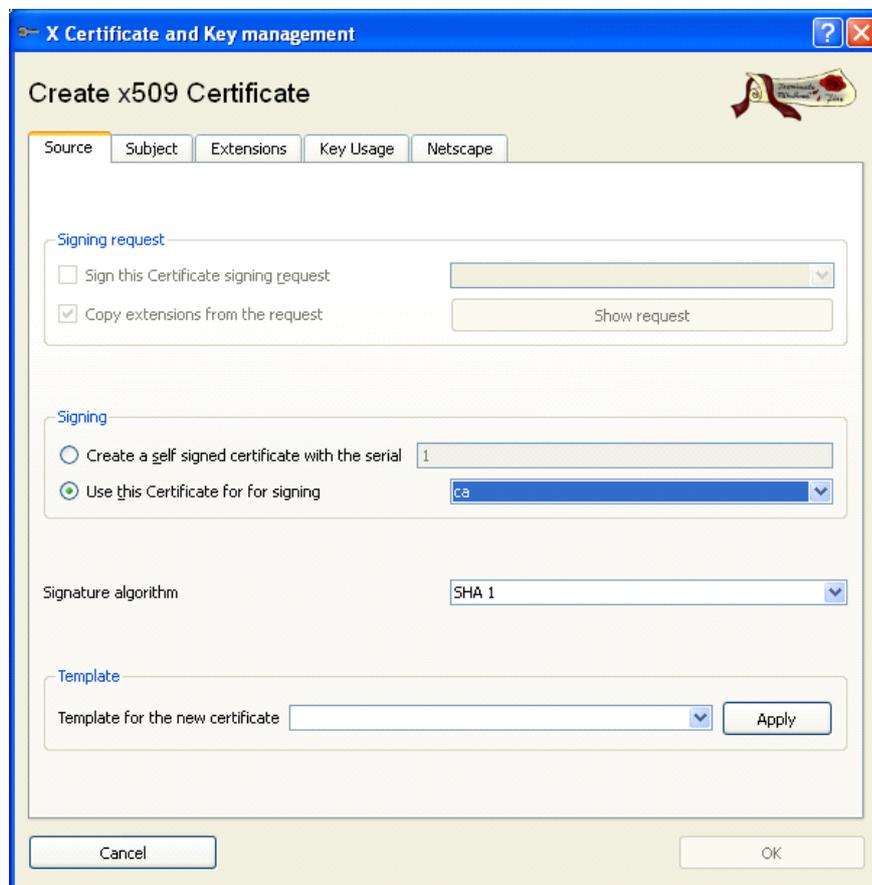


Illustration 7- CA signature for local certificate -

In the **Subject** tab, choose a different name from the rest of the Common Names already used and create the private key as shown in the images.



Illustration 8- Local certificate private key -

Note: The server is used in this example. In the case of the client, it is done in the same way as in the examples, but replacing “server1” with “client1”. In Integra, even in Gateway to Gateway connections, one of the certificates must be “Server” and the other “Client”.

In the **Subject** tab, fill in all the relevant fields (as well as the obligatory field in xca - **Internal Name**, Common Name must also be specified). The value of the *Common Name* parameter must be unique among all certificates. There cannot be two or more certificates with the same **Common Name**.

