

# **VPN with INSYS routers**

Creating X509.v3 Certificates for VPNs with XCA

Copyright © 2024 INSYS icom GmbH

Any duplication of this üublication is prohibited. All rights on this publication and the devices are with INSYS icom GmbH Regensburg.

Trademarks

The use of a trademark not shown below is not an indication that it is freely available for use.

MNP is a registered trademark of Microcom Inc.

IBM PC, AT, XT are registered trademarks of International Business Machine Corporation.

Windows<sup>™</sup> is a registered trademark of Microsoft Corporation.

Linux is a registered trademark of Linus Torvalds.

INSYS <sup>®</sup> is a registered trademark of INSYS icom GmbH.

The principles of this publication may be transferred to similar combinations. INSYS icom GmbH does not assume liability or provide support in this case. Moreover, it cannot be excluded that other effects or results than described here are produced, if other, similar components are combined and used.

INSYS icom GmbH is not liable for possible damages.

Publisher INSYS icom GmbH Hermann-Köhl-Str. 22 D-93049 Regensburg Germany

Phone	+49 941 58692 0
Fax	+49 941 58692 45
E-mail URL	info@insys-icom.com http://www.insys-icom.com

Print 17. Jan. 2024 Item No. -Version 1.6 Language EN

# 1 Introduction

### General

The present publication refers to a combination of selected hardware and software components of INSYS icom GmbH as well as other manufacturers. All components have been combined with the target to realize certain results and effects for certain applications in the field of professional data transfer.

All components have been prepared, configured and used as described in this publication. Thus, the desired results and effects have been achieved.

The exact descriptions of all used components, to which this publication refers, are described in the tables *Hardware, Accessories* and *Software* at the end of this publication.

The symbols and formattings used in this publication are explained in the correspondent section at the end of this publication.

Some configurations or preparations, which are precondition in this publication, are described in other publications. Therefore, always refer to the related device manuals. INSYS devices with web interface provide you with helpful information about the configuration possibilities, if you click on "display help text" in the header.0

## **Target of this Publication**

An appropriate certificate structure is required for setting up a VPN network with certificate-based authentication.

You'll learn from this publication how to generate the key and certificate files for Certification Authority (CA), Server, and Clients as well as an optional Certificate Revocation List (CRL) required for this.

These files are necessary to set up an OpenVPN network. Refer to <u>http://www.openvpn.eu</u> for further information about OpenVPN.

Only the CA certificate and key and the certificates of the respective clients are required for setting up a VPN network with IPsec. The certificates for an IPsec participant are identical with those for the OpenVPN client. We refrain from a separate description of the creation of certificates and keys for an IPsec participant here.

The following figures show the distribution of the different keys and certificates across the different participants in the respective VPN networks. A Diffie Hellman parameter set exists by default on the INSYS router, but can also be replaced manually.

#### Introduction



Figure 1: CA certificate structure for OpenVPN server and client with certificate-based authentication, here MoRoS as server and clients



Figure 2: CA certificate structure for IPsec participant with certificate-based authentication, here MoRoS as participant

# 2.1 Provisions and Presettings

# Provisions

Please prepare the following items before starting the configuration:

- Downloading XCA
- Installing XCA on Windows PC
- Downloading XCA
   How to download the XCA software.
- → PC with approx. 30 MB free disk space
- → Web browser
- → Internet connection
- 1. Open http://sourceforge.net/projects/xca/ to download the software
- 2. Click on Download

XCa	S Donate
<ul> <li>I07 Recommendations</li> <li>665 Downloads (This Week)</li> </ul>	Sf Download
	Browse All Files

- () If a more recent version is available, download this.
- 3. Save the file on your PC.
  - $\checkmark$  You have downloaded the XCA software with this.

### ■ Installing XCA on Windows PC

How to install the XCA software for creating the certificates and keys on your PC successfully.

- → You have downloaded the XCA setup file (version 0.9.1 or higher).
- 1. Execute the installation file (e.g. "setup\_xca-0.9.1.exe")
  - () Execute the installation file under Windows 7 by opening the context menu with a right-click and selecting "Run as administrator".
  - If a security warning is displayed, acknowledge it.

