#### **Start XCA**

0 0 37 X Certificate and Key management						
Private Keys	Certificate signing requests	Certificates	Templates Revocation lists			
			New Key			
			Export			
			Import			
			Import PFX (PKCS#12)			
			Show Details			
			Delete			
			XCH			

#### Create a new database

🛒 xca	File Import Token He	lp			
Filesystem	New DataBase	ЖN	ed Avail Capacity	iused ifree %iused M	ounted on
	Open DataBase	ж0	G1 44/G1 52% 1	26862858 11/085116 52% ,	
	Set as default DataBase		ate and key manage		
	Close DataBase	жW	ests Certificates	Templates Revocation lis	ts bileBacku
2	Dump DataBase			Naw Kay	one
	Change DataBase passwo	rd		New Key	
D	Undelete items			Export	
				Import	
				Import PFX (PKCS#12	)
				Show Details	
				Dalata	
				Delete	
					1

### Name and save your database

000	Open X0	CA Database	
	Save As: s3c3.xdb		
FAVORITES Dropbox Desktop Applications Sjan Documents Movies Music Pictures	<ul> <li>1.php</li> <li>29NewFreeFonts</li> <li>apache.html</li> <li>api.del.icio.us</li> <li>Applications</li> <li>Applicati(Parallels)</li> <li>applist.txt</li> <li>Archive</li> <li>autotwb1122.html</li> <li>away</li> <li>basic_ruleset.txt</li> </ul>		
	Format: XCA Databases	( *.xdb )	\$
New Folder			Cancel Save

# Select a password - you will need this every time you reopen this database

0	🕜 X Certificate and I	Key management
Private Keys	Certificate signing requests	Certificates Templates Revocation list
		New Key
	New Pass	word
Password		
Please enter a /Users/sjan/s	password, that will be used to en 3c3.xdb	crypt your private keys in the database file:
Reneat Passw	ord assesses	
Repear rassi		
Exit		Cancel OK
Exit		Cancel OK
Exit		Cancel OK

### Generate a new private key for the root CA

00	🖉 X Certificate and Key manage	ment
Private Keys	Certificate signing requests Certificates	Templates Revocation lists
Internal name	Type Size Use Password	New Key
		Export
		Import
		Import PFX (PKCS#12)
		Show Details
		Delete
		KOX STATE
Database:/Users/sjar	n/s3c3.xdb	

# Name it something like s3c3\_root - we are using 4098 bits for the example

000	🖉 X Certificate and Ke	y management	
Private Keys C	Certificate signing requests Cert	rtificates Templates R	evocation lists
Internal name 🔺 Typ	oe Size Use Password	N	ew Key
	X Certificate and Key ma	anagement	port
New	key		port
			X (PKCS#12)
Please	e give a name to the new key and	select the desired	
Keysia	properties		Details
			elete
Nai	me sc3c_root		
к	eytype RSA	*	
к	eysize 4096 bit		
		Cancel Create	
			mm
		×	
Database:/Users/sjan/s3	c3.xdb		//

### Your shiny new key

00	X Certificate and Key manage	ment
Private Keys	Certificate signing requests Certificates	Templates Revocation lists
Internal name A	Type Size Use Password RSA 4096 bit 0 Common	New Key
k		Export
		Import
		Import PFX (PKCS#12)
		Show Details
		Delete
		T HO STATE
Database:/Users/sjan	/s3c3.xdb	

### **Create a new self-signed certificate**

O O S X Certificate and Key management						
Private Keys	Certificate signing requests	Certificates	Templates Revocation lists			
Internal name 🔺	commonName CA Serial	Expiry date	New Certificate			
			Export			
			Import			
			Show Details			
			Delete			
			Import PKCS#12			
			Import PKCS#7			
			Plain View			
			Insuminesta Divindense Jim			
atabase:/Users/sja	n/s3c3.xdb					