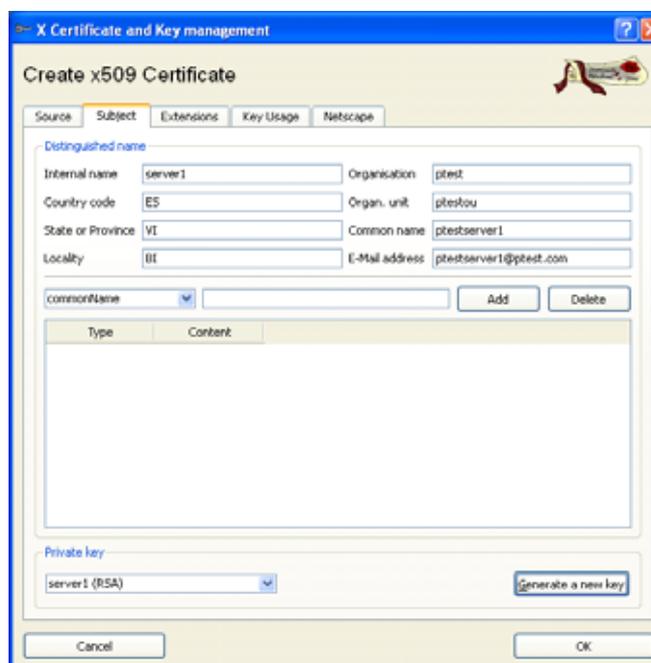


Illustration 9- Assign names to local certificate -

In the tab **Extension** -> section **Basic Constrains**, choose the type of certificate. In this case it is the **End Entity** type.

In the **Validity** section the default values offered by XCA and related to the validity interval of the local certificate can be changed. It is important that the certificate value never exceeds the validity of the CA that has signed it.

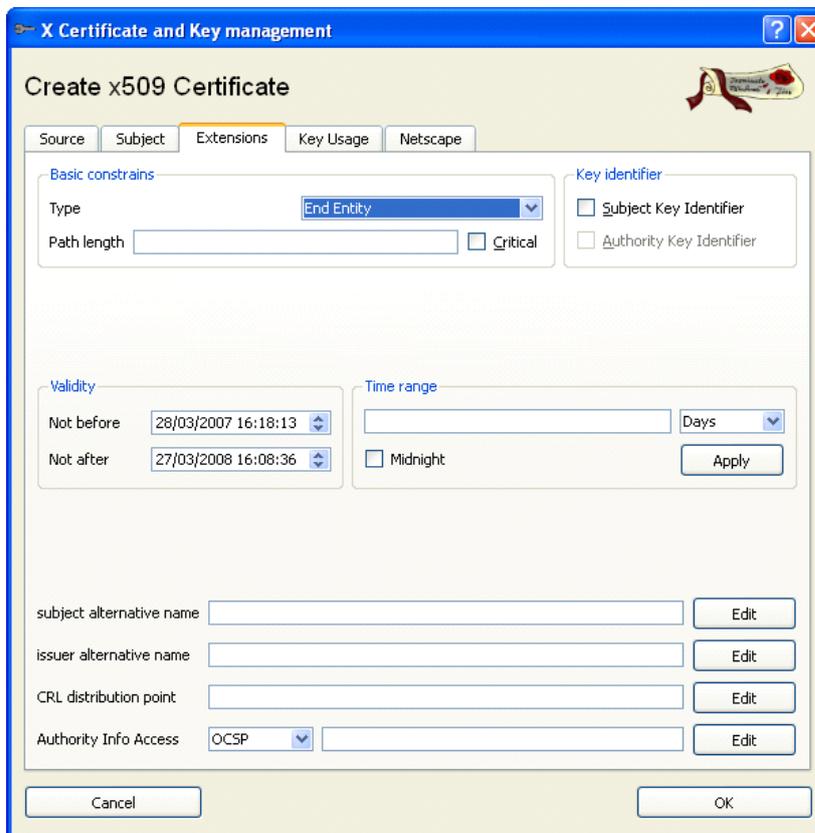


Illustration 10- Local certificate validity period -

 Bear in mind that local certificates must be created with the same options the certificates were created with, whether they are CA or local certificates.

When certificates are created by clicking **Show Details**, you can get detailed information about its characteristics.

The corresponding private key is in the **Private Keys** tab.

Once the local certificates are created, the new registries in the CA tree and its **Trusted Inherited** status can be seen in the **Certificates** tab.

3.4. Local certificate exportation for later use

To use the new certificates, they must be exported in an adequate format.

In the **Certificates** tab, click **Export**.

