## Guide to create and export custom certificates using XCA.

- 1. Download XCA : <u>https://sourceforge.net/projects/xca/</u>
- 2. After installing it you'll have to create a database within which the private keys and certificates will be stored.

File  $\rightarrow$  New DataBase  $\rightarrow$  set a file name on your disk, called for example test.xdb and a password to encrypt data within it.

- 3. Open the new created xdb file.
- 4. We'll create a chain composed of 1 ROOT  $\rightarrow$  1 CA  $\rightarrow$  and 2 user certificates:

ROOT MyOrg\_ROOT.crt CA MyOrg\_CA.crt USER\_SSL MyOrg\_USER\_SSL.p12 USER\_SSO MyOrg\_USER\_SSO.p12

## a) ROOT

In the Certificates tab click on New Certificate

ile I <u>m</u> port <u>T</u> oken Extra <u>I</u>	<u>H</u> elp									
Private Kevs Certificate signing	a requests	Certificates	Templates	Rev	ocation lis	sts				
let-mel			^ N		<b>C</b> A					_
Internal han	ne		commonivam	e			<u>N</u> ew Ce	rtificate		
							Exp	oort		
							Imp	oort		
							Show I	Details		
							Del	ete		
							Import P	KCS#12		
							Import	P <u>K</u> CS#7		
							Plain	View		
٢					>	e	DUring	ines ;	<i>Jim</i>	
atabase: C:/Users/Danutz-PC/Dc Certificate and Key management	ocuments/test	123.xdb	2	×	>		Of Thing	une6 ;	Jim	
Certificate and Key management	ocuments/test	123.xdb	2	×	>		This G	une6 , ;	Ţina	
atabase: C:/Users/Danutz-PC/Dc       Certificate and Key management       ate x509 Certificate       rce     Subject       Extensions     Key usage       Nets	ocuments/test	123.xdb	?	×	>		D.Y.	kne6	Ţina	
Certificate and Key management Certificate and Key management Deate x509 Certificate	cope Advanced	123.xdb	?	×	>		D.Viers <sup>6</sup>	kne6	Ţina	
Atabase: C:/Users/Danutz-PC/Dc Certificate and Key management Bate x509 Certificate rcc Subject Extensions Key usage Nets going request going request Son this Certificate agoing request	cope Advanced	123.xdb	?	×	>		D.Vierd	kne6	<u> </u>	
Certificate and Key management Certificate and Key management Deate x509 Certificate grace Subject Extensions Key usage Nets grang request Gopy extensions from the request	cope Advanced	123.xdb	? ? Quest	×	· ·		(D) line	ine i	<i><b>Jinn</b></i>	
Certificate and Key management Certificate and Key management	cope Advanced	123.xdb Show rec	? ? Quest	×	,	3	D.Viendo	ine 6	Ţina	
Certificate and Key management Certificate and Key management Deate x509 Certificate grace Subject Extensions Key usage Nets gring request Gopy extensions from the request Modify subject of the request gring	cape Advanced	123.xdb	? Quest	×	,		(D) Yeres		Ţina	
Certificate and Key management Certificate and Key management Certificate Certificate Certificate Certificate Copy extensions from the request Copy extensions Certificate as elf signed certificate with the serial Copy extension Certificate Certificate as elf signed certificate with the serial Certificate Certif	cape Advanced	123.xdb Show rec	? Quest	×	,		(D) Yerres	ine i	Ţina	
Certificate and Key management Certificate and Key management Sign this Certificate signing request Copy extensions from the request Modify subject of the request Igning Create a self signed certificate with the serial Copy the the Certificate for signing	couments/test	123.xdb	? Quest	×	,		(D) Viendo		Ţina	
Atabase: C:/Users/Danutz-PC/Do Certificate and Key management Bate x509 Certificate arror Subject Extensions Key usage Nets Igning request Gopy extensions from the request Igning Ocease a self signed certificate with the serial I Ouse this Certificate for signing Insture algorithm	cope Advanced	123.xdb	? Quest	×	,		(D) Yerds		Ţina	
atabase: C:/Users/Danutz-PC/Do Certificate and Key management Bate x509 Certificate Urce Subject Extensions Key usage Nets againg request Sign this Certificate signing request Copy extensions from the request Modify subject of the request againg Create a self agned certificate with the serial Use this Certificate for signing Instare algorithm Emplate for the new certificate	cape Advanced	123.xdb	quest	×	· ·		(D) Yerry		Ţina	
atabase: C:/Users/Danutz-PC/Do Certificate and Key management eate x509 Certificate urce Subject Extensions Key usage Nets signing request Sign this Certificate signing request Copy extensions from the request Modify subject of the request againg Create as self signed certificate with the serial Use this Certificate for signing nature algorithm emplate for the new certificate [default] CA	cape Advanced	123.xdb	quest	×	,		(D) Yerres		Ţina	
Atabase: C:/Users/Danutz-PC/Dc Certificate and Key management Bate x509 Certificate urce Subject Extensions Key usage Nets igning request Gopy extensions from the request Copy extensions Copy exte	couments/test	123.xdb	quest Apply subject Apply al	×	,		(D) Yerds		Ţina	
Atabase: C:/Users/Danutz-PC/Do K Certificate and Key management  eate x509 Certificate  surce Subject Extensions Key usage Nets  Signing request  Signing request  Modify subject of the request  Signing  Create a self signed certificate with the serial 1  Use this Certificate for signing  gnature algorithm  Template for the new certificate  [default] CA	cape Advanced	123.xdb	quest Apply subject Apply al	×	,		(D) Yerre		Ţina	