# Make sure the selected template is CA and click on Apply extensions

	X Certificate	e and Key manage	ment	
e x509 Certificate				Promisand
Source S	Subject Extension	ns Key usage	Netscape Advan	ced
Signing request				
Sign this Certificate signing	g request			* *
Copy extensions from the r	request		Show reques	it
Modify subject of the reque	est			
<b>N</b>				
signing				
• Create a self signed certific	ate with the serial	1		
• Create a self signed certific	cate with the serial	1		
Create a self signed certific     Use this Certificate for sign	cate with the serial	1		\$
Create a self signed certific     Use this Certificate for sign	tate with the serial	1		\$
<ul> <li>Create a self signed certific</li> <li>Use this Certificate for sign</li> <li>gnature algorithm</li> </ul>	tate with the serial	1 		÷)
• Create a self signed certific Use this Certificate for sign gnature algorithm Femplate for the new certificate	tate with the serial	1		÷
Create a self signed certific     Use this Certificate for sign gnature algorithm Template for the new certificate	tate with the serial	1 		÷
Create a self signed certific     Use this Certificate for sign gnature algorithm Template for the new certificate [default] CA	tate with the serial	1 SHA 1		4 4 4
Create a self signed certific     Use this Certificate for sign gnature algorithm Template for the new certificate [default] CA	tate with the serial	1 SHA 1	ions Apply subj	¢
• Create a self signed certific Use this Certificate for sign gnature algorithm Template for the new certificate [default] CA	tate with the serial	1 SHA 1	ions Apply subj	÷ t t t t t t t t t t t t t
• Create a self signed certific Use this Certificate for sign gnature algorithm Template for the new certificate [default] CA	tate with the serial	1 SHA 1	ions Apply subj	÷ t t t t t t t t t t t t t
Create a self signed certific     Use this Certificate for sign gnature algorithm Template for the new certificate [default] CA	tate with the serial	1 SHA 1	ions Apply subj	¢ ect Apply all

### Fill out the subject fields

	X Certificate ar	nd Key management	
ate x509 Certificate			(a) Pressant pres
Sou	rce Subject Extensions	Key usage Netscape	Advanced
Distinguished name			
Internal name	s3c3_root	organizationName	S3C3 Demo
countryName	US	organizationalUnitName	
stateOrProvinceName	Washington	commonName	S3C3 Master
localityName	Lacey	emailAddress	s3c3@example.com
Туре		Content	Add Delete
Private key sc3c_root (RSA)		🗘 🗌 Used key	vs too Generate a new key
			Cancel

#### In extensions, make sure it is marked as type "Certification Authority" and "Critical" and "Subject Key Identifier" checked - set lifetime to 10 years

						A County
	Source	Subject	Extensions	Key usage	Netscape	Advanced
Basic constraint	s					Key identifier
Туре	Certification	Authority		÷	)	Subject Key Identifier
Path length					Critical	Authority Key Identifier
ubject alterna	tive name					Edit
ubject alterna ssuer alternati	tive name ve name					Edit
subject alterna ssuer alternati CRL distributio	tive name ive name n point					Edit Edit Edit

# Make sure Certificate Sign and CRL Sign are selected under Key usage and click OK

		:	X Certificate an	id Key manage	ment	
Create x509 Certificate						() (PERMIN') ()
	Source	Subject	Extensions	Key usage	Netscape Advan	iced
Key usage				Extended	key usage	
Critical				Critica	al	
Digital Signature Non Repudiation Key Encipherment Data Encipherment Key Agreement Certificate Sign CRL Sign Encipher Only Decipher Only				TLS Web TLS Web Code Sig E-mail P Time Sta Microsof Microsof Microsof Netscape Microsof IPSec End IPSec Tui IPSec Use IP securit Microsof OCSP Sig EAP over EAP over	Server Authentication Client Authentication gning rotection imping ft Individual Code Signi ft Commercial Code Signi ft Commercial Code Signi ft Trust List Signing ft Server Gated Crypto ft Encrypted File System e Server Gated Crypto ft EFS File Recovery d System nnel er ty end entity ft Smartcardlogin gning r PPP r Lan	ng Ining
						Cancel OK

#### You should have a new CA Certificate now

0	0			S X C	Certificate a	nd Key mana	agem	ent
	Privat	te Keys	Ce	ertificate signing	requests	Certificate	es	Templates Revocation lists
F	Internal	name s3c3_ro	▲ ot	commonName S3C3 Master	CA Ves	Serial I 01 20	Expi )23	New Certificate
					k			Export
								Import
								Show Details
								Delete
								Import PKCS#12
								Import PKCS#7
								Plain View
					_			Zarmineeta Divistore 7 ina
Datab	ase:/Us	sers/sjan	/s3c	3.xdb				1