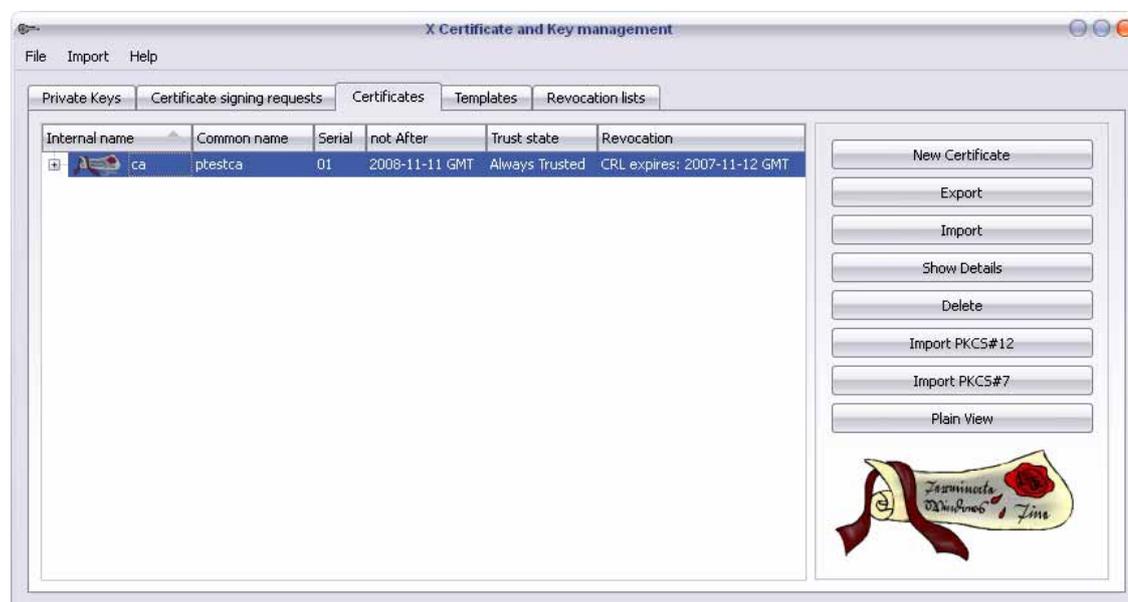


Illustration 11: Certificate tab

A new window will appear requesting the name and format of the certificate exported.



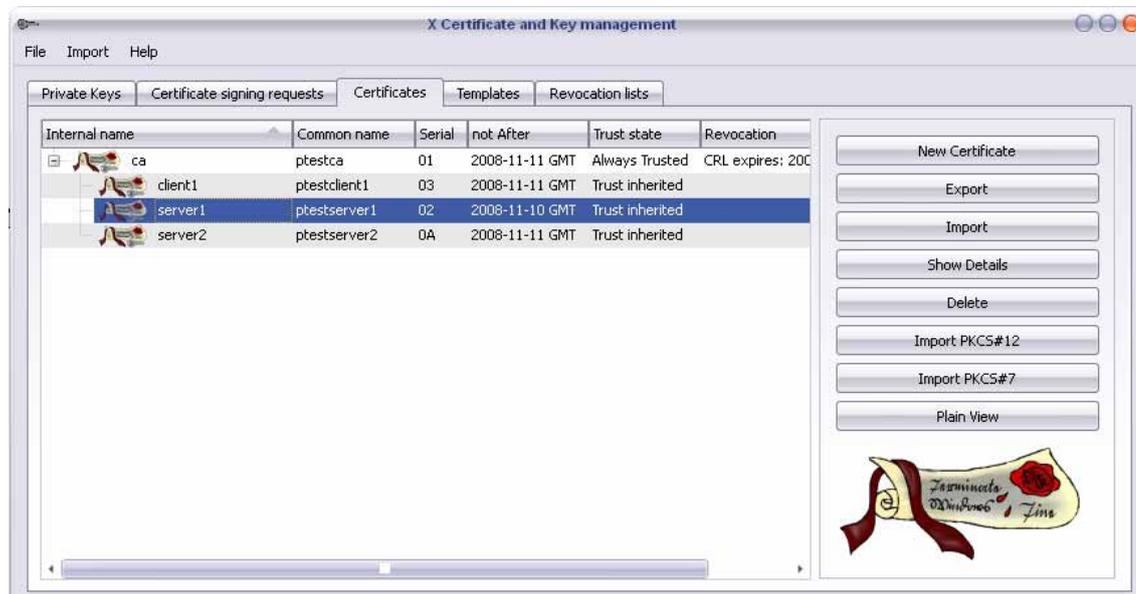
Illustration 12: Export the certificate

Choose the PKCS#12 (Public Key Cryptography Standards) format which contains the certificate and private key packaged in the same file. The file has the p12 extension in the case of local certificates and PEM format for the CA certificate – in base 64 format which contains the public key with the CRT or PEM extension only -.