Click on the second tab, **Subject** add the details of your ROOT certificate. After adding the details we'll generate the Private key by clicking on "Generate a new key".

nternal name	MyOra ROOT	organizationName		
countryName	RO	organizationalUnitN	Jame AxwayPassPort	
stateOrProvinceName	Bucharest	commonName	MyOrg ROOT	
ocalityName	Bucharest	emailAddress	support@axway.com	
				Delete
				Delete

🥑 X Certifi	cate and Key management	?	×
New ke	у	)=	<b> </b>
Please give a	a name to the new key and select the desired keysize		
Key proper	ties		
Name	MyOrg_ROOT		
Keytype	RSA		•
Keysize	2048 bit		~
Rememb	er as default Create	Canc	el

You can adjust the Name, Keytype and Keysize as per your need. In my case I'll keep the default values. Click on **Create**.

The private key for the MyOrg\_ROOT has been created.

		CLAINE IN THE NEW KEY AND	Celer Line neoren kevor	P	
X Certificate and Key	management			?	×
Create x509 Ce	ertificate			A Remark	
Source Subject I	Extensions Key usage Netscape	Advanced			
Distinguished name					
Internal name	MyOrg_ROOT	organizationName	AxwayMFT		
countryName	RO	organizationalUnitName	AxwayPassPort		
stateOrProvinceName	Bucharest	commonName	MyOrg_ROOT		
X Certificate and Key ma	anagement X	emailAddress	support@axway.com		
Successfully creat	ted the RSA private key 'MyOrg ROOT'	Content		Add	
	ter the top physic key myorg too t			Delete	
	ОК			Delete	
Private key			_		
MyOrg_ROOT (RSA:20	048 bit)	•	Used keys too Ger	nerate a new key	
			OK	Cancel	

Afterwards switch to the 3<sup>rd</sup> tab, **Extensions** and set the Type to **Certification Authority**. **Do not click on OK at this step**.

🖉 X Certificate and Key manager	nent			?	×
Create x509 Certifica	te			a Permante P	
Source Subject Extensions	Key usage Netscape A	Advanced			
X509v3 Basic Constraints Type Certification Author Path length	ity	▼ Critical	Key identifier	ey Identifier Key Identifier	
Validity Not before Not after	2019-05-28 07:28 GMT ∨ 2020-05-28 07:28 GMT ∨	Time range 1 Midnight Local time	Years  Vears Vears Vears	Apply ed expiration	
X509v3 Subject Alternative Name				Edit	
X509v3 Issuer Alternative Name				Edit	
X509v3 CRL Distribution Points				Edit	
Authority Information Access	OCSP 👻			Edit	
			ОК	Cancel	

Switch to the 4<sup>th</sup> tab,<u>Key usage</u> and set the needed, desired key usages and then **click OK**.



ate Keys Certificate signing requests	Certificates	Templates	Revocation lists		
Internal name	o MyC	ommonName	CA	New Certificate	
	-			Export	
				Import	
				Show Details	
🖉 X Certificate and Key manage	ment	×		Delete	
Successfully created th	e certificate 'N	/lyOrg_ROOT'		Import PKCS#12	
				Import PKCS#7	
		OK		Plain View	
				Jarmineeta, Dahustooo Jin	15

Congrats you've created the ROOT certificate.

## **b) INTERMEDIATE CA**

We'll proceed same way with the Intermediate CA certificate.

Click on the MyOrg\_ROOT and then click the tab New Certificate to create the CA under it.

