

# **Summary steps to generating/obtaining an SSL certificate**

(i) Create your domain zone on the CA certificate manager

- Add domain on the CA certificate manager

- Delegate domain to a registrar (KENET)

(ii) Domain Control Validation (DCV)

- CNAME record based DCV

- eMail-based DCV

- HTTP(S)-based DCV

(iii) Submit your CSR (Certificate Signing Request)

(iv) Generate your SSL certificate

# 1. Create your domain zone on the CA (Certification Authority) certificate manager

-Add the domain on the Certification Authority portal.

NB: Inorder to generate a wildcard certificate, the domain is created with the following convention. e.g. for domain kenet.or.ke add as \*.kenet.or.ke

	NAME	DELEGATION STATUS	DATE REQUESTED
<input type="radio"/>	*.africainternational.edu	Approved	24/08/2015
<input type="radio"/>	africainternational.edu	Approved	06/10/2015
<input type="radio"/>	*.kenet.or.ke	Approved	30/08/2013
<input type="radio"/>	mirror.ac.ke	Approved	19/07/2015
<input type="radio"/>	maseno.ac.ke	Approved	19/07/2015
<input type="radio"/>	daystar.ac.ke	Approved	19/07/2015
<input type="radio"/>	*.ampath.or.ke	Approved	18/08/2015
<input type="radio"/>	mmust.ac.ke	Approved	20/07/2015
<input type="radio"/>	nrip.ac.ke	Approved	20/07/2015
<input type="radio"/>	ttuc.ac.ke	Approved	21/07/2015
<input type="radio"/>	ueab.ac.ke	Approved	21/07/2015
<input type="radio"/>	elearning.usiu.ac.ke	Approved	20/07/2015

Create Domain

Domain\*

\*.kenet.or.ke

Description

KENET registered domain

Organizations/Departments

SSL

S/MIME

Code Signing

☒ KENET

☒

☒

☐

[Expand All](#)

OK

Cancel

# Perform domain delegation

-Perform domain delegation: In this case, the domain will be delegated to KENET (an authorized registrar). This means that KENET name-servers gain control of the authority of the domain.

NB: The delegation request has to be approved by the CA as shown by the delegation status in the screen-shot below

https://cert-manager.com/customer/el4Africa?locale=en#5

Search

# COMODO Certificate Manager

Logged as: [Mula Peter](#)

Dashboard Certificates Discovery Reports Admins Settings About

Organizations Domains Notifications Encryption

Delegations DCV

Filter

+ Add View Delegate

	NAME	DELEGATION STATUS	DATE REQUESTED	▲ DCV STATUS	DCV EXPIRATION	
<input type="radio"/>	*.africainternational.edu	Approved	24/08/2015	Awaiting Submit		
<input checked="" type="radio"/>	africainternational.edu	Approved	06/10/2015	Awaiting Submit		
<input type="radio"/>	*.kenet.or.ke	Approved	30/08/2013	Validated	24/06/2016	
<input type="radio"/>	mirror.ac.ke	Approved	19/07/2015	Validated	22/07/2016	
<input type="radio"/>	maseno.ac.ke	Approved	19/07/2015	Validated	22/07/2016	
<input type="radio"/>	daystar.ac.ke	Approved	19/07/2015	Validated	22/07/2016	
<input type="radio"/>	*.ampath.or.ke	Approved	18/08/2015	Validated	12/08/2016	
<input type="radio"/>	mmust.ac.ke	Approved	20/07/2015	Validated	22/07/2016	
<input type="radio"/>	nitp.ac.ke	Approved	20/07/2015	Validated	22/07/2016	
<input type="radio"/>	ttuc.ac.ke	Approved	21/07/2015	Validated	22/07/2016	
<input type="radio"/>	ueab.ac.ke	Approved	21/07/2015	Validated	22/07/2016	
<input type="radio"/>	elearning.usiu.ac.ke	Approved	20/07/2015	Validated	11/05/2016	

## 2. Domain Control Validation (DCV)

A domain control validation, or DCV, is used by the CA before issuing an SSL certificate to verify the person making the request is in fact authorized to use the domain related to that request.

There are 3 mechanisms for DCV:

**a)DNS CNAME-based-** The CSR you submit to Comodo will be hashed. The hash values are provided to you and must be entered as a DNS CNAME record for your domain.