- 2. Select "English" as installation language and click on OK.
- 3. Accept the licence agreement with I Agree.
  - $\checkmark$  The component selection window appears:

noose Components Choose which features of XCA	you want to install.	
Check the components you wa nstall. Click Next to continue.	nt to install and uncheck the comp	oonents you don't want to
Select components to install:	<ul> <li>xca (required)</li> <li>Start Menu Shortcuts</li> <li>Update</li> <li>OpenSC PKCS#11 library</li> <li>Translations</li> <li>File association</li> </ul>	Description Position your mouse over a component to see its description.
Space required: 19.1MB	<	
soft Tostall System v2 46-2		

4. Accept the selection of all components and click on Next

 $\checkmark$  The target directory selection window appears:

😽 XCA 0.9.0 Setup	
Choose Install Location Choose the folder in which to install XCA.	
Setup will install XCA in the following folder. select another folder. Click Install to start th	To install in a different folder, click Browse and e installation.
C:\Program Files\xca\	Browse
Space required: 19.1MB Space available: 1.7GB Nullsoft Install System v2,46-2	< Back Install Cancel

- 5. Specify the target directory and click on Install.
- 6. Complete the installation with Finish.
  - You have successfully installed the XCA software on your PC and completed the provisions with this.

#### Presettings in XCA

You have to create a project database before you can generate a certificate structure with XCA. All keys and certificates of this CA project are stored in this database.

It is helpful to create templates for CA, server and client certificates for a quick and accurate creation of key and certificate files.

Perform the following presettings for this:

- Starting XCA and Creating a Database
- Creating a CA Template
- Creating a Server Template
- Creating a Client Template
- Starting XCA and Creating a Database

How to start the XCA software and create a new database for the CA project.

- → You have successfully installed the XCA software on your PC.
- 1. Select in the start menu Program Files  $\rightarrow$  xca  $\rightarrow$  xca
  - (i) Execute the program under Windows 7 by opening the context menu with a right-click on "xca" and selecting "Run as administrator".
  - The XCA window appears:



2. Select in the "File" menu the option "New DataBase".

 $\checkmark$ 

- The database selection window appears: ? X **Open XCA Database** Save in: 🛅 XCA\_Database -🗢 🗈 💣 📰+ 3 My Recent Documents R Desktop My Documents My Computer CA\_Project • My Network File name: Save Places XCA Databases ( \*.xdb ) Cancel Save as type: -
- 3. Specify path and file name and click on Save
  - The password definition window appears:  $\checkmark$

🖌 New Password	? 🛛
Password	(ji)
Please enter a passy private keys in the d 'C:/XCA_Database/C	vord, that will be used to encrypt your atabase file: :A_Project.xdb'
Password	•••••
Repeat Password	•••••
	OK Cancel

- 4. Specify a password and click on Install
  - $(\mathbf{i})$ We strongly recommend to specify a password. Keep this password in mind. You'll need it every time you want to open the database of this CA project.
  - $\checkmark$ You have created a new database for the CA project with this.

#### Creating a CA Template

How to create a template for CA certificates.

- → The XCA software is started and the project database is opened.
- 1. Change to the "Templates" tab.



- 2. Select New Template
  - ✓ The template value selection window appears:



3. Select "CA" and click on OK.

oject Extension	ns 📗 Key usage	Netscape	Advanced	8		
stinguished name	Large Pro-			Same and the second	[errente	
nternal name	CA_lemplate				INSYS	
ateOrProvinceNan	DE Bauaria			commonName	Customer Support	
calityName	Regensburg			emailAddress	support@insys-tec.de	1
	Large and	1				
	Ahe			Content		AUU

- 4. Define your default values without specifying a "Common Name".
- 5. Change to the "Extensions" tab.

ubject Extensi	ons Key usage	Netscape Advanced		
Basic constraints -				Key identifier
Type Certi	fication Authority		<u> </u>	Subject Key Identifier
Path length			Critical	L Authority Key Identifier
Validity Not before 2010	-10-13 16:48 💌	Time range		Years 💌 Apply
Validity Not before 2010 Not after 2020	-10-13 16:48 💙	Time range		Years Apply Apply
Validity Not before 2010 Not after 2020	-10-13 16:48 V	Time range		Years Apply No well-defined expiration Edit Edit
Validity Not before 2010 Not after 2020 ubject alternative n suer alternative na	-10-13 16:48 V	Time range		Years Apply No well-defined expiration Edit Edit

