**Title**
Working with certificates

**Article Type**
Configuration

**Author**
Dominik Rappaport (/AristaCommunity/s/profile/0050G00000CgxbPQAR)

**Language**
English

**Published Date**
March 28, 2019

**Updated Date**
March 28, 2019

## Table of Contents

## Content

# Working with certificates

## Introduction and motivation

Encryption protocols like HTTPS use certificates to authenticate the remote server (sometimes also the client) as there are no other means to verify to which device you are currently talking. If the server (in our case the switch providing management access via an HTTP based REST API) is located in our own network, it is usually acceptable to work with so-called self-signed certificates. A self-signed certificate is not signed by a certification authority (CA), which would confirm that the CA (an institution you trust) has verified the identity of the certificate holder. By default, Arista EOS based devices use a self-signed certificate for all HTTPS based connections.

In some environments that approach causes problems. On one hand, many browsers or other tools verify the certificate’s chain of trust by default and require either manual intervention to continue or, stop progressing the script. Compliance standards or other regulation may also require that all certificates must be issued by a CA.
This article shows how to manage certificates on EOS devices using the command line interface (CLI) and presents the open source desktop CA XCA.

## Certificate management on an Arista switch

To work with a certificate, the following steps are required:

1. A pair of two keys (called public and private key) is generated using a public-key cryptosystem. EOS supports the RSA (Rivest-Shamir-Adleman) algorithm with key lengths of 2,048, 3,072, or 4,096 bit.
2. A certificate signing request (CSR) is issued specifying properties like the common name (CN) and the subject alternative name (SAN), which usually includes the DNS name and/or an IP address. The SAN must match the host part of the URL you use to access the device.
3. The CSR must be submitted to the CA. In return, you get a certificate back, which must be installed on the device.

4. The CA’s root certificate as well as intermediate certificates (if applicable) must be imported as well.

After these steps, the certificate is ready to use and can be referenced in an SSL profile.

## Step 1: Generate the key pair:

```
switch01#security pki key generate rsa 2048 switch01.key
```

The key file is saved in:

```
/persist/secure/ssl/keys/switch01.key
```

## Step 2: Generate the certificate signing request:

```
switch01#security pki certificate generate signing-request key switch01.key
Common Name for use in subject: Switch01
Two-Letter Country Code for use in subject: US
State for use in subject: CA
Locality Name for use in subject: Santa Clara
Organization Name for use in subject: Arista
Organization Unit Name for use in subject: Lab
Email address for use in subject:
IP addresses (space separated) for use in subject-alternative-name: 192.168.
DNS names (space separated) for use in subject-alternative-name: switch01.ar
Email addresses (space separated) for use in subject-alternative-name:
-----BEGIN CERTIFICATE REQUEST-----
MIIC5jCCAc4CAQAwYjELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMRQwEgYDVQQH
DAtTYW50YSBDbGFyYTEPMA0GA1UECgwGQXJpc3RhMQwwCgYDVQQLDANMYWIxETAP
BgNVBAMMCFN3aXRjaDAxMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
0/EPy/2gMsWgm8r+HTO6lxPb6NklPBwAfU/IaFfHri4uz1WM5ofMASoaw5uBg/sB
2chTy4UNodFY9D49tDg6FE4c5xLfTsnicrevRZsw6BQGl+XIdEm72bUvWPml2Kaq
cznV5XPTak3UggUZ6FNrq5ZTfAvTRW7mmDvpJi9+JRsK156VESWsimLwni9NKxrx
gbCeaw0IoRlABEt6Iub9/imTMdwuBcfxjzMVf9FtbZpNlR7TRnImTrCTCIYaR/nK
ssjVCxYwUUFvSzDHS+PZR/NwHYFgkJL9YspkflfOfXi119MSovLxzfEtAN+/Iqa1
LjnnPeh8gLpX0tRoX4Pi1QIDAQABoD8wPQYJKoZIhvcNAQkOMTAwLjAsBgNVHREE
JTAjhwTAqAEBghtzd2l0Y2gwMS5hcmlzdGFuZXR3b3Jrcy5jb20wDQYJKoZIhvcN
AQELBQADggEBAJ/jmhs96LmybYzsk9EE1jNjn9NdO4bRnd6mcoJrIr6GCrjjU/5r
XQr6aDrBHWV5JWV0EvObjOZU7TxKB9ZPqQofAE++TFiMHo/qn1MZS4YEw2+RHWFO
RW8v6JqQ6REYKZCMjQ25flroPVSa1ly2NEUvfOizAG7gbFmHHjOf+eiS0hipvGgN
HpDoDPiweK9ph9BBXFwmk55xamTPKUKdLo0O2XCkLv85rQavRsnJoofMz9mVrrfN
FEFqrf4nhdvLEoxlUSKvKUHPvKhOAEpy4DyFn3zmofxge/0PXm1Aq4urY7DWpaNk
tT/DirbO22BjxNk620LKWU6WubEiufYeEu8=
-----END CERTIFICATE REQUEST-----
```

Note: Instead of providing all parameters interactively, they can be specified as parameters to the security pki certificate generate signing-request command.

## Step 3: We submit the CSR to the CA and get the signed certificate back

In a later section, we demonstrate how to use the desktop CA XCA to handle all certificate requests.

The signing request is encoded and enclosed between the BEGIN and END

CERTIFICATE REQUEST lines. The header and the footer lines must be included. Many CAs allow you to copy/paste these lines but you can also save them to a text file and submit this file to the CA.

Copy the certificate file from the EOS CLI to certificates:switch01.crt, for example via

```
switch01#copy file:/tmp/switch01.crt certificate:switch01.crt
```

Alternatively, the certificate could be copied directly from the clipboard via

```
switch01#copy terminal: certificate:switch01.crt
enter input line by line; when done enter one or more control-d
```

Of course, the name can be any legal designator. Do the same with the CA's root certificate. We call it ca.crt.

## Step 4: Create an SSL profile using the certificate

```
switch01#configure
switch01(config)#management security
switch01(config-mgmt-security)#ssl profile profile01
switch01(config-mgmt-sec-ssl-profile-profile01)#trust certificate ca.crt
switch01(config-mgmt-sec-ssl-profile-profile01)#certificate switch01.crt key
switch01(config-mgmt-sec-ssl-profile-profile01)#exit
```

Verify that the profile is valid using this CLI command:

```
switch01#show management security ssl profile
   Profile         State
--------------- -----------
   profile01       valid
```

Note: Our certificate was issued by the root CA. If an intermediate CA had been involved, we would have had to install the intermediate certificate as well using the command

```
chain certificate intermediate.crt
```

provided intermediate.crt is the name of the intermediate certificate's filename.

## Step 5: SSL profile management

The SSL profile allows tuning other SSL/TLS parameters. The two most popular ones are:

1. Restricting the TLS algorithm to specific versions (e.g. version 1.2 only)
2. Provide a cipher list the switch should offer to the web server for encryption

In our example, we configure the profile to allow only TLS 1.2 and the AES256 encryption algorithm, SHA384 secure hash algorithm and the Elliptic Curve Diffie-Hellmann algorithm. In the context of the SSL profile we configure:

```
switch01#configure
switch01(config)#management security
switch01(config-mgmt-security)#ssl profile profile01
switch01(config-mgmt-sec-ssl-profile-profile01)#tls versions 1.2
switch01(config-mgmt-sec-ssl-profile-profile01)#cipher-list ECDHE-RSA-AES256
```

Note: The ciphers must be separated by the colon character (:). You can use this command to display all available ciphers:

```
switch01(config-mgmt-sec-ssl-profile-profile01)#bash openssl ciphers 'HIGH:!
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-S
```

## Step 6: Activate eAPI access and refer to the previously created SSL profile

```
switch01#configure
switch01(config)#management api http-commands
switch01(config-mgmt-api-http-cmds)#protocol https ssl profile profile01
switch01(config-mgmt-api-http-cmds)#no shutdown
switch01(config-mgmt-api-http-cmds)#exit
```

Note: There are many more options and protocols you can configure with eAPI but we provide only the minimum required to enable eAPI using our SSL profile.
This final step concludes the generation of a public/private key pair, the installation of an SSL certificate, tuning SSL parameters and enabling eAPI using the previously created certificate.

# Install your own CA

The previous instructions relied on the availability of a CA. As using a commercial CA for internal management is not common, the available options boil down to using

1. An Enterprise CA like Microsoft CA
2. A desktop CA

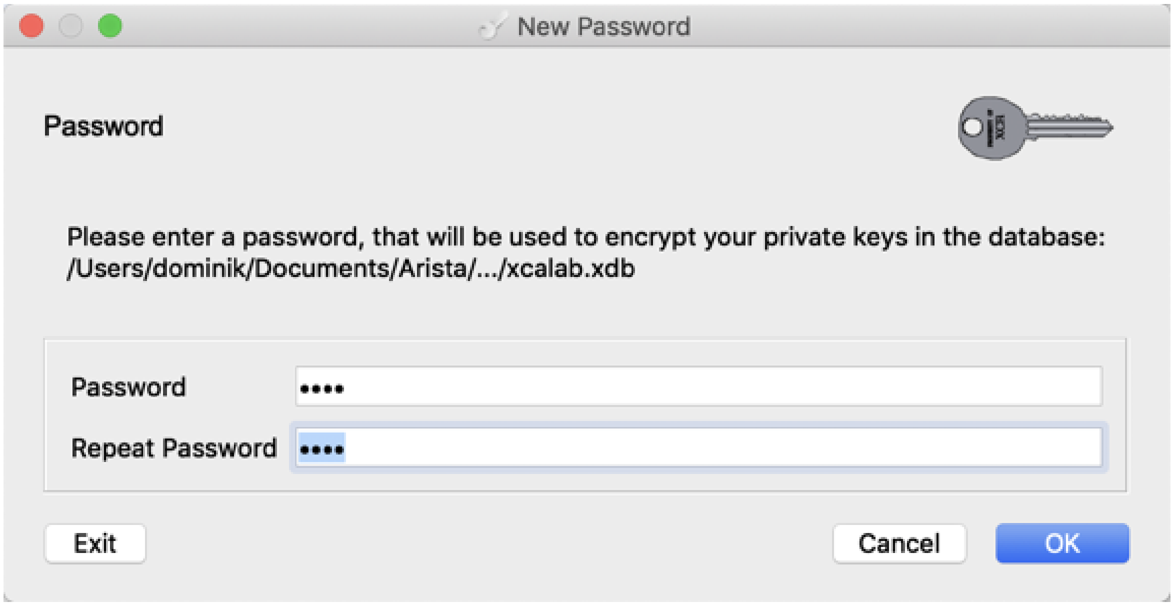
A lot of companies offer a CA as an internal service. However, fairly often the operator restricts, for example, the certificate's validity period which may be less than the projected lifetime of the devices under management. Renewing the certificates is possible of course but requires either an automation infrastructure or manual intervention. In such cases, it may be more convenient to use a CA under the network management team's control. That may also be the only option at hand if there is no Enterprise CA available.
Desktop CAs are an easy solution in such cases as they don't require a service infrastructure in place. They store all information in a file which can be put on a shared volume.
XCA is available for download at https://www.hohnstaedt.de/xca/index.php/download (https://www.hohnstaedt.de/xca/index.php/download). Builds exist for Windows and MAC.