	<u>T</u> oken <b>Extra</b> <u>H</u> e	elp					
Private Keys	Certificate signing r	equests	Certificates	Templates	Revocation	lists	
	Internal name		N.	commonName	CA	New Certificate	
	MYOLG_KOOL		riy	org_koor	<b>V</b>	Export	
						<u>I</u> mport	
						Show Details	
						Delete	
						Import PKCS#12	
						Import PKCS#7	
						Plain View	
٢					>	Janineta Dingenos Jin	Ha
t-h C/U			-+122				

Click on Subject tab,add details of your Intermediate CA certificate, followed by Generate a new key:

🞻 X Certificate and Key	management			?	×
Create x509 C	ertificate			(a) Francisco	A Time
Source Subject	Extensions Key usage Netscape	Advanced			
Distinguished name					
Internal name	MyOrg_CA	organizationName	AxwayMFT		
countryName	RO	organizationalUnitName	AxwayPassPort		5
stateOrProvinceName	Bucharest	commonName	MyOrg_CA		=
localityName	Bucharest	emailAddress	support@axway.com		=
Тур	De	Content		Add	
Private key		•	Used keys too Ge	enerate a new k	ey

Click on Create and the private key for the Intermediate certificate will be created:

-						
X Certifi	cate and Key ma	nagement			?	×
lew ke	V			6		
	,			4		
ease give a	name to the new	key and selec	ct the desired ke	ysize		
Key proper	ties					
Name	MyOrg_CA					
Keytype	RSA					-
Kowizo	20.40 hit					
Neysize	2048 DIC					~
Remembe	er as default					
				Create	C	Cancel
X Certificate an	d Key management					?
X Certificate an	d Key management					?
X Certificate an	d Key management 9 <b>Certificate</b>					?
X Certificate an reate x509	d Key management 9 <b>Certificate</b> tt Extensions Key ut	sage Netscape	Advanced			?
X Certificate an reate x509 Source Subjet Distinguished na	d Key management 9 <b>Certificate</b> It Extensions Key us	sage Netscape	Advanced			?
X Certificate an reate x50 iource Subjer Distinguished na Internal name	d Key management 9 <b>Certificate</b> tt Extensions Key us me <u>MyOrg_CA</u>	sage Netscape	Advanced organizationName	AxwayMFT		?
X Certificate an reate x50! Source Subjer Distinguished na Internal name countryName	d Key management  Certificate  Extensions Key us  MyOrg_CA RO	sage Netscape	Advanced ] organizationName ] organizationalUnitName	AxwayMFT AxwayPassPort		?
X Certificate an reate x509 source Subjer Distinguished na Internal name countryName stateOrProvince	d Key management	sage Netscape	Advanced organizationName organizationalUnitName commonName	AxwayMFT e AxwayPassPort MyOrg_CA		?
X Certificate an reate x509 iource Subjer Distinguished na Internal name countryName stateOrProvince localityName	d Key management	sage Netscape	Advanced organizationName organizationalUnitName commonName emailAddress	AxwayMFT AxwayPassPort MyOrg_CA support@axway	/.com	?
X Certificate an reate x50! iource Subjer Distinguished na Internal name countryName stateOrProvince localityName	d Key management	sage Netscape	Advanced organizationName organizationalUnitName commonName emailAddress Content	AxwayMFT e AxwayPassPort MyOrg_CA support@axway	,.com	? The second sec
X Certificate an reate x509 iource Subject Distinguished na Internal name countryName stateOrProvince localityName	d Key management	sage Netscape	Advanced organizationName organizationalUnitName commonName emailAddress Content X	AxwayMFT e AxwayPassPort MyOrg_CA support@axway	/.com	? Add Delete
X Certificate an reate x509 iource Subjer Distinguished na Internal name countryName stateOrProvince localityName	d Key management	sage Netscape	Advanced organizationName organizationalUnitName commonName emailAddress Content × e key 'MyOrg_CA'	AxwayMFT AxwayPassPort MyOrg_CA support@axway		?
X Certificate an reate x509 iource Subjet Distinguished na Internal name countryName stateOrProvince localityName	d Key management	sage Netscape	Advanced  organizationName organizationalUnitName commonName emailAddress  Content  ke key 'MyOrg_CA'	AxwayMFT e AxwayPassPort MyOrg_CA support@axway	y.com	?
X Certificate an reate x509 iource Subject Distinguished na Internal name countryName stateOrProvince localityName	d Key management	sage Netscape	Advanced  organizationName organizationalUnitName commonName emailAddress  Content  ke key 'MyOrg_CA' OK	AxwayMFT e AxwayPassPort MyOrg_CA support@axway	/.com	? Add Delete
X Certificate an reate x509 iource Subjer Distinguished na Internal name countryName stateOrProvince localityName	d Key management	sage Netscape	Advanced  organizationName organizationalUnitName commonName emailAddress Content  ke key 'MyOrg_CA' OK	AxwayMFT e AxwayPassPort MyOrg_CA support@axway		? Add Delete
X Certificate an reate x509 Source Subjer Distinguished na Internal name countryName stateOrProvince localityName	d Key management	sage Netscape	Advanced  organizationName organizationalUnitName commonName emailAddress  Content  ke key 'MyOrg_CA'  OK	AxwayMFT AxwayPassPort MyOrg_CA support@axway	y.com	? Add Delete
X Certificate an reate x509 Source Subjer Distinguished na Internal name countryName stateOrProvince localityName	d Key management	sage Netscape	Advanced  organizationName organizationalUnitName commonName emailAddress  Content  key 'MyOrg_CA'  OK	AxwayMFT AxwayPassPort MyOrg_CA support@axway	,.com	? Add Delete
X Certificate an reate x509 Source Subjer Distinguished na Internal name countryName stateOrProvince localityName	d Key management	sage Netscape	Advanced  organizationName organizationalUnitName commonName emailAddress  Content  ke key 'MyOrg_CA'  OK	AxwayMFT AxwayPassPort MyOrg_CA support@axway	/.com	? Add Delete
X Certificate an reate x509 iource Subjer Distinguished na Internal name countryName stateOrProvince localityName	d Key management 9 Certificate tt Extensions Key us me MyOrg_CA RO Name Bucharest Bucharest Type X Certificate and Key m Successfully creations	sage Netscape	Advanced  organizationName organizationalUnitName commonName emailAddress  Content  ke key 'MyOrg_CA'  OK	AxwayMFT e AxwayPassPort MyOrg_CA support@axway	/.com	? Add Delete
X Certificate an reate x509 isource Subjet Distinguished na Internal name countryName stateOrProvince localityName	d Key management	sage Netscape	Advanced  organizationName organizationalUnitName commonName emailAddress  Content  key 'MyOrg_CA'  OK	AxwayMFT e AxwayPassPort MyOrg_CA support@axway	/.com	? Add Delete
X Certificate an reate x509 Gource Subjer Distinguished na Internal name countryName stateOrProvince localityName Private key	d Key management 9 Certificate t Extensions Key us me MyOrg_CA RO Name Bucharest Bucharest Type X Certificate and Key m Successfully creations Successfully creations A:2048 bit)	sage Netscape	Advanced  organizationName organizationalUnitName commonName emailAddress  Content  ke key 'MyOrg_CA'  OK	AxwayMFT AxwayPassPort MyOrg_CA support@axway	/.com	? Add Delete