- 6. If required, adjust the validity period of the certificate and click on OK.
  - Select a time range that is reasonable for your purpose. The default values are a good guideline. Too long time ranges may cause security or compatibility problems.
- 7. Confirm the template creation with OK .
  - You have created a CA certificate template with this. When using this template while creating a CA certificate, the respective fields are initial-ised with the default values entered here.
- Creating a Server Template

When creating the server certificate template, proceed in the same way as for the CA, but select "HTTPS\_server" when selecting the preset template values.

Creating a Client Template

When creating the client certificate template, proceed in the same way as for the CA or server template, but select "HTTPS\_client" when selecting the preset template values.

# 2.2 Creating Certificates

## Creating a Certificate Structure with XCA

A Public Key Infrastructure (PKI) comprises services for encryption and digital signature on the basis of public key procedures.

First, the files for the CA (Certification Authority) are generated. Then, a key pair is generated for the server and each client. One key pair for both clients (participants) is necessary for setting up an IPsec connection. These key pairs will be uploaded to the respective devices later.

You will need the following files for setting up an OpenVPN network with certificate-based authentication:

For the OpenVPN server:

the CA certificate (e.g. ca.crt)

the server certificate (e.g. server.crt)

the server key (e.g. server.key)

a Diffie-Hellman parameter set (e.g. dh1024.pem)

 The generation of a Diffie-Hellman parameter set using XCA (menu File – Generate DH parameter) is not described here, because such is stored on each INSYS router in delivery state. The Diffie-Hellman parameter set can be downloaded in the INSYS router web interface on the "OpenVPN-Server" page in the "Authentication based on certificate" section.

For each OpenVPN client (1-n):

the CA certificate (e.g. ca.crt)

a client certificate (e.g. client1.crt)

a client key (e.g. client1.key)

- () A separate pair of certificate and key is necessary for each OpenVPN client.
- () The CA certificate is the same for each client (and also the server).
- () The respective keys are secret and may only be known by the related Open-VPN participant besides the issuing CA. The CA key is essential for the security of the OpenVPN network. It must be kept top secret by the CA and never be exported.

You will need the following files for setting up an IPsec connection with certificatebased authentication:

For each of both IPsec participants:

the CA certificate (e.g. ca.crt)

a participant certificate (e.g. peer1.crt)

a participant key (e.g. peer1.key)

The respective keys are secret and may only be known by the related VPN participant besides the issuing CA. The CA key is essential for the security of the VPN network and must be kept top secret by the CA.

Generate the files in the sequence of the following sections:

- Generating CA Certificate and Key
- Generating Certificate and Key for a Server
- Generating Certificate and Key for a Client

#### Generating CA Certificate and Key

How to create your own certification authority (CA, Certificate Authority) with XCA. The CA certificate structure comprises the secret key and the public certificate.

(1) The non-disclosure of the key is essential for the security of the complete network.

- → The XCA software is started and the project database is opened.
- → A CA template has been created.
- → Time and date of the PC are correct.
  - Certificates have an expiry date. A wrong system time (time and date) is a frequent failure source. Therefore, ensure that the system time of the PC and the INSYS router is correct when creating as well as commissioning the server or clients.
- 1. Change to the "Certificates" tab.



2. Select New Certificate

The dialogue window for creating a certificate appears:

ource Subject Extensions Key usage Netsc	cape Advanced
Signing request	
Sign this Certificate signing request	×
Copy extensions from the request	Show request
Modify subject of the request	
gnature algorithm	SHA 1
Template for the new certificate	
	Apply extensions Apply subject Apply all
	(ubbit excensional (ubbit septeral (ubbit an

- 3. Select the previously created CA template as template.
- 4. Click on Apply all.

 $\checkmark$ 

5. Change to the "Subject" tab.

Distinguished name	Extensions key usage netscape	Auvanceu		
Internal name	ca	organizationName	INSYS	
countryName	DE	organizationalUnitName	Customer Support	
stateOrProvinceName	Bavaria	commonName	са	
localityName	Regensburg	emailAddress	support@insys-tec.de	
Туре		Content		Add
				Delete

- 6. Specify the "Common Name" and assign this also as internal name (e.g. "ca").
- 7. Click on Create a new key .