# **Create a new client certificate - start with a new Certificate signing request**

000	🖉 X Certificate ar	nd Key managen	nent
Private Keys	Certificate signing requests	Certificates	Templates Revocation lists
Internal name 🔺	commonName Signed		New Request
			Export
			Import
			Show Details
			Delete
			Faunineeta Dingono Tina
Database:/Users/sjar	n/s3c3.xdb		10

#### Set the template to HTTPS\_client and click Apply extensions

	X Certific	ate and Key management	
te Certificate signing	request		(a) 200 mark
	ource Subject Extens	ions Key usage Netscape Advan	ced
Signing request			
unstructuredName	server1_client		
challengePassword			
Signing			
• Create a self sig	ned certificate with the seria	ıl 1	
O Use this Certification	ate for signing	s3c3_root	Å V
ignature algorithm		SHA 1	\$
Template for the new ce	rtificate		
[default] HTTPS_cli	ent		\$
		Apply extensions Apply sub	ject Apply all
			Cancel OI

#### Fill out the subject and click on Generate a new key

te Certificate signing re-	quest	X Certificate an	d Key management	(a) Prestande	
So	urce Subject	Extensions	Key usage Netscape	Advanced	
Distinguished name					
Internal name	server1_client		organizationName	S3C3 Demo	
countryName	US		organizationalUnitName		
stateOrProvinceName	Washington		commonName	Server 1	
localityName	Lacey		emailAddress	s3c3@example.com	
Туре			Content	Add Delete	
Private key			🗘 🗌 Used key	rs too Generate a new key	
				Cancel	

# Set the name of the server (server1 in this example) and add \_client to the name - use a 2048 bit key or larger

S	ource Subject	Extensions	Key usage	Netscape	Advanced		
Distinguished name							
Internal name	server1_client		organizationNa	ame	S3C3 Demo		
countryName		X Certificate and Key management					
stateOrProvinceNam localityName Type	Please give a keysize Key propertie Name Keytype	a name to the r es server1_clien RSA	iew key and sele t	ct the desi	red ‡	le.com Add Delete	
Private key	Keysize	2048 bit		Cancel	Create		

# Make sure to also select Non Repudiation in the Key usage pane and click OK

reate Certificate signing request          Source       Subject       Extensions       Key usage       Advanced         Key usage       Critical       Critical       Critical         Digital Signature       Critical       TLS Web Server Authentication         Non Repudiation       Key Agreement       Critical         Cartificate Sign       E-mail Protection       Tuse Starping         Microsoft Individual Code Signing       Microsoft Color Signing       Microsoft Color Signing         Decipher Only       Microsoft Encrypted File System       Netscape Server Gated Crypto         Microsoft Signing       PSec Tunnel       PSec Tunnel         PSec User       IP Security end entity       Microsoft Smartcardlogin         OCSP Signing       EAP over Lan       EAP over Lan			)	( Certificate ar	id Key manage	ement		
Source       Subject       Extensions       Key usage       Advanced         Key usage       Critical       Critical       Critical         Digital Signature       TLS Web Server Authentication       TLS Web Client Authentication         Non Repudiation       Key Agreement       Code Signing         Data Encipherment       Extended key usage       E-mail Protection         CRL Sign       Encipher Only       Microsoft Individual Code Signing         Decipher Only       Microsoft Server Gated Crypto       Microsoft Ers File Recovery         IPSec End System       IPSec User       IPSec User         IPSec User       IP Security end entity       Microsoft Smartcardlogin         OCSP Signing       EAP over PPP       EAP over PPP         EAP over Lan       EAP over Lan       EAP over Lan	eate Certificate signin	g request						(a) Provinste Trucken <sup>o</sup> 7/10
Key usage       Extended key usage         Critical       Critical         Digital Signature       TLS Web Server Authentication         Non Repudiation       Code Signing         Key Agreement       Code Signing         Certificate Sign       Microsoft Individual Code Signing         Microsoft Individual Code Signing       Microsoft Trust List Signing         Microsoft Trust List Signing       Microsoft Trust List Signing         Decipher Only       Microsoft Encrypted File System         Netscape Server Gated Crypto       Microsoft EFS File Recovery         IPSec End System       IPSec User         IP Sec User       IP Security end entity         Microsoft Server PPP       EAP over PPP		Source	Subject	Extensions	Key usage	Netscape	Advanced	1
Critical         Digital Signature         Non Repudiation         Key Encipherment         Data Encipherment         Certificate Sign         CRL Sign         Encipher Only         Decipher Only         Decipher Only         Microsoft Encrypted File System         Netscape Server Gated Crypto         Microsoft ESF File Recovery         IPSec End System         IPSec User         IP Security end entity         Microsoft Smartcardlogin         OCSP Signing         EAP over PPP         EAP over Lan	Key usage				Extended	key usage		
Digital Signature Non Repudiation Key EnciphermentTLS Web Server Authentication TLS Web Client Authentication 	Critical				Critical			
	Digital Signature Non Repudiation Key Encipherment Data Encipherment Certificate Sign CRL Sign Encipher Only Decipher Only				TLS Web TLS Web Code Sig E-mail P Time Sta Microsof Microsof Microsof Netscap Microsof IPSec En IPSec Tu IPSec Us IP securi Microsof OCSP Sig EAP over	o Server Auther o Client Authen gning Protection amping ft Individual Co ft Commercial ft Trust List Sig ft Server Gated ft Encrypted Fil e Server Gated ft EFS File Reco d System innel er ity end entity ft Smartcardlog gning r PPP r Lan	ntication ntication code Signing Code Signing l Crypto le System Crypto overy gin	g