Then switch to the 3<sup>rd</sup> tab, Extensions and set Type as Certification Authority.

Note:As long as this certificate will not be the last one in the chain(entity) it will be set as CA(Certification Authority).Only the last certificate in the chain, the user one, will be set as the End Entity.

Validity of Certificate can be adjusted as well.

X Certificate and Key management					?	$\times$
Create x509 Certificate						and a state of the
Source Subject Extensions Key usag	e Netscape	Advanced				
X509v3 Basic Constraints				Key identifier		
Type Certification Authority			•	Subject K	ey Identifier	
Path length			Critical	Authority	Key Identifie	r
Validity Not before 2019-05-28 ( Not after 2020-05-28 (	17:46 GMT	Time range	Local time	Years  Vowell-define	Apply ed expiration	
X509v3 Subject Alternative Name					Edit	
X509v3 Issuer Alternative Name					Edit	
X509v3 CRL Distribution Points					Edit	
Authority Information Access OCSP	•				Edit	
				OK	Cano	el

Set the Key usage and afterwards click OK to create the Intermediate CA certificate:

urce Subject	Extensions	Key usage	Netscape	Advanced		
Subject Subject Subject Solv 3 Key Usage - Crotecal Digital Signature Non Repudiation Key Encipherment Data Encipherment Certificate Sign Cretificate Sign Cretificate Sign Encipher Only Decipher Only Decipher Only	Extensions			XS09V3 ED Critica TLS Wel TLS Wel Code Sig E-mail P Time St. Microso Microso Microso Microso Microso Microso Netscap Microso Netscap Microso Netscap Microso Netscap Microso Netscap Microso Netscap Microso Netscap Microso Netscap Microso Netscap Microso	ctended Key Usage ctended Key Usage Server Authentication o Client Authentication amping ft Individual Code Signing ft Commercial Code Signing ft Crownercial Code Signing ft Trust List Signing ft Server Gated Crypto ft Eserver Gated Crypto ft ES File Recovery id System innel ier ft Smartcardlogin gning p PP r Lan thentication	

🛷 X Certificate and Key management		- 🗆 X
<u>F</u> ile I <u>m</u> port <u>Token</u> Extra <u>H</u> elp	ef x C	ertificate and Key management X
Private Keys Certificate signing requests	Certificates	Successfully created the certificate 'MyOrg_CA'
Internal name	cc	
MyOrg_ROOT	MyOr	ОК
		Import
		Snow Details
		Delete
		Import PKCS#12
		Import PKCS#7
		Plain View
٢		Jesminete Muchanos - Jine
Database: C:/Users/Danutz-PC/Documents/te	est123.xdb	

Click OK and afterwards expand the arrow and it should look like this:

	Certificates Templates	Revocation lists			-
Internal name	commonNam	ne CA Ser	ial Expiry date	CRL Expiration	New Certificate
MyOrg_RUOT	MyOrg_ROOT	Ves	01 2020-05-28		Export
Mars Hind on	inford_or	V 105	02 2020 00 20		Import
					Import
					Show Details
					Delete
					Import PKCS#12
					Import PKCS#7
					Plain View
					Zarmineeta 10
					De OWinderoo Jim

**c. USER** : Now let's create the USER certificate for the Passport SSL.

Click on the Intermediate Certificate and afterwards click on the New Certificate buton.