 $\checkmark$  The dialogue window for creating a new key appears:

💣 X Certif	icate and Key management	? 🛛
New ke	<b>'Y</b> a name to the new key and select the desired keysize ties	
Name	ca	
Keytype	RSA	×
Keysize	1024 bit	×
	Create	Cancel

- 8. Preferably assign the same name like the "Common Name".
- 9. Click on Create.
- 10. Confirm the key creation with OK.
- 11. Click on OK.
- 12. Confirm the certificate creation with OK.
  - $\checkmark$  The CA creation is completed with this.

#### ■ Generating Certificate and Key for a Server

How to generate the private key and the public certificate for a server with XCA.

You need a "Common Name" for the server for the generation. The "Common Name" is the unique member name of a participant in the secured network and is used for routing into the client networks for example. The "Common Name" must only be used for one participant and cannot be changed any more after the generation. Observe the capitalization for the "Common Name" and preferably use only one of these possibilities consistently.

- () The maximum length of the "Common Name" for all INSYS routers is 29 characters (15 characters for MoRoS 1.3).
- → The XCA software is started and the project database is opened.
- → A server template has been created.
- → A CA certificate has been created.
- → Time and date of the PC are correct.
  - Certificates have an expiry date. A wrong system time (time and date) is a frequent failure source. Therefore, ensure that the system time of the PC and the INSYS router is correct when creating as well as commissioning the server or clients.
- 2. Change to the "Certificates" tab.



3. Highlight the CA certificate and select New Certificate

 $\checkmark$  The dialogue window for creating a certificate appears:

	scape Advanced
Signing request	
Sign this Certificate signing request	
Copy extensions from the request	Show request
Modify subject of the request	
Se uns certaincate for signing	
jnature algorithm	SHA 1
Template for the new certificate	
Server_Template	

- 4. Select the previously created CA certificate in the "Signing" section.
- 5. Select the previously created server template in the "Template for new certificate" section.
- 6. Click on Apply all.
- 7. Change to the "Subject" tab.

urce Subject	Extensions k	key usage 📗 Nets	cape Advanced		
vistinguished name					
nternal name	server		organizationName	INSYS	
ountryName	DE		organizationalUnitName	e Customer Support	
tateOrProvinceName	Bavaria		commonName	server	
ocalityName	Regensburg		emailAddress	support@insys-tec.de	í
Tvn					
	e		Content		Add Delete
	e		Content		Add

- 8. Specify the "Common Name" and assign this also as internal name (e.g. "server").
- 9. Click on Create a new key.

 $\checkmark$  The dialogue window for creating a new key appears:

💣 X Certif	icate and Key management	? 🛛
	<b>y</b>	
Key prope	ties	
Name	server	
Keytype	RSA	~
Keysize	1024 bit	~
	Create	Cancel

- 10. Preferably assign the same name like the "Common Name".
- 11. Click on Create.
- 12. Confirm the key creation with OK.
- 13. Click on OK.

 $\checkmark$ 

14. Confirm the certificate creation with OK.

The generation of server certificate and key is completed with this.

#### ■ Generating Certificate and Key for a Client

When generating certificate and key for a client, proceed in the same way as for the server, but select the client template when selecting a template.

If required, generate further client certificates.

# 2.3 Exporting Certificates

# Exporting Certificates and Keys from XCA

The certificates and keys created with XCA are stored in the respective XCA database. In order to upload the certificates and keys to the respective INSYS router, these must be exported.

XCA offers different file formats for export. We describe the export to the data format PKCS#12 in this manual, because this is suitable for all INSYS routers except MoRoS PRO of version 1. In addition, PKCS#12 allows to export complete key pairs into a container, which reduces the upload effort. Since the certificate chain can also be exported, the CA certificate does not have to be exported separately. A password protection can be applied starting with firmware 2.3.0 with this.

Never export the CA key, because this is essential for the security of the VPN network.