Then, you only have to import the certificates already created in Panda GateDefender Integra.

To export a local certificate:

1- Select the local certificate in the **Certificates** tab, and click **Export**.



2- A new window will be displayed requesting the name and format of the certificate exported.



Illustration 13: Name for certificate

3- Choose the PKCS#12 (Public Key Cryptography Standards) format which contains the certificate and private key packaged in the same file. A password will be requested to protect the certificate.

4- Then, you only have to import the certificates already created in Panda GateDefender Integra.

Important note: VPN servers other than Integra or roadwarriors may require local certificates in other formats, such as .KEY or .CRT. In these cases, you have to export the certificates in .PEM and rename them as .KEY and/or .CRT, since the .pem format is a container which contains the key and the certificate.

[Content](#)

4. CSR Certificate Signing Request management

4.1. Step 1: Create the signing request in Integra

There are two ways of entering the local certificates in Panda GateDefender Integra:

When they are created and signed by other entities/ applications. In this case, they must be imported as indicated before (see Chapter 3).

When the certificates have been created in Panda GateDefender Integra, they are still pending signing. Then, the exportation of the CRS certificate signing requests begins. A CA will sign them and they will then be imported in Integra as signed certificates.



Among the cases that appear in Integra, it is only necessary to import the CA certificate that signed the certificates from other connection points (roadwarriors and other VPN servers). The rest of the VPN connection points must only be provided with the CA certificate that belongs to CA which signed our local certificate.

4.2. Steps to create CSR in Panda GateDefender Integra

In order to create CSR, apply the following steps:

In Digital certificate management click **Generate** to create a local certificate pending signing.

Next, enter the data bearing in mind that the number of the required set of parameters must be exactly the same for all certificates, as the ones configured for other certificates.

Once the certificate is generated, select **CSR** and click **Request Signature**.

A file with a CSR extension will be gained, so you only have to export it to XCA, sign it using the CA certificate and import it again to Panda GateDefender Integra.

4.3. Step 2: Sign CSR in XCA

Please proceed as follows:

In the **Certificate signing request** tab in the main XCA window, click **Import**.

Then specify the name of the CSR file that is going to be imported.

