APPTEC360
Enterprise Mobility Management

Troubleshooting Certificate Errors using XCA and OpenSSL
„Enterprise Mobile Manager“

What is XCA?

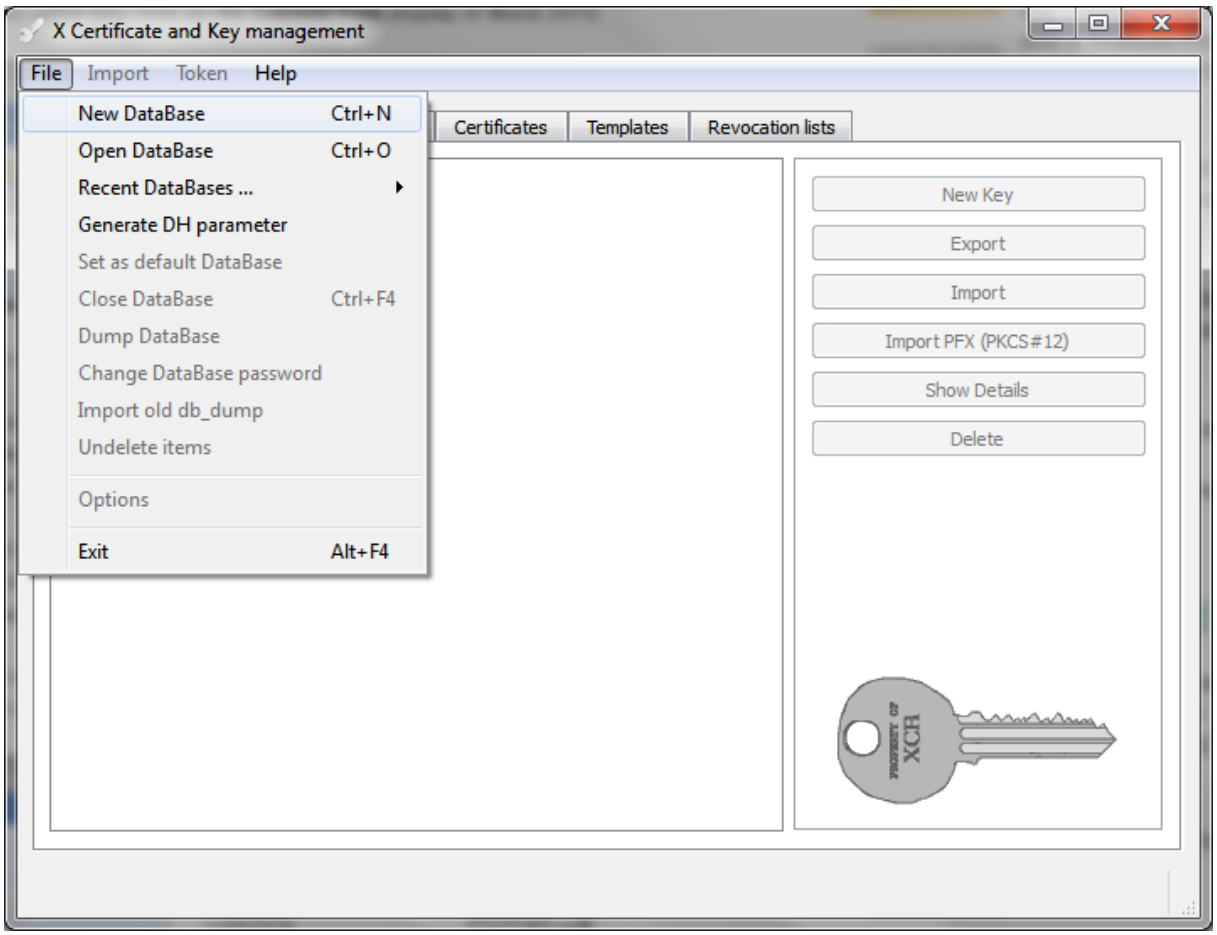
"X Certificate and Key management is an interface for managing asymetric keys like RSA or DSA. It is intended as a small CA for creation and signing certificates. It uses the OpenSSL library for the cryptographic operations"

Getting XCA

Download and install XCA from http://sourceforge.net/projects/xca/ (on some Linux Distributions it can also be installed via the package manager)

Setting up XCA

Create a new Management Database:



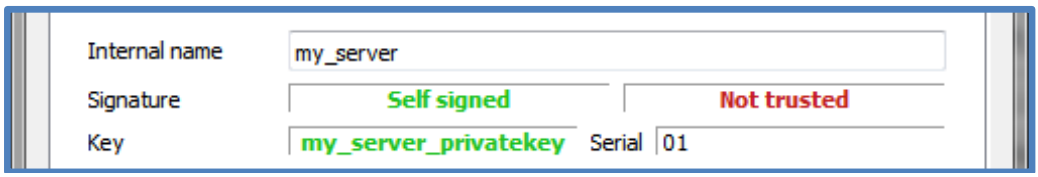
After creating the file you will be asked to add a password protection. You can also leave the password blank and press "OK"

Check if private key is password protected with XCA

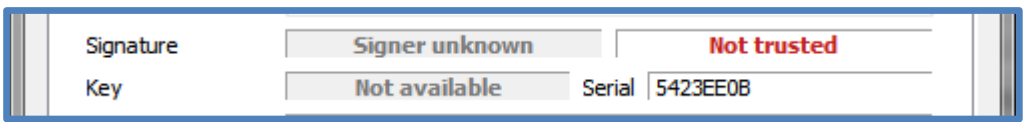
Drag and Drop the Key file into XCA. If it's protected, you'll get asked for the password. After importing you can remove the password from the file by exporting the key and leaving "Encrypt the Key with as password" unchecked.

Check if private key matches the certificate with XCA

Drag and Drop the Server Private Key and the Server Certificate into XCA. Go to the Certificates Tab and double click the server certificate. The entry for "Key" should show the name of the private key in green, if the right private key was imported into XCA.

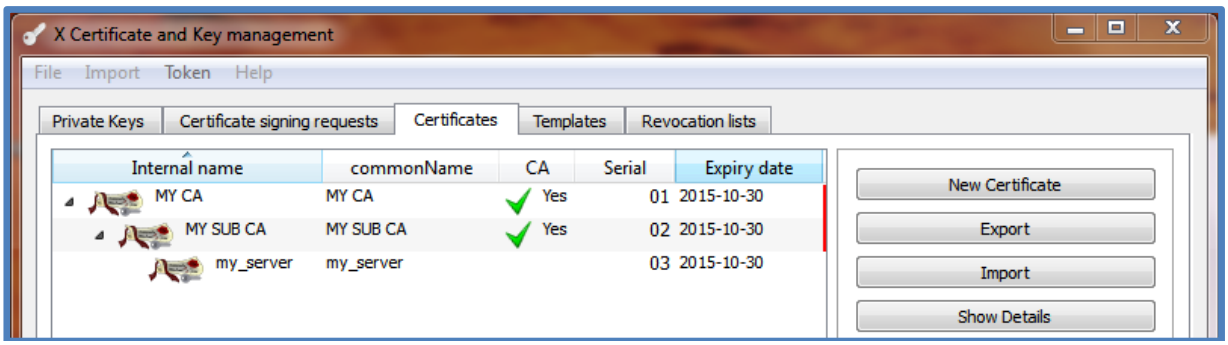


If the key can't be found, it will show up as "Not available".



Check the intermediate certificate file for the correct certificate chain with XCA

Drag and Drop the intermediate certificate and server certificate into XCA. Go to the "Certificates" tab. The server certificate should show up below the whole certificate chain.



Check if the correct certificate chain gets delivered by the server using openssl

You can see the certificate chain delivered by the server to the clients by issuing the following command:

openssl s_client –connect <your EMM VA Domain>:<Port>

Please check the Ports for the Webinterface (default: 443) and the Device Server (default: 8080).

The first lines show the certificate chain. In the screenshot you see the result of google.com on port 443:

```
$openssl s_client -connect google.com:443
CONNECTED(00000003)
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA
verify error:num=20:unable to get local issuer certificate
verify return:0
---
Certificate chain
 0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=*.google.com
   i:/C=US/O=Google Inc/CN=Google Internet Authority G2
 1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
   i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
 2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
   i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
---
```

As you can see we have three entries. Depending on your Certificate Provider it could show more on your appliance. Entry number 0 is the server certificate.
Every entries "i:/C=…." should match the next entries "s:/C=…" entry, otherwise the Certificate Chain is broken.

CONTACT

Questions? Simply contact us at:

support@apptec360.com

DISCLAIMER

The information provided in this document does not warrant or assume any legal liability or responsibility for the accuracy and completeness. This document is meant to provide a general structure on the discussed issue. Thus it is not meant to document specific licensing terms. Please refer to your license agreements, available product licensing information and other sources provided by respective software vendor to review valid terms and conditions for license compliance reconciliation.