- The hash values are as shown below:

COMODO  
Certificate Manager

Logged as: [Muja Peter](#)

Dashboard

Certificates

Discovery

Reports

Admins

Settings

About

Organizations

Domains

Notifications

Encryption

Delegations

DCV

Filter

DCV

REGISTERED DOMAIN [+/-]	DCV STATUS
<input type="radio"/> <a href="#">tukenya.ac.ke</a>	Expired
<input type="radio"/> <a href="#">pu.ac.ke</a>	Expired
<input type="radio"/> <a href="#">kablanga.ac.ke</a>	Expired
<input type="radio"/> <a href="#">kirdi.go.ke</a>	Expired
<input checked="" type="radio"/> <a href="#">aua.ac.ke</a>	Expired
<input type="radio"/> <a href="#">chuka.ac.ke</a>	Validated
<input type="radio"/> <a href="#">machakosuniversity.ac.ke</a>	Validated
<input type="radio"/> <a href="#">scott.ac.ke</a>	Validated
<input type="radio"/> <a href="#">mua.ac.ke</a>	Validated
<input type="radio"/> <a href="#">mruc.ac.ke</a>	Validated
<input type="radio"/> <a href="#">eduroam.ac.ke</a>	Validated
<input type="radio"/> <a href="#">uon.ac.ke</a>	Validated

Domain - aua.ac.ke

1 Get Validation Info

2 Preliminary Test

3 Awaiting Validation

Requested Domain Name	aua.ac.ke
DCV Status	Expired
DCV Method	CNAME_CSR_Hash

SHA1 Hash	35E7973C0F6B6F50632A581A9915D26A9D622E35
MD5 Hash	C5B3FB3E3092AC4F98427503EF169FDD

Instructions for CNAME DCV:

1. Create a CNAME DNS record for **aua.ac.ke** as follows

C5B3FB3E3092AC4F98427503EF169FDD.aua.ac.ke. CNAME  
35E7973C0F6B6F50632A581A9915D26A9D622E35.comodoca.com.

2. After you have created the CNAME record, click the **Test** button below.

Cancel

Back

Test



**(b) eMail-based DCV** - an email is sent to an administrative contact for your domain. The email will contain a unique validation code and link. Clicking the link and entering the code will prove domain control.

**NB:** Valid email addresses would include admin@, administrator@, postmaster@, hostmaster@, and [webmaster@kenet.or.ke](mailto:webmaster@kenet.or.ke) where kenet.or.ke is the domain for which the certificate is being applied

### **(c) HTTP(S)-based DCV**

The CSR you submit to Comodo will be hashed. The hash values are provided to you and you must create a simple plain-text file and place this in the root of your webserver and served over HTTP-only!

The file and it's content should be as follows:

<http://yourdomain.com/><Lower case value of MD5 hash of

### 3. Generating CSR using openssl

Refer to the link below for a step-by-step procedure of generating a CSR

[http://www.rackspace.com/knowledge\\_center/article/generate-a-csr-with-openssl](http://www.rackspace.com/knowledge_center/article/generate-a-csr-with-openssl)

Steps can be summarized as follows:

(a) Create a new directory and switch to it

```
> mkdir conf
```

```
> cd conf
```

(b) Install openssl

```
> sudo apt-get install openssl
```

(c) Generate the RSA key (private key)

```
> openssl genrsa -out MYSSL.key 2048
```

## 4. Generate your certificate

-On the certificate manager, select the certificates tab and request for a certificate by providing the CSR and other details required as below:

The screenshot shows the Comodo Certificate Manager interface. On the left is a sidebar with navigation links: Dashboard, Certificates (selected), and Discovery. Under Certificates, there are links for SSL Certificates and Client Certificates. Below these are buttons for Filter, Add, Export, Add For Auto Install, and Edit. A table lists existing certificates with columns for Common Name and Organization. The main area displays the 'Request New SSL Certificate' form. The form includes dropdown menus for Organization (KENET), Department (ANY), Certificate Type (Comodo PlatinumSSL Certificate), Certificate Term (1 year), and Server Software (AOL). There is a text area for CSR and buttons for 'Get CN from CSR' and 'Upload CSR'. Below these are text fields for Common Name, Requester (Muia Peter), External Requester, and a comments box. At the bottom, there is a Subscriber Agreement section with a link to the agreement and OK/Cancel buttons.

COMODO Certificate Manager

Dashboard Certificates Discovery

SSL Certificates Client Certificates

Filter

Add Export Add For Auto Install Edit

COMMON NAME	ORGANIZATION
*.aua.ac.ke	KENET
*.mu.ac.ke	KENET
*.aiu.ac.ke	KENET
*.cue.or.ke	KENET
*.mu.ac.ke	KENET
*.kenet.or.ke	KENET
*.pacuniversity.ac.ke	KENET
*.uonbi.ac.ke	KENET

### Request New SSL Certificate

\*-required fields

Organization\* KENET Refresh

Department\* ANY

[Click here to edit address details](#)

Certificate Type\* Comodo PlatinumSSL Certificate

Certificate Term\* 1 year

Server Software\* AOL

CSR\*

Max CSR size is 32K Get CN from CSR Upload CSR

Common Name\*

Requester Muia Peter

External Requester

Comments

Subscriber Agreement

COMODO CERTIFICATE SUBSCRIBER AGREEMENT IMPORTANT—PLEASE READ THIS

OK Cancel

- After your certificate is issued, download ready for installation.  
An installation guide can be found at:

***[http://www.rackspace.com/knowledge\\_center/article/installing-an-ssl-certificate-on-apache](http://www.rackspace.com/knowledge_center/article/installing-an-ssl-certificate-on-apache)***