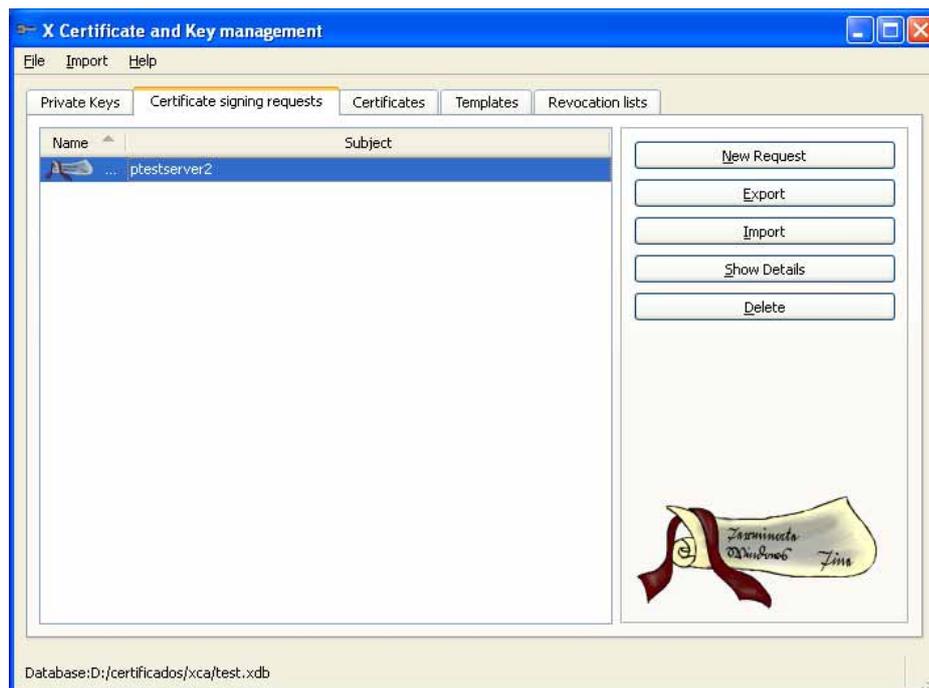


Illustration 14- CSR to import -

Once imported, select the new registry that appears in the tab by right clicking on it and choose the **Sign** option.

The same tabs will appear on the new window except for the **Subject** tab. This is because it is a previously created certificate but pending signing. Therefore, you only have to choose the **Use this Certificate for signing** option in the **Source** tab.

Next the adequate CA certificate must be specified to sign the managed CSR and in the **Extensions** tab, select the type of certificate and validity, as explained in step 3: [Create a local certificate signed by your CA](#) of chapter 3 in this HowTo.

[Content](#)

5. Revocation list management (CRL)

For those occasions in which a certificate is not being used by the VPN points or any other justified reason, there is a possibility of invalidating this certificate and therefore maintaining the PKI structure integrity, preventing the non-authorized parts from gaining access to the virtual private networks.

To do this, use the right-click menu of the certificate in the **Certificates** tab which offers the **Revoke** option among others. This option cancels the validity of the certificate in question. After canceling the validity, see the change in the Trust state status column from **Trust inherited** to **Not trusted**.

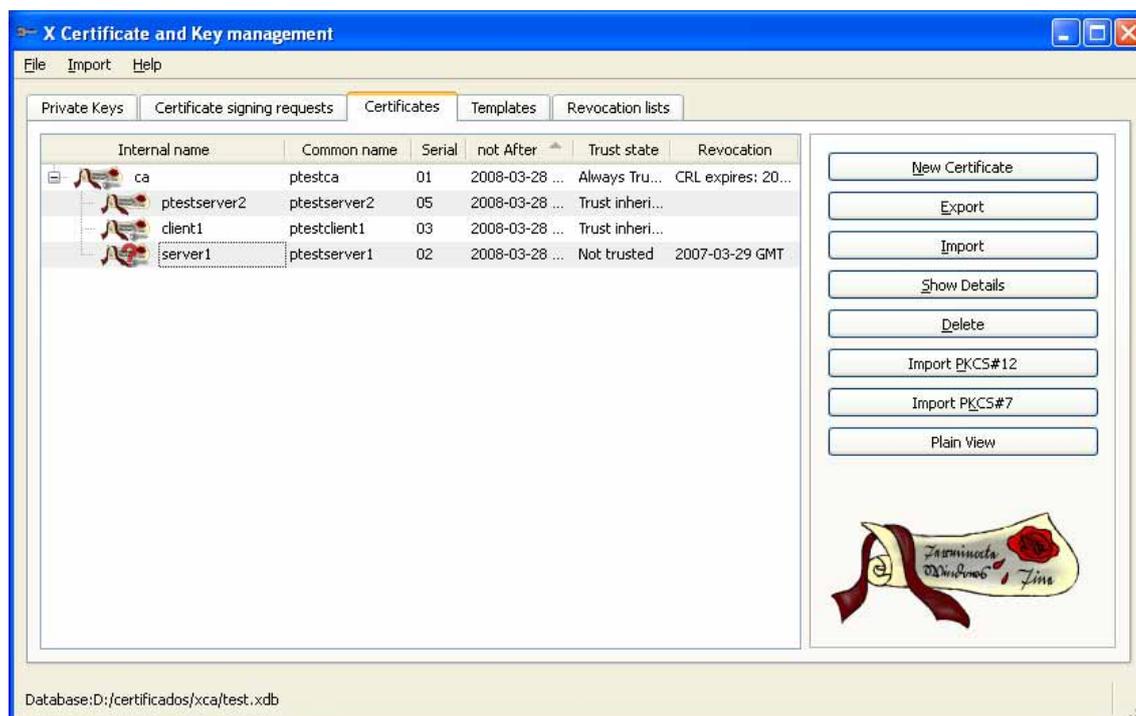


Illustration 15- Validity cancellation: Status -

With a cancelled certificate in PKI, it is necessary to spread this event to all the affected VPN servers. Without the propagation, the change in the certificate status will not be effective.