## Step 1: Download and install XCA on your machine

Please follow the installation instructions specific to your platform.

## Step 2: Create a new database

Start XCA and choose File > New DataBase and provide the filename for your CA infrastructure. You are requested to provide a password, which is used to encrypt the file:



Password

Please enter a password, that will be used to encrypt your private keys in the database:
/Users/dominik/Documents/Arista/.../xcalab.xdb

Password ••••
Repeat Password ••••

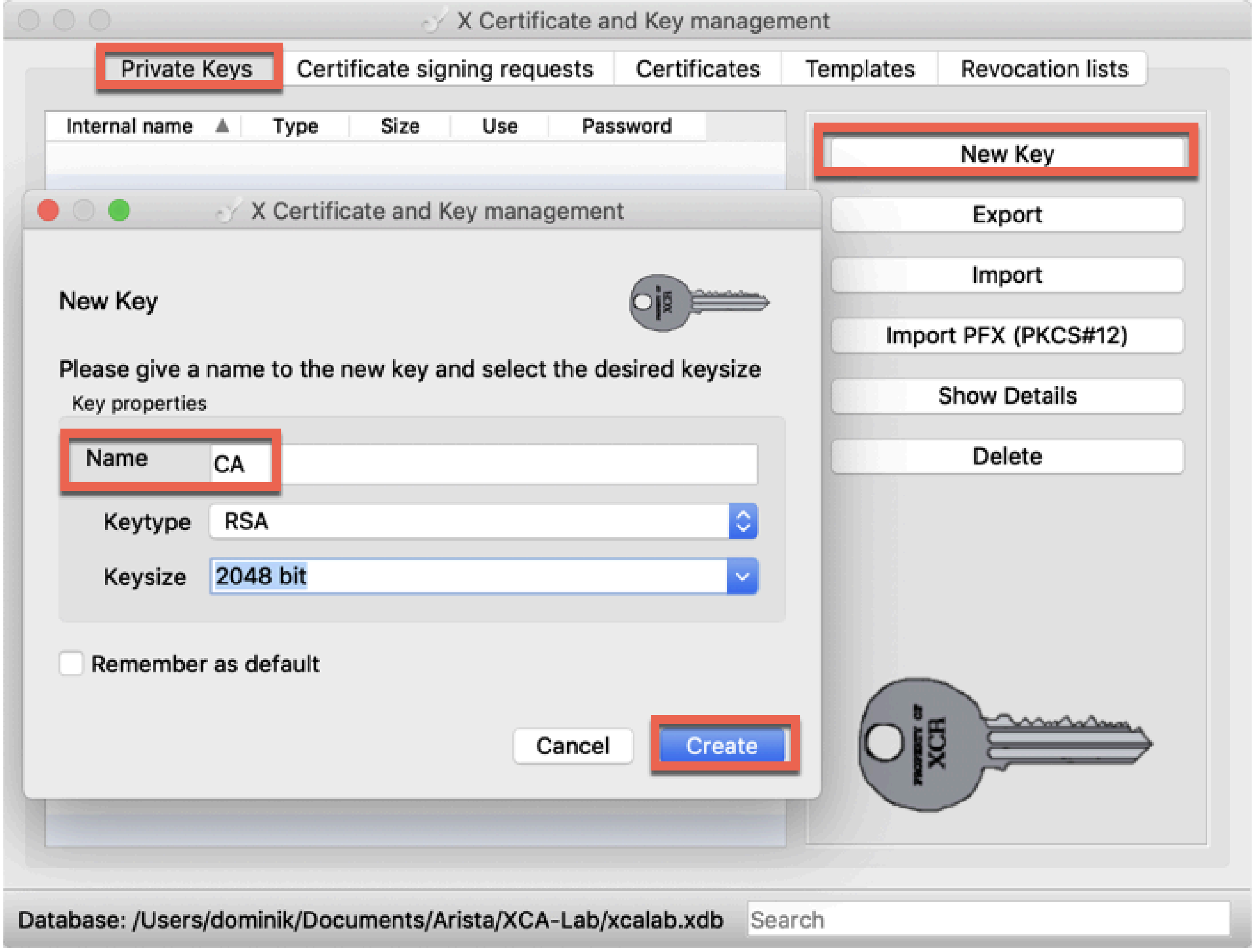
(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XD5rQAG&oid=00DA0000000H7UG)

## Step 3: Create a new CA certificate

A CA certificate features two properties:

1. It is self-signed
2. “Certificate sign” and “CRL sign” are flagged as key usages

The first step is to create a new private key:
On the “Private Keys” tab, select “New Key”. Then provide a meaningful name to identify the key later on and adjust if require the key type and key size. Confirm your selection with “Create”.



X Certificate and Key management

New Key

Please give a name to the new key and select the desired keysize

Key properties

Name: CA

Keytype: RSA

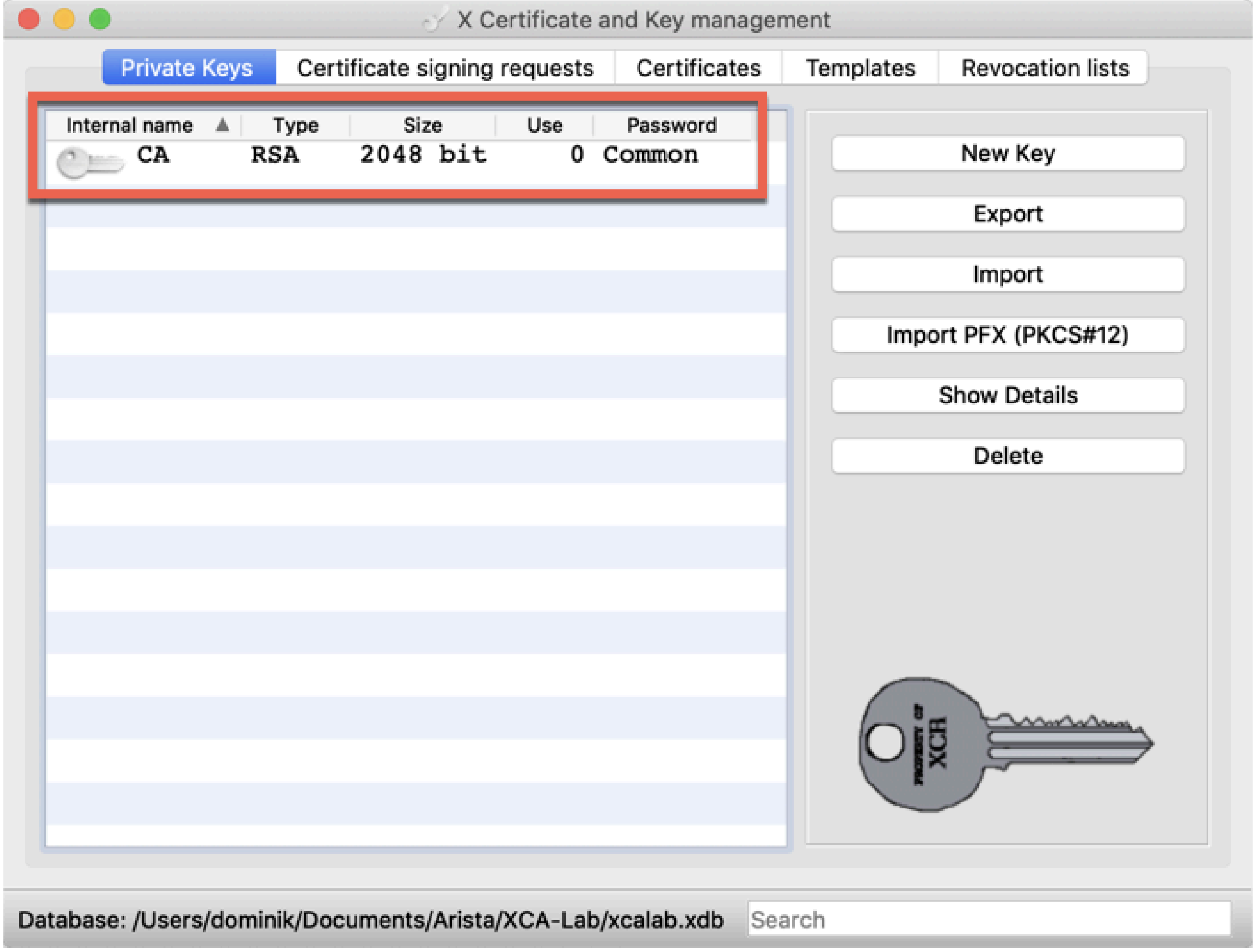
Keysize: 2048 bit

□ Remember as default

Database: /Users/dominik/Documents/Arista/XCA-Lab/xcalab.xdb

(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XDRBQA4&oid=00DA0000000H7UG)