	– 🗆 X
Private Keys Certificate signing requests Certificates Templates Revocation lists	
Internal name MyOrg_ROOT MyOrg_ROOT MyOrg_CA MyOrg_CA MyOrg_CA MyOrg_CA Ves 02 2020-05-28 CRL Expiration CRL Expiration Ves 02 2020-05-28 CRL Expiration MyOrg_CA MyOrg_CA Ves 02 2020-05-28	Lew Certificate         Export         Import         Show Details         Delete         Import BKCS#12         Import PKCS#7         Plain View
Database. Cir oseis/Danutz-FC/Documents/test125300	

Add the details in the Subject tab and generate the Private key correspondent to this certificate.

reate x509 C	ertificate		
Source Subject	Extensions Key usage Netscape	Advanced	
Distinguished name			
Internal name	MyOrg_USER_SSL	organizationName	AxwayMFT
countryName	RO	organizationalUnitName	AxwayPassPort
stateOrProvinceName	Bucharest	commonName	MyOrg_USER_SSL
localityName	Bucharest	emailAddress	support@axway.com
Please give a na	المحتجمان وملقاته والمحاصر ليحجز بتجنأ بتنجح وملقا مقاصي		
Key properties	Org_USER_SSL	eysize	
Key properties Name My Keytype RS Keysize 20	A 148 bit	eysize	

🖋 X Certificate and Key management	? ×
Create x509 Certificate	(a) Westing The
Source Subject Extensions Key usage Netscape Advanced	
Distinguished name	
Internal name X Certificate and Key management	wayMFT
countryName	kwayPassPort
stateOrProvinc Successfully created the RSA private key 'MyOrg_USER_SSL'	yOrg_USER_SSL
localityName	pport@axway.com
ОК	
Type Content	Add
	Delete
Private key	
MyOrg_USER_SSL (RSA:2048 bit)	Used keys too Generate a new key
	OK Cancel

In the 3<sup>rd</sup> tab, Extensions set the **Type** to **End Entity** being the last certificate in the chain :

X509v3 Basic Constraints       Key identifier         Type       End Entity         Path length       Critical         Validity       Critical         Validity       Time range         Not before       2019-05-28 07:57 GMT          2020-05-28 07:25 GMT        Midnight         Local time       No well-defined expiration	X509v3 Basic Constraints       Key identifier         Type       End Entity       Subject Key Identifier         Path length       Critical       Authority Key Identifier         Validity       Time range       Authority Key Identifier         Not before       2019-05-28 07:57 GMT        I         Years       Apply         Not after       2020-05-28 07:28 GMT        Midnight         S09v3 Subject Alternative Name       Edit
Type       End Entity <ul> <li>Subject Key Identifier</li> <li>Critical</li> <li>Subject Key Identifier</li> <li>Authority Key Identifier</li> </ul> Validity         Time range           Not before         2019-05-28 07:57 GMT            1         Years < Apply           Not after         2020-05-28 07:28 GMT            Midnight         Local time           No well-defined expiration	Type       End Entity <ul> <li>Subject Key Identifier</li> <li>Critical</li> <li>Subject Key Identifier</li> </ul> Validity       Time range         Not before       2019-05-28 07:57 GMT          1       Years < Apply         Not after       2020-05-28 07:28 GMT          509v3 Subject Alternative Name       Edit
Validity       Time range         Not before       2019-05-28 07:57 GMT          2020-05-28 07:28 GMT        Midnight         Local time       No well-defined expiration	Path length       Critical       Authority Key Identifi         Validity       Time range         Not before       2019-05-28 07:57 GMT        I         Years       Apply         Not after       2020-05-28 07:28 GMT        Image         S09v3 Subject Alternative Name       Edit
Validity  Not before  2019-05-28 07:57 GMT   Not after  2020-05-28 07:28 GMT  Midnight Local time No well-defined expiration	Validity  Not before  2019-05-28 07:57 GMT  Not after  2020-05-28 07:28 GMT  Kook after  Cook after Cook after Cook after  Cook after  Cook after  Coo
Validity Not before 2019-05-28 07:57 GMT V Not after 2020-05-28 07:28 GMT V Midnight Local time No well-defined expiration	Validity Not before 2019-05-28 07:57 GMT V Not after 2020-05-28 07:28 GMT V Midnight Local time No well-defined expiration 509v3 Subject Alternative Name
	2509v3 Subject Alternative Name
	(509v3 Subject Alternative Name
	(509v3 Subject Alternative Name
	(509v3 Subject Alternative Name
509v3 Subject Alternative Name Edit	
	(509v3 Issuer Alternative Name Edit
509v3 Issuer Alternative Name	
(509v3 Issuer Alternative Name Edit	
509v3 Subject Alternative Name Ed	