Export the certificates and keys in the sequence of the following sections:

- Exporting the Server Certificate Container
- Exporting the Client Certificate Container
- Exporting the Server Certificate Container

How to export the generated server key pair from the XCA database into a PKCS#12 container. The container contains the server certificate and the associated public key. If the certificate chain is exported with them, the CA certificate will also be packed into the container.

- → The XCA software is started and the project database is opened.
- → A server certificate has been created.
- 1. Change to the "Certificates" tab.

vate Keys 👘 Certifica	te signing requests	Certificates	Templa	ates 📔 Revocation li	ists
Internal name 🛛 📥	commonName	CA	Serial	Expiry date	
🛛 💦 📬 ca	ca	🗸 0	01	2020-10-13 GM1	New Certificate
client1	client1	No	03	2011-10-13 GMT	Export
lient2	client2	No	04	2011-10-13 GMT	Import
Server	server	No	02	2011-10-13 GMT	Import
					Show Details
					Delete
					Turnet BKCC #40
					Import PKCS#12
					Import P <u>K</u> CS#7
					Plain View
					Zusmineeta Diversense Jine

- 2. Highlight the server certificate and select Export.
  - $\checkmark$  The certificate export dialogue window appears:

💕 X Certif	icate and Key management	? 🔀
Certifik	ate export	Community of the second
Please ent	er the filename for the certificate.	
Filename	C:/XCA_Database/server.p12	
DER is a b PEM is a b PKCS#7 is PKCS#12	nary format of the Certificate ise64 encoded Certificate an official Certificate exchange format s an encrypted official Key-Certificate exchange format	
Export For	MAL PKC5 #12 with Certificate chain	✓
		OK Cancel

- 3. Specify a path and file name.
  - () It is recommended to select the file name identical to the "Common Name" to enhance clarity if this is not contrary to any security concerns.
- 4. Select the export format "PKCS#12 with Certificate chain".
- 5. Click on OK.

✓ The password definition window appears:

of X Certificate and Key management	? 🛛
Password	
Please enter the password to encrypt the PKCS#12 file	
Password ••••• Repeat Password •••••	
ОК	Cancel

- 6. Specify a password if you want to enhance the security of the certificate file transmission and click on OK
  - $\checkmark$  You have exported the server certificate container with this.
- Exporting the Client Certificate Container

When exporting the certificate containers for the individual clients, proceed in the same way as for the export of the server certificate container.

# 2.4 Revoking Certificates

### **Revoking Certificates**

It is possible to create a Certificate Revocation List (CRL) for OpenVPN, which contains the revoked certificates. If certificates have to be revoked before their expiry (due to misuse for example), they can be entered into this list. Every updated list must then be uploaded to the device, which acts as OpenVPN server.

Proceed in the sequence of the following sections to revoke certificates:

- Revoking a Certificate
- Generating a Certificate Revocation List
- Exporting a Certificate Revocation List

#### Revoking a Certificate

How to revoke a certificate before its expiry date (due to misuse for example) to add it to the Certificate Revocation List.

- () A Certificate Revocation List is not mandatory for setting up an OpenVPN network with certificate-based authentication.
- → The XCA software is started and the project database is opened.
- → Client or server certificates have already been created.
- 1. Change to the "Certificates" tab.

vate Keys 📗 Certifica	ate signing requests	Certificates	Template:	Revocation I	ists
Internal name 🔺	commonName	CA S	5erial	Expiry date	
- Act ca	ca	🗸 0	01 20	20-10-13 GMT	New Certificate
Client1	client1	No	03 20	11-10-13 GMT	Export
client2	client2	Nn Iertificate	04 20	11-10-13 GMT	Import
- Spa	Impor	t t PKCS#12			Show Details
	Impor	t from PKCS#7			Delete
	Show	Details			Import PKCS#12
	Expor Delete	t 9			Import PKCS#7
	Delete Trust	from Security tol	ken		Plain View
	CA		+		
	Renev	val			
	Revok	e			
	Colum	ns	- •		A Farmineta
					Dinburg of Time

2. Select the certificate you want to revoke and select in the context menu (rightclick) "Revoke".

🖌 xca Revokation details —			? 🛛
Invalid since	2010-10-13 17:02		~
Revokation reason		Unspecified	~
			ОК

- 3. If require, select a reason for the revocation and click on OK.
  - $\checkmark$  You have prepared the certificate for a revocation with this.
  - () The Certificate Revocation List must be generated again after this.
- Generating a Certificate Revocation List

How to create a Certificate Revocation List with XCA.