The new key should appear on the list:



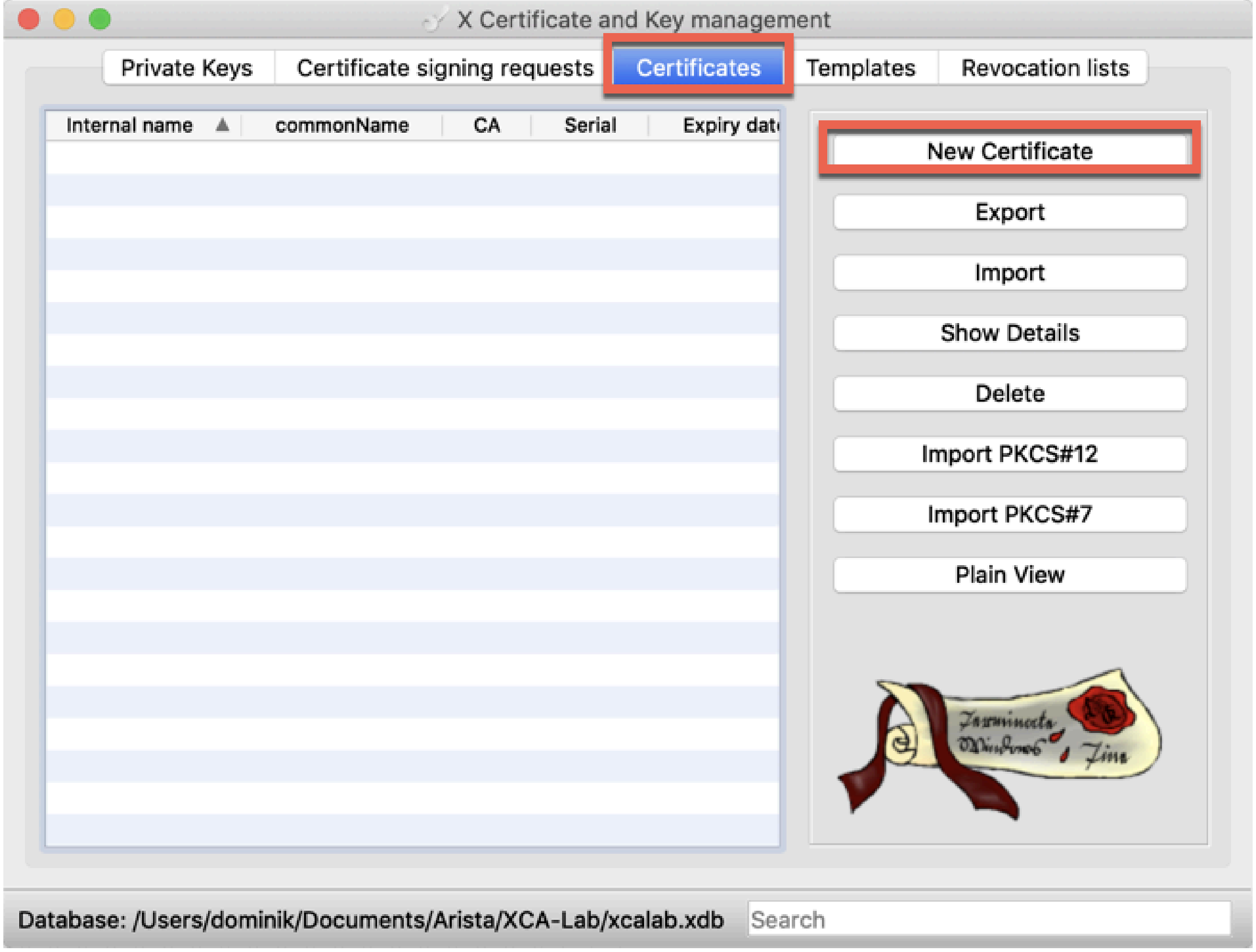
| Internal name ▲ | Type | Size | Use | Password |
|---|---|---|---|---|
| CA | RSA | 2048 bit | 0 | Common |

Database: /Users/dominik/Documents/Arista/XCA-Lab/xcalab.xdb

Search

(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XDFrQAO&oid=00DA0000000H7UG)

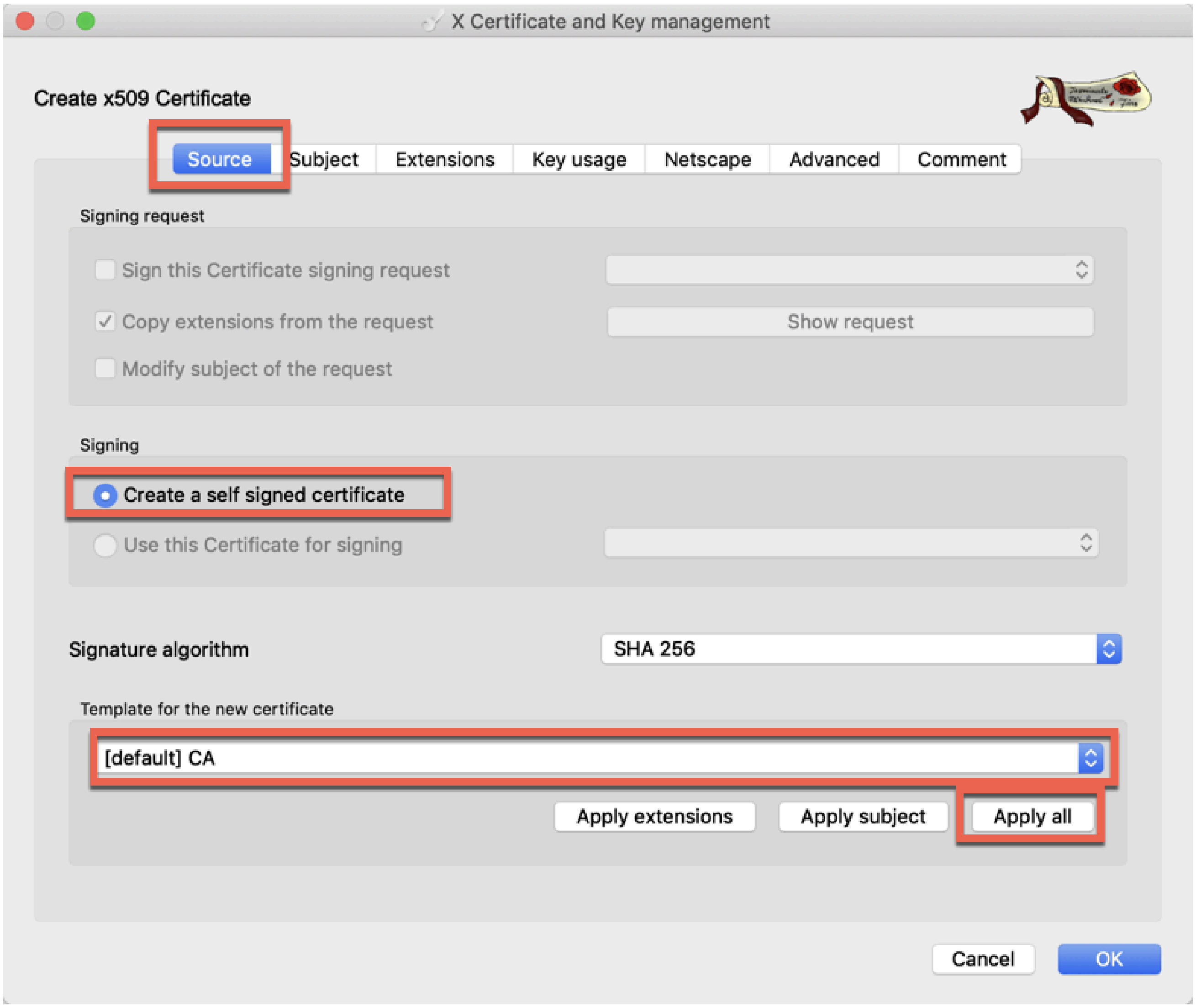
The next step is to create a certificate. On the “Certificates” tab, select “New Certificate”.



Database: /Users/dominik/Documents/Arista/XCA-Lab/xcalab.xdb

(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XDFsQAO&oid=00DA0000000H7UG)

On the first tab “Source” select “Create a self-signed certificate”, make sure “[default] CA” is selected as a template and press the “Apply all” button to apply the template’s settings to your certificate.