Set the Key usages and the <b>c</b>	click OK to create it
-------------------------------------	-----------------------

	(a) and 3 700	
rce Subject Extensions Key usage Netscape	Advanced	
09v3 Key Usage	X509v3 Extended Key Usage	
Critical	Critical	
igital Signature	TLS Web Server Authentication	
on Repudiation	TLS Web Client Authentication	
ey Encipherment	Code Signing	
ev Agreement	E-mail Protection	
ertificate Sign	Microsoft Individual Code Signing	
RL Sign	Microsoft Commercial Code Signing	
rcipher Only ecipher Only	Microsoft Trust List Signing Microsoft Server Gated Counto	
capiter only	Microsoft Encrypted File System	
	Netscape Server Gated Crypto	
	Microsoft EFS File Recovery	
	IPSec Tunnel	
	IPSec User	
	IP security end entity	
	Viicrosoft Smartcardlogin OCSP Signing	
	EAP over PPP	
	EAP over Lan	
	KDC Authentication	
Certificate and Key management		
Certificate and Key management <u>mport</u> <u>Ioken</u> Extra <u>H</u> elp to Kours <u>Certificates</u> T		
ertificate and Key management mport Joken Extra Help te Keys Certificate signing requests Certificates T	emplates Revocation lists	
Certificate and Key management Import Ioken Extra Help te Keys Certificates signing requests Certificates T Internal name com MyOrg_ROOT MyOrg	emplates Revocation lists monName CA Serial Expiry date CRL Expiration Ref X X Certificate and Key management X	
ertificate and Key management mport Ioken Extra Help te Keys Certificates signing requests Certificates T Internal name com MyOrg_ROOT MyOrg_ > MyOrg_CA MyOrg_	emplates Revocation lists           monName         CA         Serial         Expiry date         CRL Expiration           M         X         Certificate and Key management         X	<u>N</u> ew Certificate
ertificate and Key management mport Ioken Extra Help te Keys Certificates signing requests Certificates T Internal name com MyOrg_ROOT MyOrg_ MyOrg_CA MyOrg_	emplates Revocation lists           monName         CA         Serial         Expiry date         CRL Expiration           R4         X         Certificate and Key management         X           C4         Image: Successfully created the certificate 'MyOrg_USER_SSL'         Successfully created the certificate 'MyOrg_USER_SSL'	
ertificate and Key management mport Ioken Extra Help te Keys Certificate signing requests Certificates T Internal name com MyOrg_ROOT MyOrg_ MyOrg_CA MyOrg_	emplates Revocation lists monName CA Serial Expiry date CRL Expiration	
ertificate and Key management mport Ioken Extra Help te Keys Certificate signing requests Certificates T Internal name com MyOrg_ROOT MyOrg_ MyOrg_CA MyOrg_	emplates Revocation lists monName CA Serial Expiry date CRL Expiration Revocation lists C Successfully created the certificate 'MyOrg_USER_SSL' OK	 <u>N</u> ew Certificate <u>Export</u> <u>Import</u> <u>Show Details</u> <u>Delete</u>
ertificate and Key management mport Ioken Extra Help te Keys Certificates signing requests Certificates T Internal name com MyOrg_ROOT MyOrg_ MyOrg_CA MyOrg_	emplates Revocation lists  monName CA Serial Expiry date CRL Expiration  R  X  C  Successfully created the certificate 'MyOrg_USER_SSL'  OK	New Certificate Export Import Show Details Delete Terrort PECC #12
ertificate and Key management mport Ioken Extra Help te Keys Certificates signing requests Certificates T Internal name com MyOrg_ROOT MyOrg_ MyOrg_CA MyOrg_	Implates       Revocation lists         monName       CA       Serial       Expiry date       CRL Expiration         R       X Certificate and Key management       X         G       Successfully created the certificate 'MyOrg_USER_SSL'         OK	Liew Certificate Export Import Show Details Delete Import PKCS#12
ertificate and Key management mport Ioken Extra Help te Keys Certificate signing requests Certificates T Internal name com MyOrg_ROOT MyOrg_ MyOrg_CA MyOrg_	emplates       Revocation lists         monName       CA       Serial       Expiry date       CRL Expiration         R       X Certificate and Key management       X         Successfully created the certificate 'MyOrg_USER_SSL'         OK	New Certificate       Export       Import       Show Details       Delete       Import PKCS#12       Import PKCS#7
ertificate and Key management mport Ioken Extra Help te Keys Certificate signing requests Certificates T Internal name com MyOrg_ROOT MyOrg_ MyOrg_CA MyOrg_	emplates       Revocation lists         monName       CA       Serial       Expiry date       CRL Expiration         R       X Certificate and Key management       X         G       Successfully created the certificate 'MyOrg_USER_SSL'         OK	Lew Certificate Export Import Show Details Qelete Import PKCS#12 Import PKCS#7 Plain View