### In the Certificates pane, click on New Certificate

0	0		S∕ x c	ertificate an	d Key managen	nent
	Private Keys	C	ertificate signing	requests	Certificates	Templates Revocation lists
F	Internal name	▲ root	commonName S3C3 Master	CA Ves	Serial Expi 01 2023	New Certificate
						Export
						Import
						Show Details
						Delete
						Import PKCS#12
						Import PKCS#7
						Plain View
						Zasemineata Dadiuseno6 Jim
Datab	ase:/Users/sja	an/s3o	:3.xdb			

#### Check Sign this request, uncheck copy extensions, make sure to check "Use this Certificate for signing" and use your root, select HTTPS\_client in templates and click Apply all

X Certificate a	nd Key management
Create x509 Certificate Source Extensions Ke	y usage Netscape Advanced
Signing request	
Sign this Certificate signing request	server1_client
Copy extensions from the request	Show request
Modify subject of the request	
Signing	
O Create a self signed certificate with the serial	
• Use this Certificate for signing	\$\$c3_root
Signature algorithm	SHA 1 \$
Template for the new certificate	
[default] HTTPS_client	\$
	Apply extensions Apply subject Apply all
	Cancel OK

#### Make sure Non Repudiation is also selected and click on OK

	X Certifica	cate and Key management
Create x509 Certificate		Contraction of the second seco
	Source Extensions	Key usage Netscape Advanced
Key usage		Extended key usage
Critical		Critical
Digital Signature Non Repudiation Key Encipherment Data Encipherment Certificate Sign CRL Sign Encipher Only Decipher Only		TLS Web Server AuthenticationTLS Web Client AuthenticationCode SigningE-mail ProtectionTime StampingMicrosoft Individual Code SigningMicrosoft Commercial Code SigningMicrosoft Trust List SigningMicrosoft Server Gated CryptoMicrosoft Encrypted File SystemNetscape Server Gated CryptoMicrosoft EFS File RecoveryIPSec End SystemIPSec TunnelIPSec UserIP security end entityMicrosoft SmartcardloginOCSP SigningEAP over PPPEAP over Lan
		Cancel OK

# Generating a server certificate is the same as a client, except you will use the HTTPS\_server template

Note that you WILL need to choose "Use this Certificate for signing" and select your root key. I forgot to while building the screenshots and had to rebuild this certificate.

	Source Su	bject Extension	s Key usage Ne	tscape Advanced	
Signing request					
unstructuredName	server1				
challengePassword					
Cianina					
O Use this Certification	ate for signii	ng	s3c3_root		÷
Use this Certification	ate for signii	ng	s3c3_root		÷
Use this Certification Use this Certification Use this Certification I use the set of the new certification of the new ce	ate for signin	ng	s3c3_root		¢)
Use this Certification Use this Certification Use this Certification Use the second se	ate for signin ertificate erver	ng	s3c3_root		¢

### X Certificate and Key management

00	🕜 X Certificate a	and Key managen	nent
Private Keys Certifica	te signing requests	Certificates	Templates Revocation lists
Internal name	commonName S3C3 Master	CA Serial Yes 01	New Certificate
server1	Server 1 Server N	o 03	Export
server1_client	Server 1 N	0 02	Import
			Show Details
			Delete
			Import PKCS#12
			Import PKCS#7
			Plain View
			Zaumineeta Dinstono Jima
Database:/Users/sjan/s3c3.xdb			1.