Create x509 Certificate

Signing request

□ Sign this Certificate signing request

☑ Copy extensions from the request

□ Modify subject of the request

Signing

● Create a self signed certificate

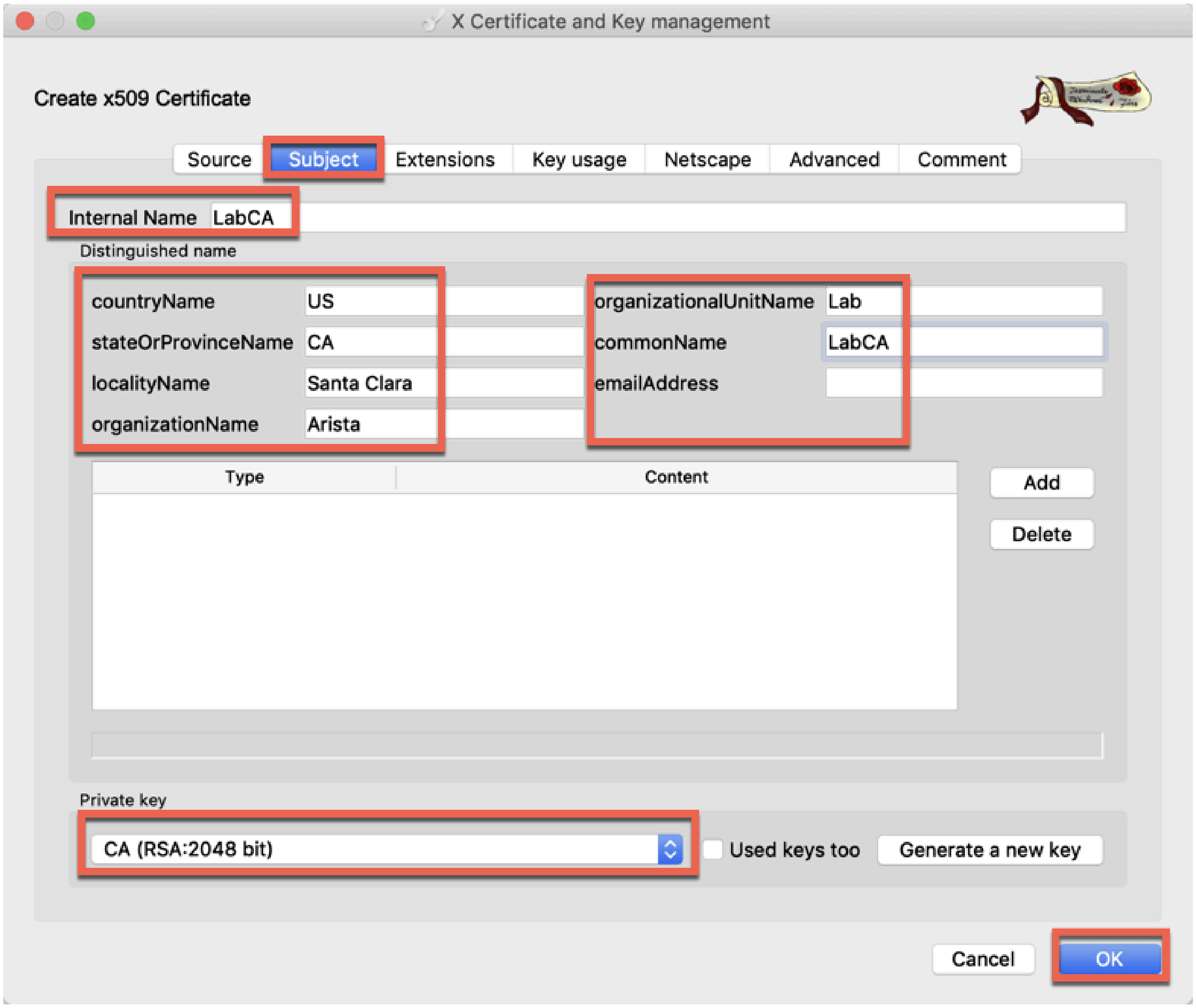
○ Use this Certificate for signing

Signature algorithm: SHA 256

Template for the new certificate: [default] CA

[(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XD5sQAG&oid=00DA0000000H7UG)](https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XD5sQAG&oid=00DA0000000H7UG)

On the “Subject” tab, provide the distinguished name properties and select the previously generated private key. As we leave all other settings to their default, we confirm with “OK”.



Internal Name LabCA

Distinguished name

countryName US

stateOrProvinceName CA

localityName Santa Clara

organizationName Arista

organizationalUnitName Lab

commonName LabCA

emailAddress

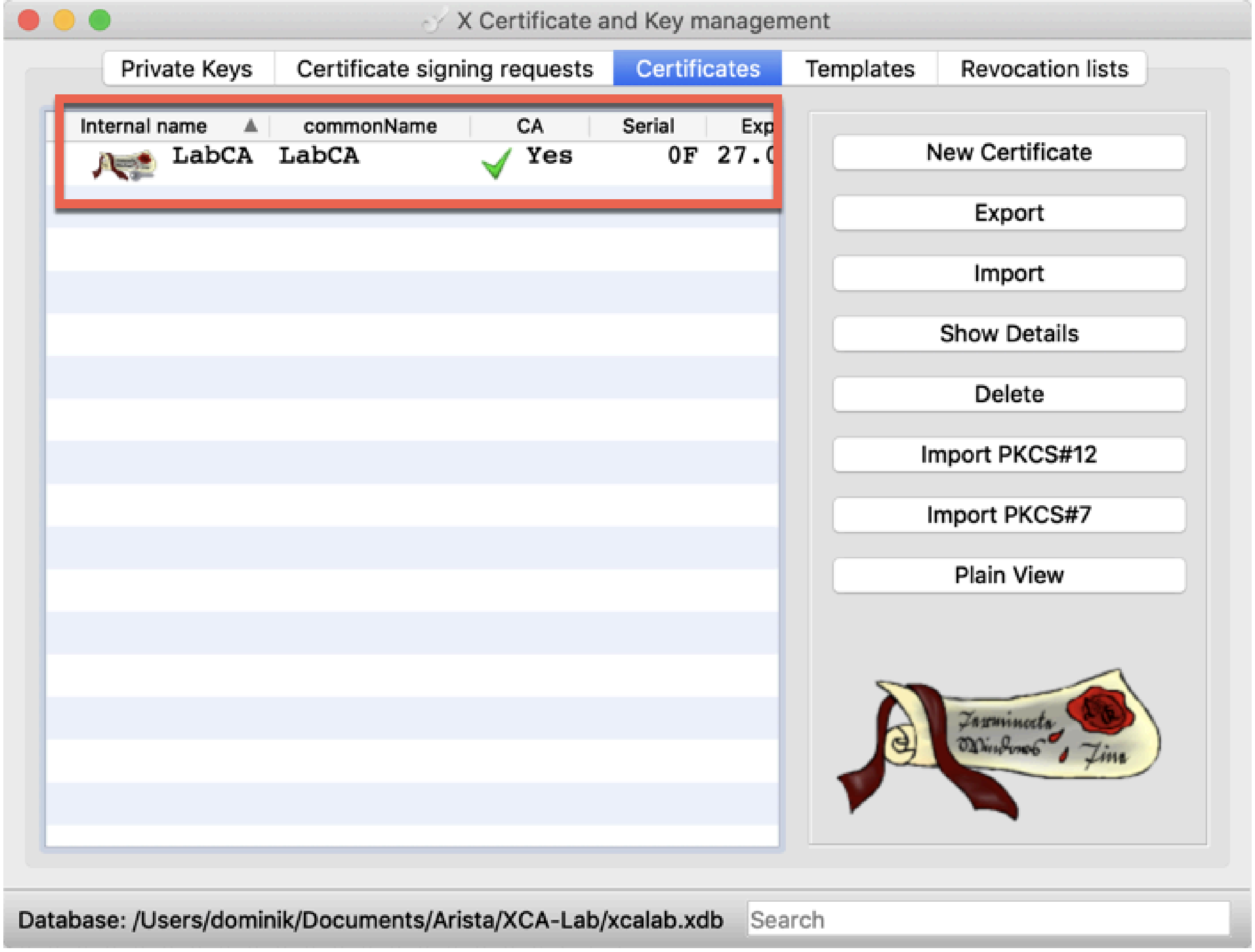
| Type | Content |
|---|---|

Private key

CA (RSA:2048 bit)

[(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XD5tQAG&oid=00DA0000000H7UG)](https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XD5tQAG&oid=00DA0000000H7UG)

The freshly generated certificate is now listed:

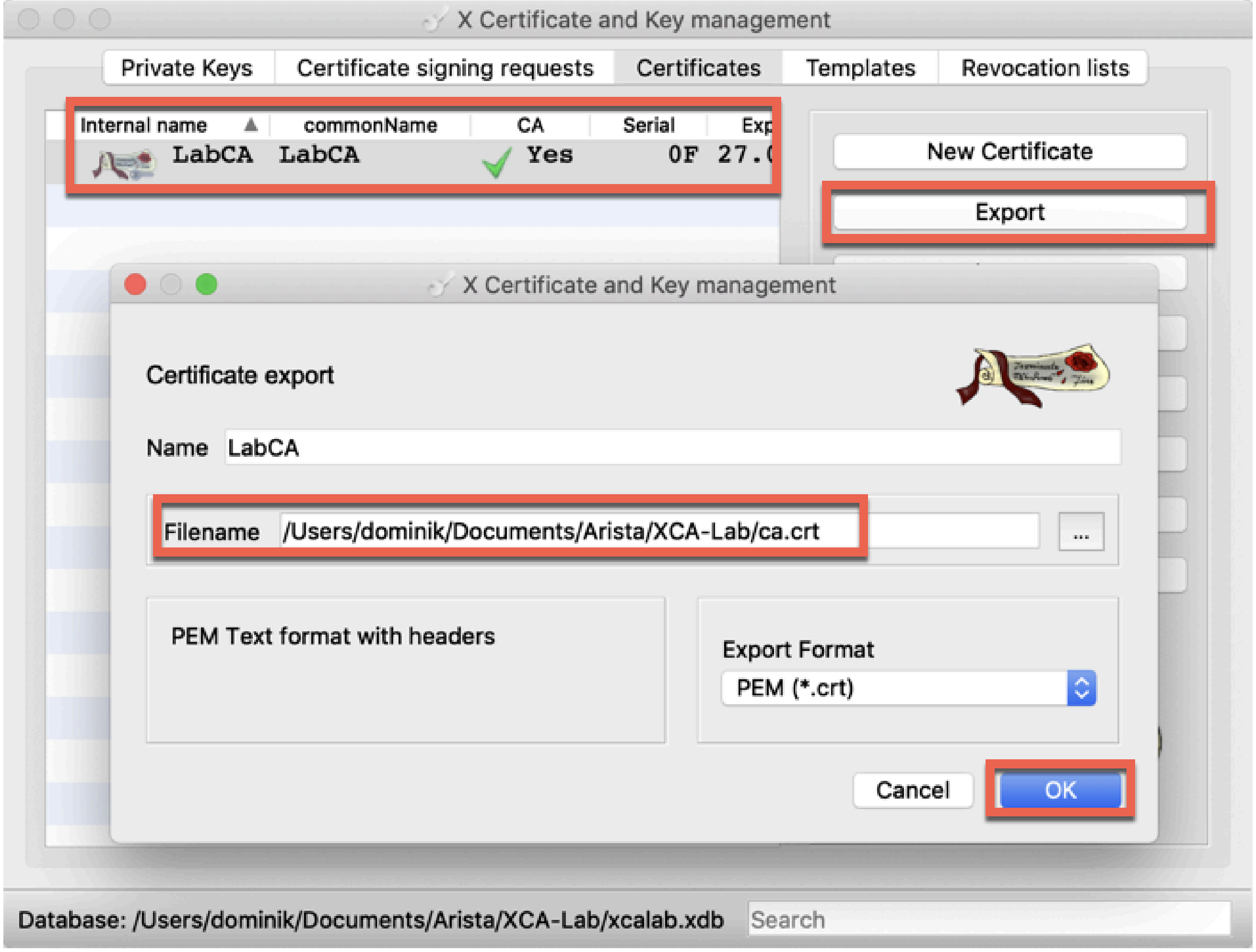


| Internal name ▲ | commonName | CA | Serial | Exp |
|---|---|---|---|---|
| LabCA | LabCA | ✓ Yes | 0F | 27.0 |

Database: /Users/dominik/Documents/Arista/XCA-Lab/xcalab.xdb

(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XDFtQAO&oid=00DA0000000H7UG)

As we have to import the root certificate on every switch, we conclude its generation by the export to file. Make sure the certificate is selected and click on “Export”. Provide a filename and confirm by clicking on the “OK” button.



| Internal name | commonName | CA | Serial | Exp |
|---|---|---|---|---|
| LabCA | LabCA | ✓ Yes | 0F | 27.( |

Certificate export

Name LabCA

Filename /Users/dominik/Documents/Arista/XCA-Lab/ca.crt

PEM Text format with headers

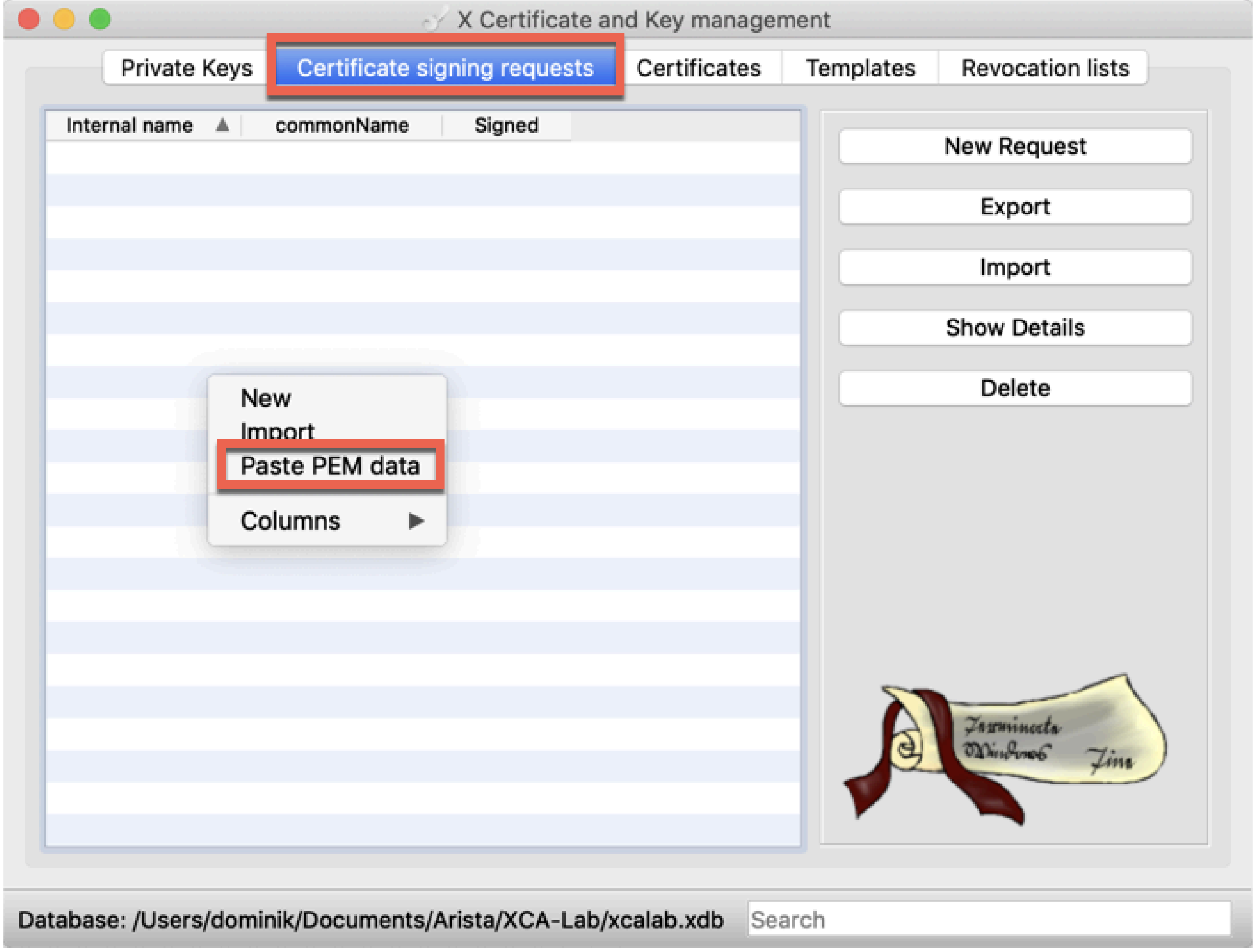
Export Format PEM (*.crt)

Database: /Users/dominik/Documents/Arista/XCA-Lab/xcalab.xdb Search

(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XDRCQA4&oid=00DA0000000H7UG)

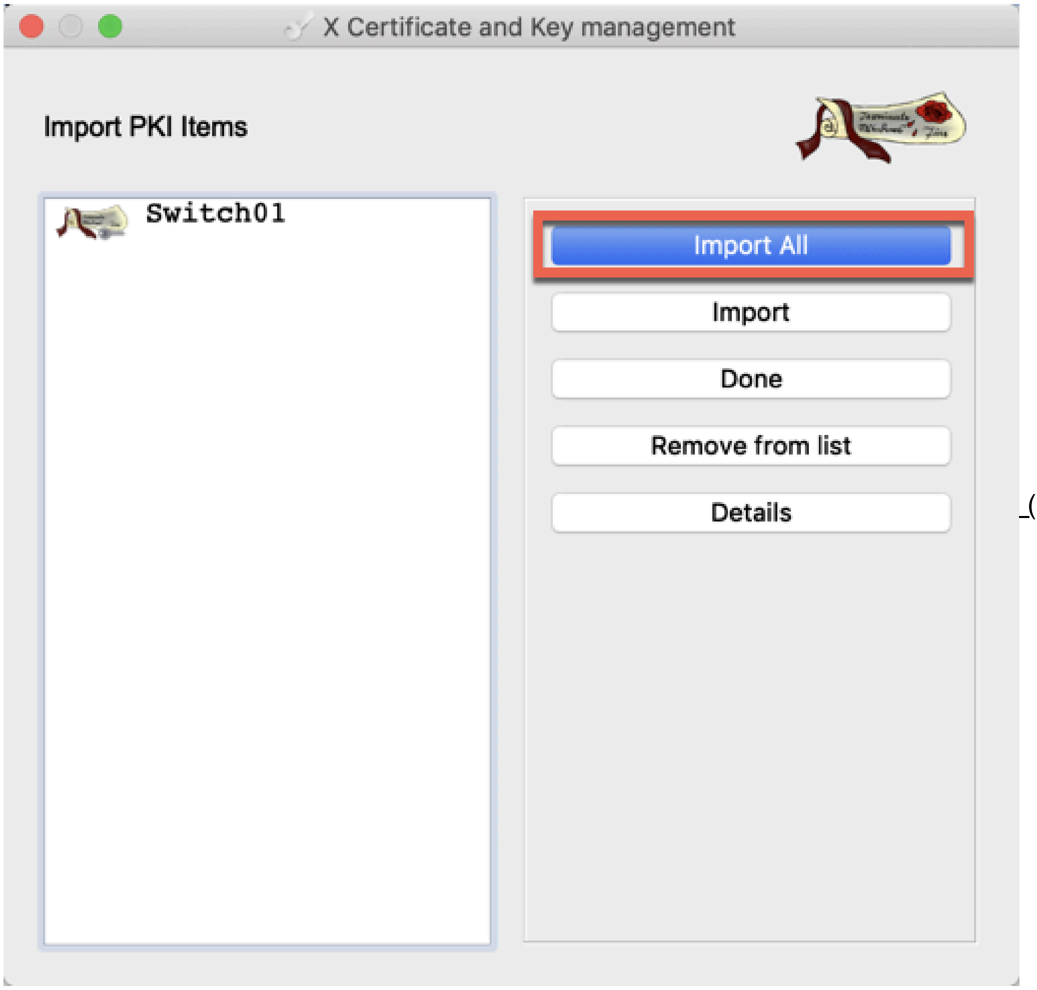
## Step 4: Import the CSR

Now we are ready to import the CSR from the switch. That easiest way is to copy the request into the clipboard. On the “Certificate signing requests” right-click on the empty space of the CSR list and select “Paste PEM data”.