Certificate and Key management Import Ioken Extra Help te Keys Certificate signing requests Certificates T Internal name com MyOrg_ROOT MyOrg_ > MyOrg_CA MyOrg_	implates       Revocation lists         monName       CA       Serial       Expiry date       CRL Expiration         R       X       Certificate and Key management       X         G       Successfully created the certificate 'MyOrg_USER_SSL'         OK	New Certificate Export Import Show Details Qelete Import PKCS#12 Import PKCS#12 Import PKCS#7 Plain View
Certificate and Key management Import Ioken Extra Help te Keys Certificates signing requests Certificates T Internal name com MyOrg_ROOT MyOrg_ > MyOrg_CA MyOrg_	iemplates       Revocation lists         monName       CA       Serial       Expiry date       CRL Expiration         R       X Certificate and Key management       X       X         Successfully created the certificate 'MyOrg_USER_SSL'       OK	New Certificate Export Import Show Details Delete Import PKCS#12 Import PKCS#12 Plain View
Certificate and Key management Import Ioken Extra Help tte Keys Certificates signing requests Certificates T Internal name com MyOrg_ROOT MyOrg_ > Me MyOrg_CA MyOrg_	emplates Revocation lists monName CA Serial Expiry date CRL Expiration	New Certificate         Export         Import         Show Details         Qelete         Import PKCS#12         Import PKCS#7         Plain View
Certificate and Key management Import Ioken Extra Help ate Keys Certificate signing requests Certificates T Internal name com MyOrg_ROOT MyOrg_ > MyOrg_CA MyOrg_	Implates       Revocation lists         monName       CA       Serial       Expiry date       CRL Expiration         M       X Certificate and Key management       X       X         Image: Comparison of the series	New Certificate       Export       Import       Show Details       Qelete       Import PKCS≠12       Import PKCS≠7       Plain View
Certificate and Key management Import Ioken Extra Help tet Keys Certificates igning requests Certificates T Internal name com MyOrg_ROOT MyOrg MyOrg_CA MyOrg_CA	Implates       Revocation lists         monName       CA       Serial       Expiry date       CRL Expiration         R       X Certificate and Key management       X       X         G       Successfully created the certificate 'MyOrg_USER_SSL'       OK	Liew Certificate Export Import Show Details Delete Import PKCS#12 Import PKCS#7 Plain View
Certificate and Key management Import Ioken Extra Help ste Keys Certificates igning requests Certificates T Internal name com MyOrg_ROOT MyOrg_ > ₩90rg_CA MyOrg_	emplates       Revocation lists         monName       CA       Serial       Expiry date       CRL Expiration         R       X Certificate and Key management       X       X         G       Successfully created the certificate 'MyOrg_USER_SSL'       OK	Liew Certificate Export Import Show Details Delete Import PKCS#12 Import PKCS#12 Plain View
Certificate and Key management Import Ioken Extra Help ste Keys Certificates signing requests Certificates T Internal name com MyOrg_ROOT MyOrg_ MyOrg_CA MyOrg_	emplates       Revocation lists         monName       CA       Serial       Expiry date       CRL Expiration         R       X Certificate and Key management       X         Successfully created the certificate 'MyOrg_USER_SSL'         OK	New Certificate         Export         Import         Show Details         Oplete         Import PKCS#12         Import PKCS#7         Plain View
Certificate and Key management Import Ioken Extra Help tte Keys Certificates signing requests Certificates T Internal name com MyOrg_ROOT MyOrg_ > ♪ ♪ ↓ MyOrg_CA MyOrg_	emplates       Revocation lists         monName       CA       Serial       Expiry date       CRL Expiration         R       X Certificate and Key management       X         Image: Successfully created the certificate 'MyOrg_USER_SSL'       Image: Successfully created the certificate 'MyOrg_USER_SSL'         Image: OK       Image: Successfully created the certificate 'MyOrg_USER_SSL'	New Certificate         Export         Import         Show Details         Qelete         Import PKCS#12         Import PKCS#12         Import PKCS#7         Plain View

