# **Creating X.509 certificates**

Quick Reference Guide QRG\_037\_EN\_01\_Creating-X509-certificates.docx

© PHOENIX CONTACT 2014-01-20

Certificates are required for a secure VPN connection.

Certificates can be acquired from certification authorities or you can create them using the appropriate software. For example, X.509 certificates are created using Version 0.9.3 of the XCA program.

The XCA program can be downloaded at http://xca.sourceforge.net.

#### 1 Installing XCA

Start the setup\_xca-0.9.3.exe setup file and follow the on-screen instructions of the setup program.

#### 2 Creating a database

Once installed, start the XCA program and create a new database via the "File... New Database" menu item.





Assign a password to encrypt the database.

Private Keyr	Ioken nep
Private Keys	Certificate signing requests Certificates remplates Revocation lists
	New Key
	New Password
	Password
	Please enter a password, that will be used to encrypt your private keys in the database file: C:/Users/User/Documents/workshop.xdb
	Password
	Repeat Password
	Exit OK Cancel

### 3 Creating a CA certificate

First you have to create a certification authority (CA) certificate. This root certificate acts as an entity that certifies and authenticates the signing of all certificates that are derived from it and thus guarantees the authenticity of the certificate that is in circulation. Switch to the "Certificates" tab and click on "New Certificate". In the program window shown, there is already a preset self-signed certificate with the signature algorithm SHA-1.

ource	Subject	Extensions	Key usage	Netscape	Advanced			
Signing	request							
Sigi	n this Certific	ate signing requ	lest					
Cop	y extension:	s from the reque	est			Show re	equest	
Mo	dify subject o	of the request						
Signing Cre Use	ate a self sig this Certific	gned certificate v ate for signing	with the serial	1				
Signing Cre Use	ate a self sig this Certific algorithm	gned certificate water for signing	with the serial	1	SHA 1			
Signing     Ore     Use  ignature  Templai  Idefau	ate a self sig this Certific algorithm te for the ne	gned certificate v ate for signing w certificate	with the serial	1	SHA 1			

QRG\_037\_EN\_01\_Creating-X509-certificates.docx

urce Subject	Extensions	Key usage	Netscape	Advanced		
istinguished name						
nternal name	Workshop_CA		organizationName	Phoenix Contact Electronics		
ountryName	DE			organizationalUnitName	BU ION	
tateOrProvinceName	NDS			commonName	Workshop_CA	
calityName	Bad Pyrmont	t		emailAddress		
Tvn	e			Content		Add
					(	Delete
						Delete

Switch to the "Subject" tab. Here, enter the information about the owner of the root certificate.

Click on "Generate a new key" for the certificate. You can keep the default key size and type as well as the name.

Disting	Subject	Extensions	Key usage	Netscape	Advanced			
Interna	l name	Workshop_(	CA		organization	Name	Phoenix Contact Electron	ics
country	Name	🕜 X Certifica	ate and Key m	anagement			? ×	
stateOr locality	ProvinceNai Name	New ke	У					
	1	Please give a Key proper	name to the n ties	ew key and se	lect the desired	d keysize		Add
		Name	Workshop_CA					Delete
	_	Keytype	RSA				•	
	_	Keysize	1024 bit				•	
	_							
	_							
						Create	Cancel	
	-							
Private	key							
Private	кеу							

Switch to the "Extensions" tab.

The period of validity of the certificate is specified on the "Extensions" tab. The root certificate should have a longer period of validity than the machine certificates that are to be created later. In this example, the period of validity is set to 10 years. The certificate type is already set to "Certificate Authority" by default. Activate all the options as shown in the Figure.

ource Sub	oject Exten	isions Key usage	Netscape	Advanced		
Basic constra	ints					Key identifier
Туре	Certification Au	uthority			-	Subject Key Identifier
Path length					Critical	Authority Key Identifier
Not after		2014-12-20 11:	34 GMT 🔻	Midnight	Local time	No well-defined expiration
Not after		2014-12-20 11:	34 GMT 🔻	Midnight	Local time	No well-defined expiration
Not after	tive name	2014-12-20 11:	34 GMT ▼	Midnight	Local time	No well-defined expiration
Not after ubject alterna suer alternatio	tive name ve name	2014-12-20 11:	34 GMT 🔻	Midnight	Cocal time	No well-defined expiration

Click "OK" to complete root certificate creation.

A new root certificate from which further machine certificates can be derived now appears in the overview.

Private Keys	Certificate s	signing requests	Certificates	Templates	Revocation	n lists
Interna	I name	commonNam	e CA	Serial	Expiry	
Acts	Workshop_CA	Workshop_CA	🖌 Yes	01	2014-12-20	New Certificate
						Export
						Import
						Show Details
		🔗 X Certifica	ate and Key ma	nagement		Delete
		Su Su	ccessfully creat	ted the certif	ïcate 'Worksh	hop_CA' Import PKCS#12
					_	Import PKCS#7
					C	Plain View
						2 Tominale Contractor

## 4 Creating templates

The further creation of machine certificates can be simplified by using templates. Switch to the "Templates" tab. Click on "New Template" to create a terminal certificate. In the "Preset Template Values" prompt that appears, select "Nothing".