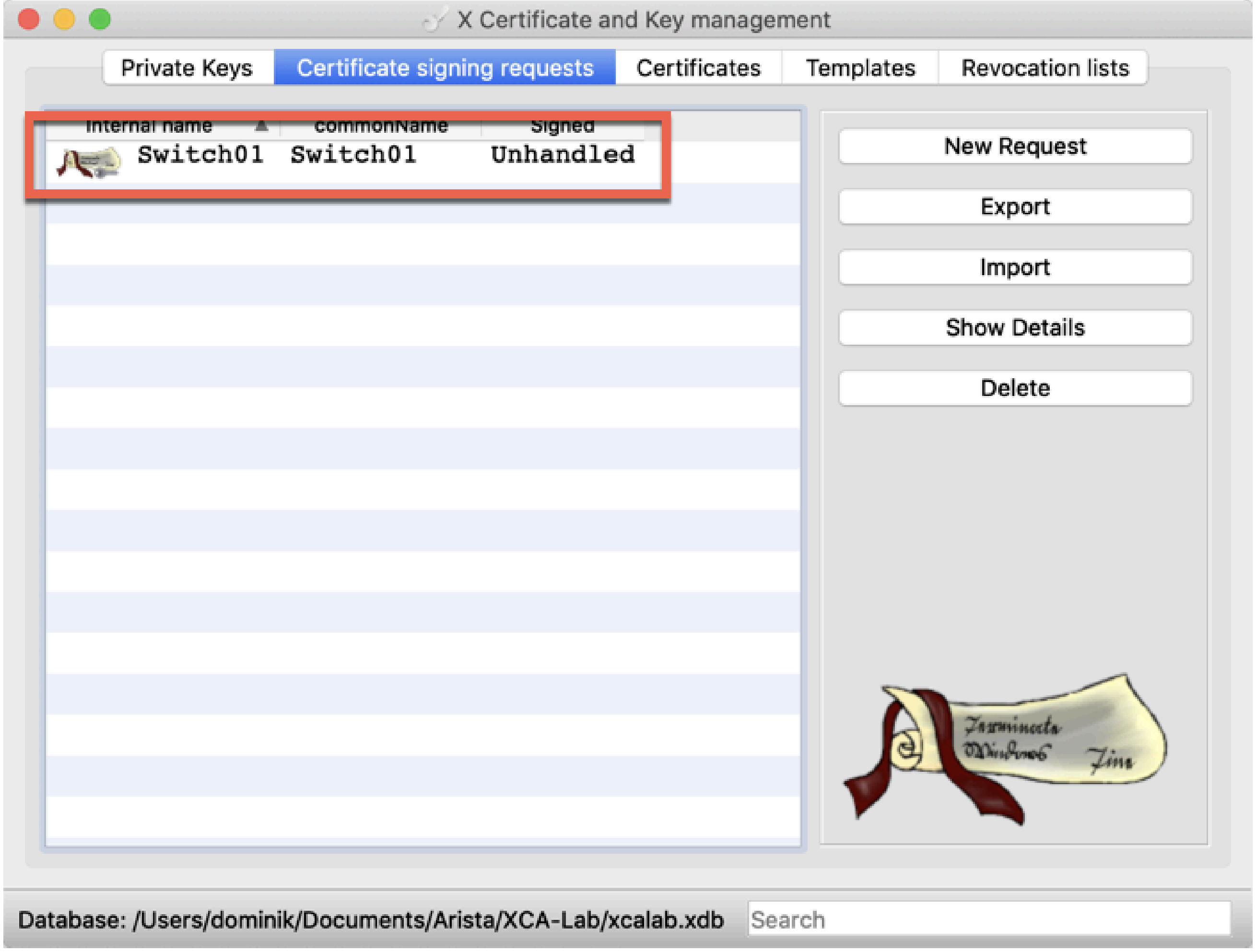
(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XDFuQAO&oid=00DA0000000H7UG)

XCA will import the CSR from the clipboard and present it to you already decoded. Click on “Import All” to proceed:



(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XD5uQAG&oid=00DA0000000H7UG)

The CSR is now listed:



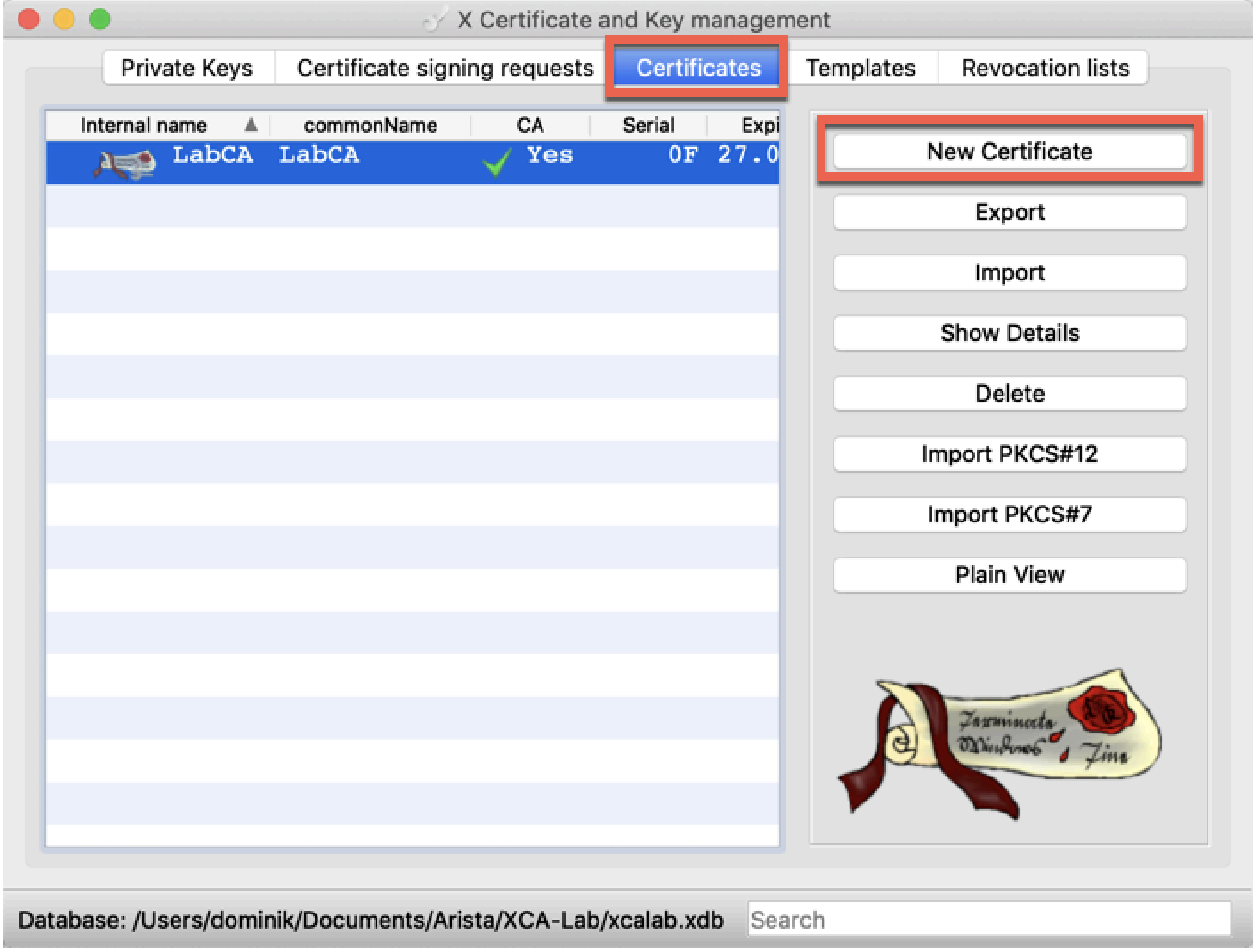
| Internal name | commonName | Signed |
|---|---|---|
| Switch01 | Switch01 | Unhandled |

Database: /Users/dominik/Documents/Arista/XCA-Lab/xcalab.xdb

(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XDRDQA4&oid=00DA0000000H7UG)

## Step 5: Issue the certificate

On the “Certificates” tab, click on “New Certificate”:

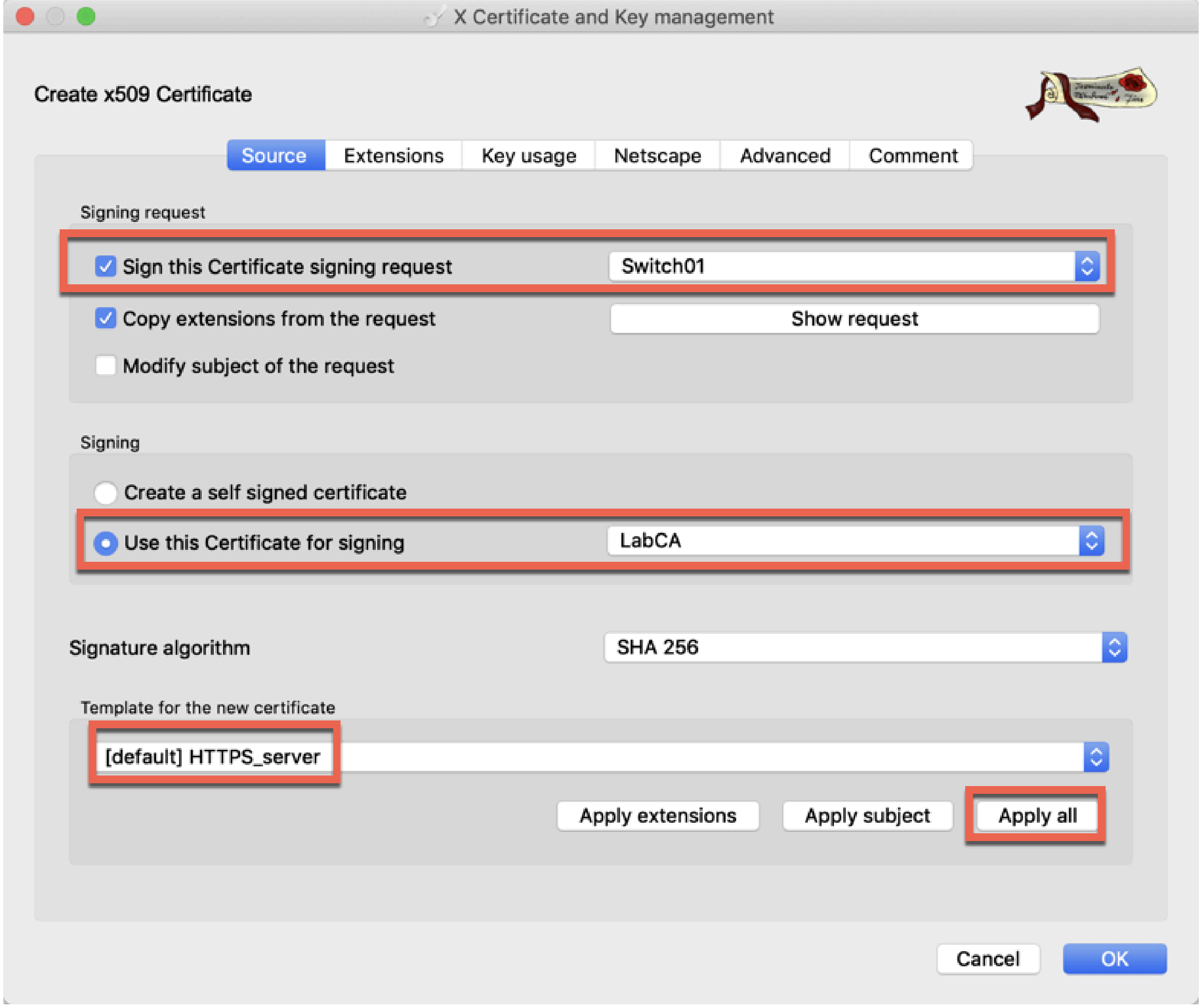


| Internal name ▲ | commonName | CA | Serial | Expi |
|---|---|---|---|---|
| LabCA | LabCA | ✓ Yes | 0F | 27.0 |

Database: /Users/dominik/Documents/Arista/XCA-Lab/xcalab.xdb

(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XDFvQAO&oid=00DA0000000H7UG)

On the “Source” tab, select the CSR, the CA’s certificate as signing certificate the “[default] HTTPS_server” as a template and click on “Apply all”.



X Certificate and Key management

Create x509 Certificate

Signing request

☑ Sign this Certificate signing request
Switch01

☑ Copy extensions from the request

□ Modify subject of the request

Signing

○ Create a self signed certificate

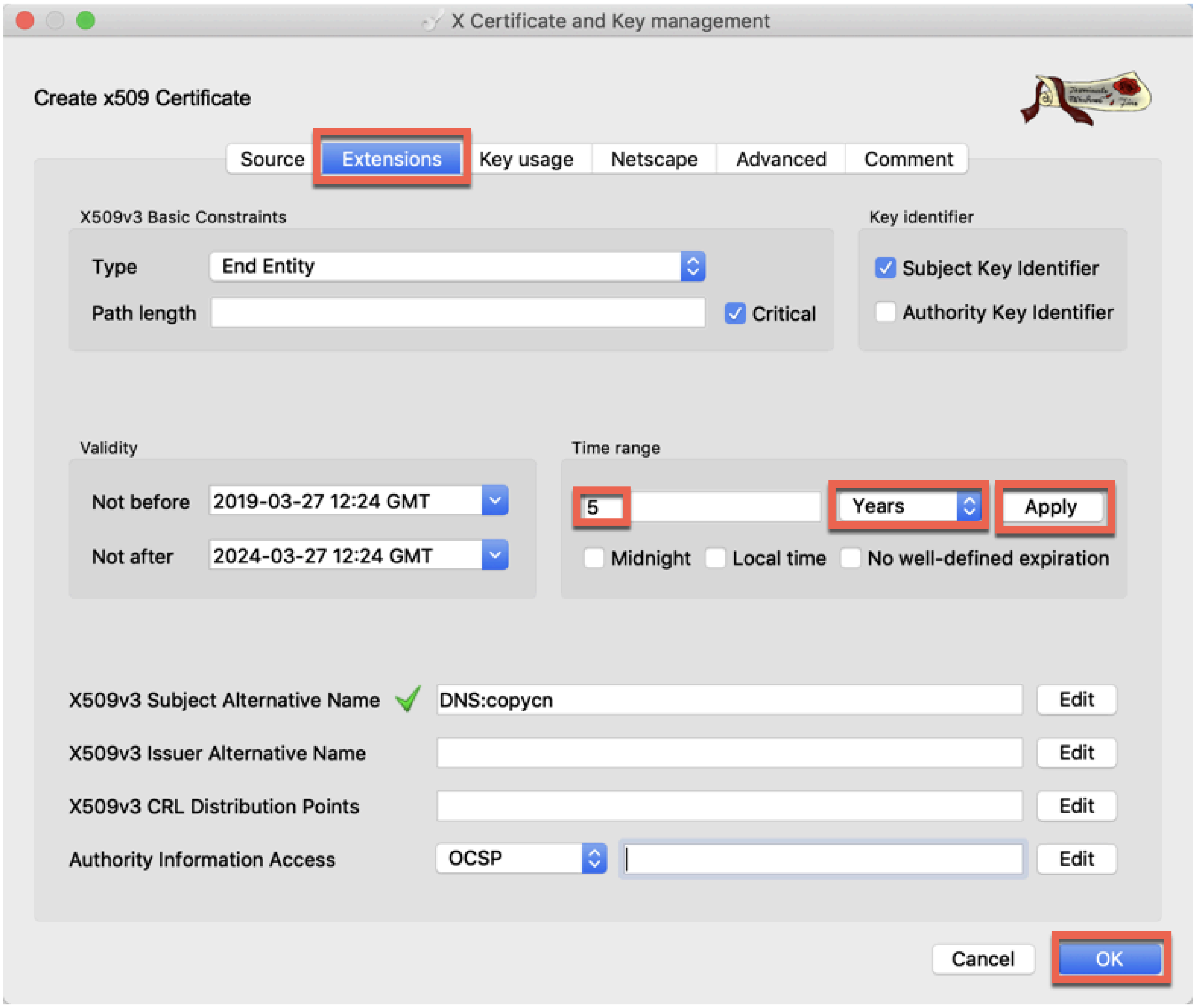
● Use this Certificate for signing
LabCA

Signature algorithm
SHA 256

Template for the new certificate
[default] HTTPS_server

(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XDREQA4&oid=00DA0000000H7UG)

On the “Extensions” tab adjust the certificate’s validity period and confirm your selection with “Apply”. Then confirm everything with “OK”.



X509v3 Basic Constraints

Type: End Entity

Path length:

☑ Critical

Key identifier

☑ Subject Key Identifier

□ Authority Key Identifier

Validity

Not before: 2019-03-27 12:24 GMT

Not after: 2024-03-27 12:24 GMT

Time range

5 Years Apply

□ Midnight □ Local time □ No well-defined expiration

X509v3 Subject Alternative Name ✓ DNS:copycn Edit

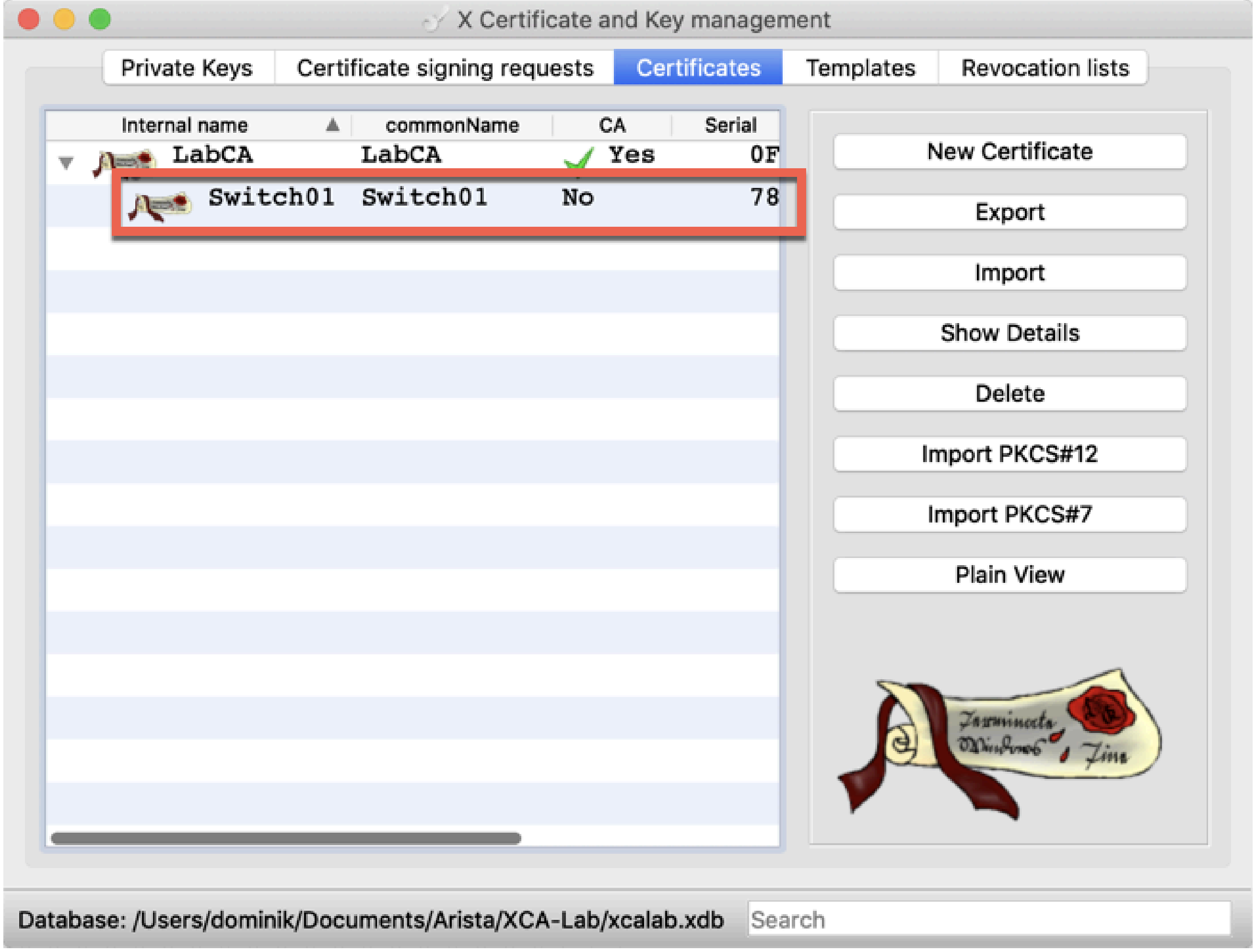
X509v3 Issuer Alternative Name Edit

X509v3 CRL Distribution Points Edit

Authority Information Access OCSP Edit

(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XDRFQA4&oid=00DA0000000H7UG)