### Export the keys for server 1, the private server key ...

0 0		S X Cert	ificate a	and Key manage	ment
Private Keys	Certificate	signing re	quests	Certificates	Templates Revocation lists
Internal name Cesso sc3c_root	▲ Type RSA	Size 4096 bit	Use 1	Password Common	New Key
server1	RSA	2048 bit 2048 bit	2	Common	Export
Server1_cile	III KJA	2010 24	-	Common	Import
					Import PFX (PKCS#12)
					Show Details
					Delete
atabase:/Users/sjan/	s3c3.xdb				

# ... which should be named servername.pem (server1.pem for our example server1)

000	♂ X Certificate and Key management	
Private	X Certificate and Key management	1 lists
Internal C sc3 C sen	Key export	
Ser Ser	Please enter the filename for the key. Filename /Users/sjan/keyexport/server1.pem	#12)
	DER is a binary format of the key without encryption PEM is a base64 encoded key with optional encryption PKCS#8 is an encrypted official Key-exchange format Export Format PEM ‡	
	When exporting the private key it should be encrypted.  Export the private part of the Key too  Export as PKCS#8  Encrypt the Key with a password	
Database:/User:	Cancel OK s/sjan/s3c3.xdb	

# Export the client private key (servername\_client.pem - or server1\_client.pem for our example server1)

000	♂ X Certificate and Key management	
Private	X Certificate and Key management	1 lists
Internal C sc3 C sen	Key export	
ser ser	Please enter the filename for the key. Filename /Users/sjan/keyexport/server1_client.pem	#12)
	DER is a binary format of the key without encryption PEM is a base64 encoded key with optional encryption PKCS#8 is an encrypted official Key-exchange format Export Format PEM \$	
	When exporting the private key it should be encrypted. Export the private part of the Key too Export as PKCS#8 Encrypt the Key with a password	
Database:/User	Cancel OK	

# Export the certificates - same naming scheme as the keys, but with the crt extension

000	🔗 X Certificate ar	nd Key managen	nent	
Private	Keys Certificate signing requests	Certificates	Templates Revocat	ion lists
Inter	X Certificate and	Key manageme	unt	
▼ , 🦛 -	X Certificate and	r key manageme	int	e
	Certifikate export			
	Please enter the filename for the ce	ertificate.		
	Filename /Users/sjan/keyexport/	server1.crt		
	DER is a binary format of the Certif PEM is a base64 encoded Certificat PKCS#7 is an official Certificate exc PKCS#12 is an encrypted official Ke	ficate e change format ey-Certificate ex	change format	7
	Export Format PEM		\$	
			Cancel OK	Time
Database:/Use	rs/sjan/s3c3.xdb			

#### ... client certificate the same

000	🖉 X Certificate and Key management
Private	Keys Certificate signing requests Certificates Templates Revocation lists
Inter	X Certificate and Key management e
A: A:	Certifikate export
	Please enter the filename for the certificate.         Filename       /Users/sjan/keyexport/server1_client.crt
	DER is a binary format of the Certificate       12         PEM is a base64 encoded Certificate       7         PKCS#7 is an official Certificate exchange format       7         PKCS#12 is an encrypted official Key-Certificate exchange format       12
	Export Format PEM +
	Cancel OK
Database:/Use	rs/sjan/s3c3.xdb

### And don't forget the root CA certificate

000	✓ X Certificate and Key management
Private	Keys Certificate signing requests Certificates Templates Revocation lists
Inter	X Certificate and Key management
A	Certifikate export
	Please enter the filename for the certificate.         Filename       /Users/sjan/keyexport/s3c3_root.crt
	DER is a binary format of the Certificate PEM is a base64 encoded Certificate PKCS#7 is an official Certificate exchange format PKCS#12 is an encrypted official Key-Certificate exchange format
	Export Format PEM +
	Cancel OK
Database:/User	rs/sjan/s3c3.xdb