To generate the list of the revoked certificates (CRL Certificate revocation list), follow the steps below:

In the **Certificates** tab of the right-click menu of the CA in question, select the option **CA -> Generate CRL**.

The new screen provides the validity interval which can be shorter than the CA validity interval and the hash algorithm, SHA1 in this case.

The new CRL will appear in the **Revocation Lists** tab, where a single click on **Export** saves the certificate in PEM format.

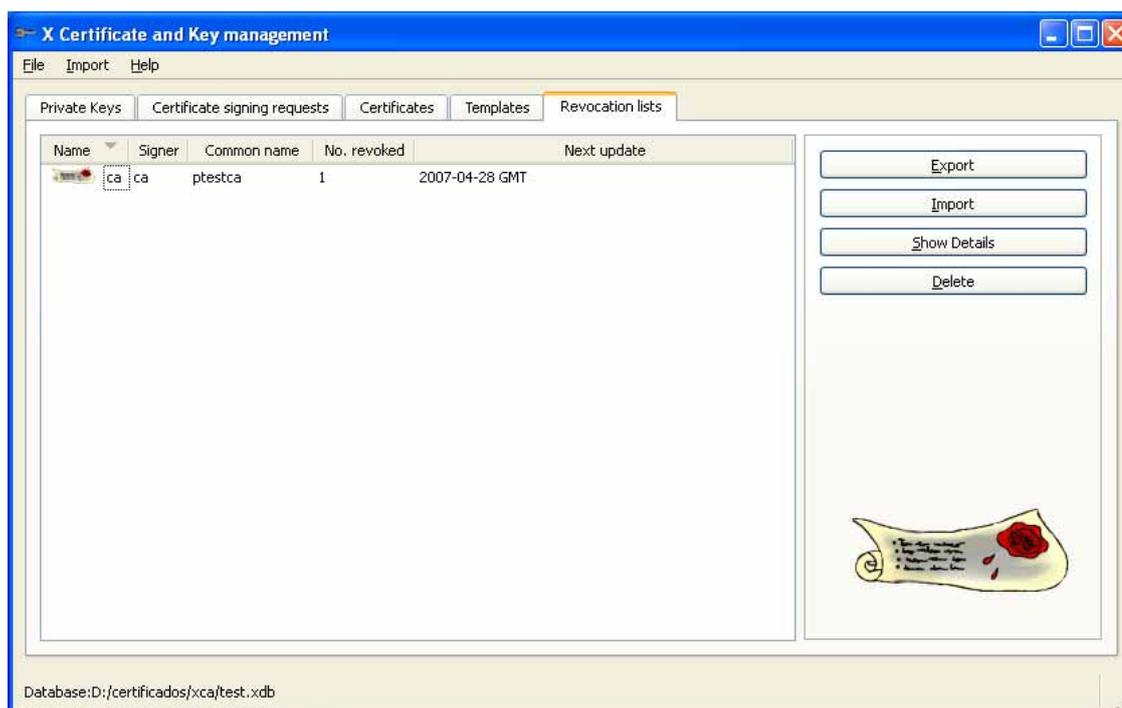


Illustration 16- Export CRL -

Integra offers the possibility of updating the CRL lists manually and automatically.

To import the updated CRL list in Integra, you only have to click on the icon in the CRL column of the managed CA registry. A new window will open where you have to choose the mode and corresponding data. The checkbox will then appear as enabled.



It is recommended to keep the PKI server isolated from the internal network and use the USB pen, cd dvd-type means to transfer the certificates to the clients. The CA private keys will not be exported, unless the whole PKI structure is transferred to another server.

Content