- () A Certificate Revocation List is not mandatory for setting up an OpenVPN network with certificate-based authentication.
- → The XCA software is started and the project database is opened.
- → At least one certificate has been revoked.
- 1. Change to the "Certificates" tab.

vate Keys 📗 Certificate signing	grequests Certificates Tem	olates Revocation lists	
Internal name 🔶 comi Nesto ca ca	nonName CA Serial	Expiry date	<u>N</u> ew Certificate
client1 client1	New Certificate Import	2011-10-13 GM1	Export
server server	Import PKCS#12 Import from PKCS#7	2011-10-13 GMT	Import
	Rename Show Details		<u>S</u> how Details
	Export +		Delete
	Delete from Security token		Import <u>P</u> KC5#12
	Trust		Import PKCS#7
	CA +	Properties	Plain View
	Renewal Revoke Columns •		
			Jarminata Osvindonos Jina

- 2. Select the CA certificate and select in the context menu (right-click) CA → Create CRL.
  - $\checkmark$  The dialogue window for creating a CRL appears:

🖋 X Certificate and Key manag	ement	? 🛛
Create CRL		
Dates		
last update	2010-10-13 17:03	~
next update	2010-11-13 17:03	~
1 Midnight		Months
Hashing algorithm		~
Extensions  Authority key identifier  Subject alternative name  CRL Number  Revokation reasons		
	ОК	Cancel

- 3. Click on OK.
- 4. Confirm the generation of the Certificate Revocation List with OK.

- You have generated a Certificate Revocation List with this that contains all revoked certificates of this CA.
- () If further certificates are revoked after generating the Certificate Revocation List, the certificate revocation list must be generated again.

#### Exporting a Certificate Revocation List

How to export the Certificate Revocation List from the XCA database.

- → The XCA software is started and the project database is opened.
- → A Certificate Revocation List has been created.
- 1. Change to the "Revocation Lists" tab.

rivate Keys Certificate signing requests	Certificates	Templates	Revocation lists	
Internal name	Signer	No. revoked	Net	
📷 ca	ca		1 2010-1	Export
				Import
				Show Details
				Delete
		Υ.		Contraction of the second seco
<u>{  </u>				

2. Highlight the Certificate Revocation List and select Export

 $\checkmark$ 

The Certificate Revocation List export dialogue window appears:

🖌 X Certi	ficate and Key management	? 🛛
Revok	ation list export	O REAL OF
Please en	ter the filename	
Filename	C:/XCA_Database\ca.crl	
DER is a b PEM is a b	inary format ase64 encoded DER file	
Export Fo	rmat PEM	
		OK Cancel

- 3. Specify a path and file name.
  - () It is recommended to select the file name identical to the "Common Name" of the certificate and change the suffix to "crl" to enhance clarity if this is not contrary to any security concerns.
- 4. Select the "PEM" export format.
- 5. Click on OK.
  - ✓ You have exported the Certificate Revocation List with this. The CRL must now be uploaded to the OpenVPN server that the certificates will be revoked.

# 3 Used Components

# Software

Description	Manufacturer	Туре	Version
XCA	Christian Hohn- städt (Freeware)	X certificate and key management	0.9.1 or higher
Operating system	Microsoft	Windows	XP, Vista, 7

#### Germany

INSYS icom GmbH Hermann-Köhl-Str. 22 93049 Regensburg Germany

 Phone
 +49 941 58692 0

 Fax
 +49 941 58692 45

 E-mail
 info@insvs-icom.com

E-mail <u>info@insys-icom.com</u> URL <u>www.insys-icom.com</u>

#### **Czech Repulic**

INSYS icom CZ, s.r.o. Slovanská alej 1993 / 28a 326 00 Plzen-Východní Předměstí Czech Republic

Phone	+420 377 429 952
Fax	+420 377 429 952
Mobile	+420 777 651 188

E-mail <u>info@insys-icom.cz</u> URL <u>www.insys-icom.cz</u>