The new certificate is now listed below the CA's certificate:

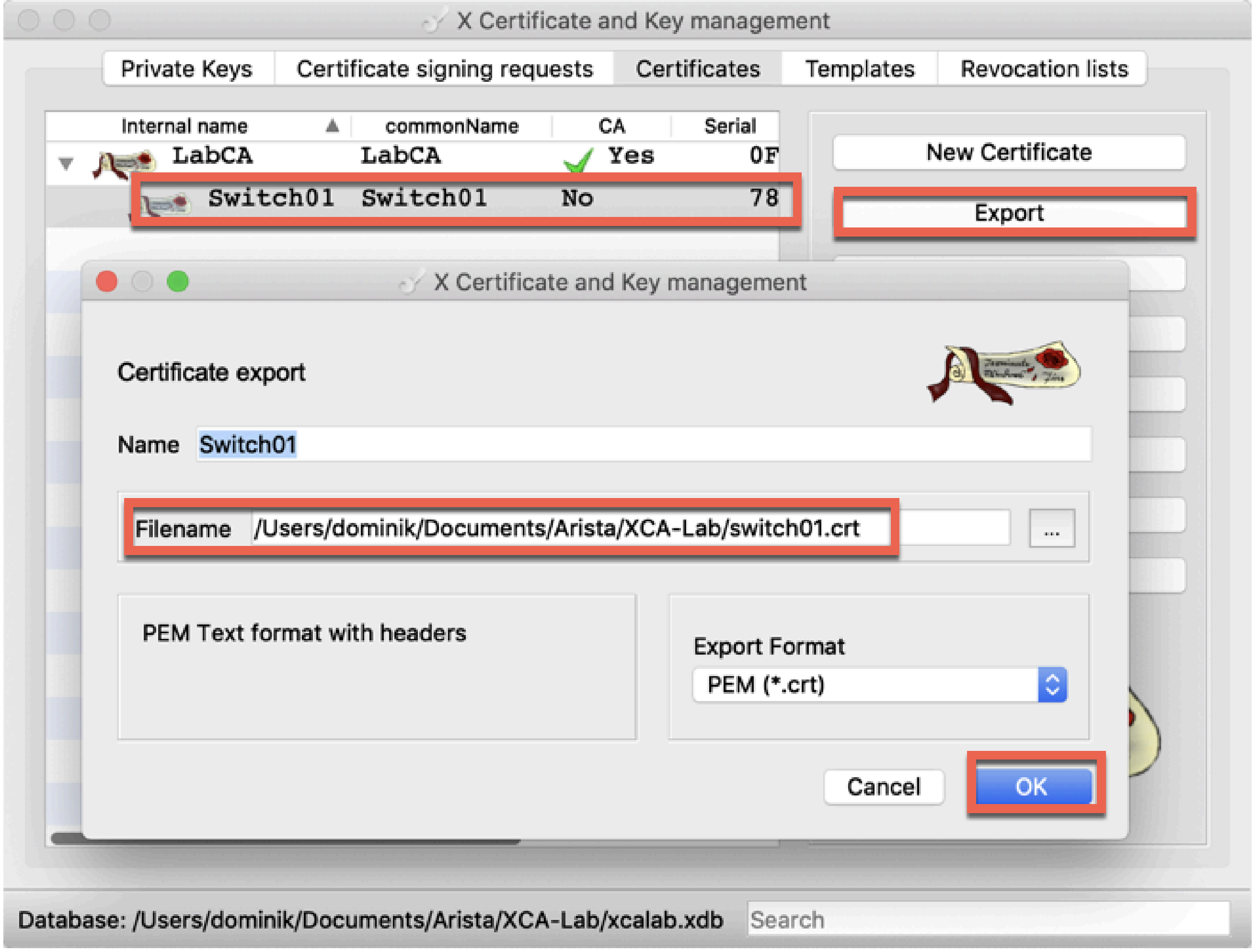


| Internal name | commonName | CA | Serial |
|---|---|---|---|
| LabCA | LabCA | ✓ Yes | 0F |
| Switch01 | Switch01 | No | 78 |

Database: /Users/dominik/Documents/Arista/XCA-Lab/xcalab.xdb

(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XD5vQAG&oid=00DA0000000H7UG)

Eventually, we export the certificate to a file. To do so, make sure the certificate is selected in the list and click on “Export”. Provide a filename and confirm by clicking on “OK”.


X Certificate and Key management
Private Keys
Certificate signing requests
Certificates
Templates
Revocation lists
New Certificate
Export
X Certificate and Key management
Cancel
OK

| Internal name | commonName | CA | Serial |
|---|---|---|---|
| LabCA | LabCA | ✓ Yes | 0F |
| Switch01 | Switch01 | No | 78 |

Certificate export

Name: Switch01

Filename: /Users/dominik/Documents/Arista/XCA-Lab/switch01.crt

PEM Text format with headers

Export Format: PEM (*.crt)

Database: /Users/dominik/Documents/Arista/XCA-Lab/xcalab.xdb

Search

(https://arista--c.na93.content.force.com/servlet/servlet.ImageServer?id=0152I000009XDFwQAO&oid=00DA0000000H7UG)

This concludes all the work necessary to install a desktop CA, generate a root certificate, import the CSR from a switch and issue a certificate based on that CSR. You may use this for your own lab or production environment.

Routing/Switching (/AristaCommunity/s/topic/0TO2I00…

EOS/cEOS/vEOS (/AristaCommunity/s/topic/0TO2I00…

Was this article helpful? 0 0

I (0) (/AristaCommunity/s/relatedlist/ka02I000000QqYTQA0/AttachedContentDocuments)

## Related Articles

| | |
|---|---|
| How to Work with Groups on CloudVision Wi-Fi (/AristaCommunity/s/article/how-to-works-with-groups-on-cloudvision-wifi) | 👁 604 |
| Significance of Certificates in Arista APs (/AristaCommunity/s/article/Significance-of-Custom-Certificates) | 👁 514 |
| Working of a Hidden SSID (/AristaCommunity/s/article/working-of-a-hidden-ssid) | 👁 1.14K |
| How to Configure Certificates on the On-Premises Wireless Manager (/AristaCommunity/s/article/how-to-configure-certificates-on-the-on-prem-wireless-manager) | 👁 695 |
| Wi-Fi Network Counters (/AristaCommunity/s/article/Wi-Fi-Network-Counters) | 👁 383 |

## Trending Articles

**DCS-7050SX3-48YC8/48C8 and 7050TX3-48C8: Logical port usages and limitations**
(/AristaCommunity/s/article/DCS-7050SX3-48YC8-and-7050TX3-48C8-Logical-port-usages-and-limitations)

**Wireshark for Troubleshooting - Part2**
(/AristaCommunity/s/article/Wireshark-for-troubleshooting-Part2)

**Understanding CloudVIsion APIs and accessing NetDB data**
(/AristaCommunity/s/article/Understanding-CloudVIsion-APIs-and-accessing-NetDB-data)

**VXLAN-EVPN Troubleshooting Guidebook**
(/AristaCommunity/s/article/VxLAN-EVPN-Troubleshooting-Guidebook)

**VeloCloud SD-WAN: VCE Links DEAD briefly after certificate renewal**
(/AristaCommunity/s/article/Velocloud-SD-WAN-VCE-Links-DEAD-briefly-after-certificate-renewal)

## Trending Topics

| | |
|---|---|
| **Routing/Switching**<br>(/AristaCommunity/s/topic/0TO2I000000DaWGWA0/routingswitching) | **13** |

## Get In Touch Today

Contact Us (https://www.arista.com/en/company/contact-us)

ARISTA

(https://www.facebook.com/AristaNW) (https://twitter.com/@AristaNetworks)
(https://www.linkedin.com/company/arista-networks-inc)

## Support

Support & Services (https://www.arista.com/en/support/customer-support)

Training (https://www.arista.com/en/partner/partner-portal/training)

Product Documentation (https://www.arista.com/en/support/product-documentation)

Software Downloads (https://www.arista.com/en/support/software-download)

## Contacts & Help

Contact Arista (https://www.arista.com/en/company/contact-us)

Contact Technical Support (https://www.arista.com/en/support/customer-support)

Order Status (https://orders.arista.com/)

## News

News Room (https://www.arista.com/en/company/news/in-the-news)

Events (https://www.arista.com/en/company/news/events)

Blogs (https://www.arista.com/blogs)

## About Arista

Company (https://www.arista.com/en/company/company-overview)

Management Team (https://www.arista.com/en/company/management-team)

Careers (https://www.arista.com/en/careers)

Investor Relations (https://investors.arista.com/)