Expand the second arrow and you'll see the new MyOrg\_USER\_SSL under the MyOrg\_CA.

X Certificate and Key management <u>File</u> Import <u>Ioken</u> Extra <u>H</u> elp		– o ×
Private Keys Certificate signing requests	Certificates Templates Revocation lists	
Internal name V MyOrg_EOOT V MyOrg_CA MyOrg_USER_SSL	commonName MyOrg_ROOT     CA Yes     Serial     Expiry date     CRL Expiration       MyOrg_CA     Yes     01     2020-05-28       MyOrg_USER_SSL     No     03     2020-05-28	New Certificate         Export         Import         §how Details         Qelete         Import PKCS≠12         Import PKCS≠12         Import PKCS≠7         Plain View
Database: C:/Users/Danutz-PC/Documents/te	est123.xdb	

Redo the same step for the MyOrg\_USER\_SSO , step c).

X Certificate and Key management <u>File</u> Import <u>I</u> oken Extra <u>H</u> elp		– 🗆 X
Private Keys Certificate signing requests	Certificates Templates Revocation lists	
Internal name V MyOrg_ROOT V MyOrg_CA MyOrg_USER_SSL Not MyOrg_USER_SSO	commonName MyOrg_ROOT     CA     Serial     Expiry date     CRL Expiration       MyOrg_ROOT     Yes     01     2020-05-28       MyOrg_USER_SSL     No     03     2020-05-28       MyOrg_USER_SSO     No     04     2020-05-28	New Certificate         Export         Import         Show Details         Delete         Import PKCS#12         Import PKCS#7         Plain View
Database: C:/Users/Danutz-PC/Documents/te	st123.xdb	

## Export the certificates

We'll export the USER SSL and SSO certificates in private format, pkcs12.

Right click on the MyOrg\_USER\_SSO  $\rightarrow$  Export  $\rightarrow$  File  $\rightarrow$  Set the Export format for PKCS #12 chain (\*.p12), click OK

🛷 X Certificate and Key management		- 🗆 X
<u>File Import <b>Token</b> Extra H</u> elp		
Private Keys Certificate signing requests Certifica	ates Templates Revocation lists	
Internal name	commonName CA Serial Expiry date CRL Expiration MyOrg_ROOT  Yes 01 2020-05-28	New Certificate
V MyOrg_CA	MyOrg CA 🖌 Yes 02 2020-05-28	Export
MyOrg_USER_SSL	√ X Certificate and Key management ? X	Import
MyOrg_USER_SSO	Certificate export	<u>S</u> how Details
		Delete
	Name MyOrg_USER_SSO	Import PKCS#12
	Filename C:/Program Files (x86)/xca\MyOrg_USER_SSO.p12	Import PKCS#7
	The complete certificate chain and the private key as encrypted PKCS#12 file  Export Format  PKCS #12 chain (*.p12)	Plain View
	OK Cancel	
		2 Porminaele Tine
Database: C:/Users/Danutz-PC/Documents/test123.xdb		

Enter a password to encrypt the PCKS12 file. This password will be used/needed when importing the certificate in the sso.jks file.

Same procedure for the MyOrg\_USER\_SSL certificate, used for ssl.jks

We'll export the ROOT certificate in public format , .pem or .crt

🛷 X Certificate and Key management		- 🗆 X
<u>F</u> ile l <u>m</u> port <u>Token</u> Extra <u>H</u> elp		
Private Keys Certificate signing requests Certifica	ates Templates Revocation lists	
Internal name	commonName         CA         Serial         Expiry date         CRL Expiration           MyOrg_ROOT         ✓ Yes         01 2020-05-28         Image: CRL Expiration         Image: CRL Expiration	New Certificate
V MyOrg_CA	MyOrg CA 🖌 Yes 02 2020-05-28	Export
MyOrg_USER_SSL	√ X Certificate and Key management ? X	Import
MyOrg_USER_SSO		Show Details
		<u>D</u> elete
	Name MyOrg_CA	Import PKCS#12
	Filename C:/Program Files (x86)/xca WyOrg_CA.crt	Import PKCS#7
	PEM Text format with headers	Plain View
	Export Format	
	OK Cancel	
		Josminecto Dinbaro 7 Jins
Database: C:/Users/Danutz-PC/Documents/test123.xdb		

Certained to Signing requests		
Internal name	commonName CA Serial Expiry date CRL Expiration	New Certificate
MyOrg_ROOT	MyOrg_ROOT Ves 01 2020-05-28	Export
MyOrg USER SSL	X Certificate and Key management ? X	Export
MyOrg USER SSO		Import
	Certificate export	Show Details
		Delete
	Name MyOrg_ROOT	Import PKCS#12
	Filename C:/Program Files (x86)/xra WwOrg ROOT.crt	Internet DKCC #7
		Import PKCS#7
	PEM Text format with headers	Plain View
	Export Format	
	PEM (*.crt)	
	OK Cancel	
		Janningte 10
		Dinberno Time

At the end of the exports we should have:

MyOrg\_ROOT.crt (public format), correspondent to the ROOT certificate

MyOrg\_CA.crt (public format), correspondent to the INTERMEDIATE certificate MyOrg\_USER\_SSL.p12 (private format), correspondent to the SSL USER certificate MyOrg\_USER\_SSO.p12 (private format), correspondent to the SSO USER certificate