X Certificate a	and Key management Token Help	
Private Keys	Certificate signing requests Certificates Templates Revocation lists	
Internal n	ame commonName Type	New template
	C	hange Template
		Delete
		Import
	X Certificate and 2	Export
	Veset Template values	
latabase:C:/Use	ers/User/Documents/workshop.xdb	

On the "Subject" tab, specify the settings for the certificates that are to be created later. Two names appear in angular brackets ("Internal name" and "Common name"). The names in the angular brackets are simply placeholders, as the actual names are assigned to the certificates. When using the template, the names are set individually.

oject	Extensions	Key usage	Netscape	Advanced			
istinguis	shed name						
nternal	name	<template rout<="" th=""><th>er&gt;</th><th></th><th>organizationName</th><th>Phoenix Contact Electron</th><th>nics</th></template>	er>		organizationName	Phoenix Contact Electron	nics
ountryN	lame	DE			organizationalUnitName	BU ION	
tateOrP	ProvinceName	NDS			commonName	<template router=""></template>	
calityN	ame	Bad Pyrmont			emailAddress		
	Tvn				Content		Add
							Delete
							Delete

Switch to the "Extensions" tab. Change the certificate type to "End Entity", as the template is to be used for machine certificates. 365 days should be specified as the period of validity of the certificates to be created. After the resulting end date, the certificates can no longer be used.

Subject Ex	tensions	Key usage	Netscape	Advanced	1			
Basic constra	ints						Key identifie	r
Туре	End Entity					•	Subject P	Key Identifier
Path length						Critical	Authority	YKey Identifier
Not before		2013	-12-20 11:43	GMT 👻	365	_	Days 🔻	Apply
Not before Not after		2013	-12-20 11:43 -12-20 11:43	GMT v	365 Midnight	Local time	Days   No well-defin	Apply ned expiration
Not before Not after	tive name	2013	-12-20 11:43 -12-20 11:43	GMT V	365 Midnight	Cocal time	Days	Apply ned expiration Edit
Not before Not after ubject alterna	tive name ve name	2013	-12-20 11:43 -12-20 11:43	GMT v	365 Midnight	Cocal time	Days	Apply ned expiration Edit Edit

Click "OK" to create the template.

The template can now be used as a basis to create certificates signed with the root certificate.

## 5 Creating machine certificates based on a template

A template can be used to create certificates signed with the root certificate.

Switch to the "Certificates" tab and click on "New Certificate".

On the "Source" tab, specify the root certificate that is to be used for signing. In addition, you can select a template that has been created and read it in by clicking "Apply All".

X Certificate and Key management	୍ ନ <mark>-</mark> ×
Create x509 Certificate	A REAL STREET
Source Subject Extensions Key usage Netscap	e Advanced
Signing request	
Sign this certificate signing request	
Madify a biast of the request	Show request
Prodity subject of the request	
Signing	
Create a self signed certificate with the serial	
Output Use this Certificate for signing	Workshop_CA 🗸
Signature algorithm	SHA 1
Template for the new certificate	
<template router=""></template>	•
	Apply extensions Apply subject Apply all
	OK Cancel
	Calicei

Switch to the "Subject" tab.

Here, enter the information about the owner of the machine certificate. When entering information on this tab, please note that the certificates must differ at least with regard to their name ("Internal name" and "Common name"). The equipment identification of the machine or router, for example, can be used as the name.

urce Subject	Extensions	Key usage	Netscape	Advanced		
Distinguished name						
internal name	Router_01			organizationName	Phoenix Contact Electroni	cs
countryName	DE			organizationalUnitName	BU ION	
stateOrProvinceNar	me NDS			commonName	Router_01	
ocalityName	Bad Pyrmont			emailAddress		
1	vpe			Content		Add
						Delete
						Deele

Click on "Generate a new key". Do not change the default key size, type, and name.

Distinguished name	Extensions   Key usage   Netscape   Advanced
Internal name countryName	Router 01 organizationName Phoenix Contact Electronics
stateOrProvinceNa localityName	New key Please give a name to the new key and select the desired keysize Key properties Name Router_01 Keysize 1024 bit Create Cancel
Private key	

Click on "OK" to finish the creation of the machine certificate. You now made machine certificate , which has been signed by the CA certificate.

Private	Keys	Certificate	signing requests	Certificates	Templates	Revocation li	ists
	Intern	al name	commonNar	ne CA	Serial	Expire	
4 N		Workshop_CA	Workshop_CA	V Ye	es 01	2014-12-20	New Certificate
	n	e Router	Router_01	No	02	2014-12-20	Export
							Import
							Show Details
							Delete
							Import PKCS#12
							Import PKCS#7
							Plain View
•			m			4	2 Farminada 100

#### 6 Exporting machine certificates

The machine certificate must be exported so that it can be used on the router. Select the relevant certificate from the list and click on "Export". The entire certificate including the private key must be in PKCS#12 format with certificate chain and can then be uploaded to the relevant component as a own machine certificate.



For security reason the machine certificate is encrypted with a password. Enter a password. This password is needed to load the machine certificate to the device.

ie import loken H	elp			
Private Keys Certificat	e signing requests Certificates Templates Revocation lists			
Internal name	commonName CA Serial Expiry	Certificate		
Workshop_C	X Certificate and Key management	xport		
	Password	nport v Details		
	Please enter the password to encrypt the PKCS#12 file	elete : PKCS#12 t PKCS#7		
	Password  Password Repeat Password	in View		
	OK Cancel	mineeta 60		
•	······································	Windows Jims		

The partner certificate should also be exported. This is stored in PEM format without the private key.

X Certificate a	and Key man	agement						- 0	23
Private Keys	Certificate	signing requests Cer	rtificates	Templates	Revocation	n lists			
Internal	name	commonName	CA ment	Serial	Expiry	Ner	v Certificate	1	
R	Certifikate export								
	Piename     C:/Program Hies (xsb/)xca Kouter.ort       DER is a binary format of the Certificate       PPM is a base64 encoded Certificate       PKCSF# /s an official Certificate exchange format       PKCSF# /s an encrypted official Key-Certificate exchange format       Export Format     PEM								
						ок с	ancel	<b>B</b> Time	
•		111			Þ				
Database:C:/Use	rs/User/Doc	uments/workshop.xdb							