

## 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

COMODO Certificate Manager

Logged as: [Mujia Peter](#)

Dashboard Certificates Discovery Reports Admins Settings About

Organizations Domains Notifications Encryption

Delegations DCV

Filter

+ Add

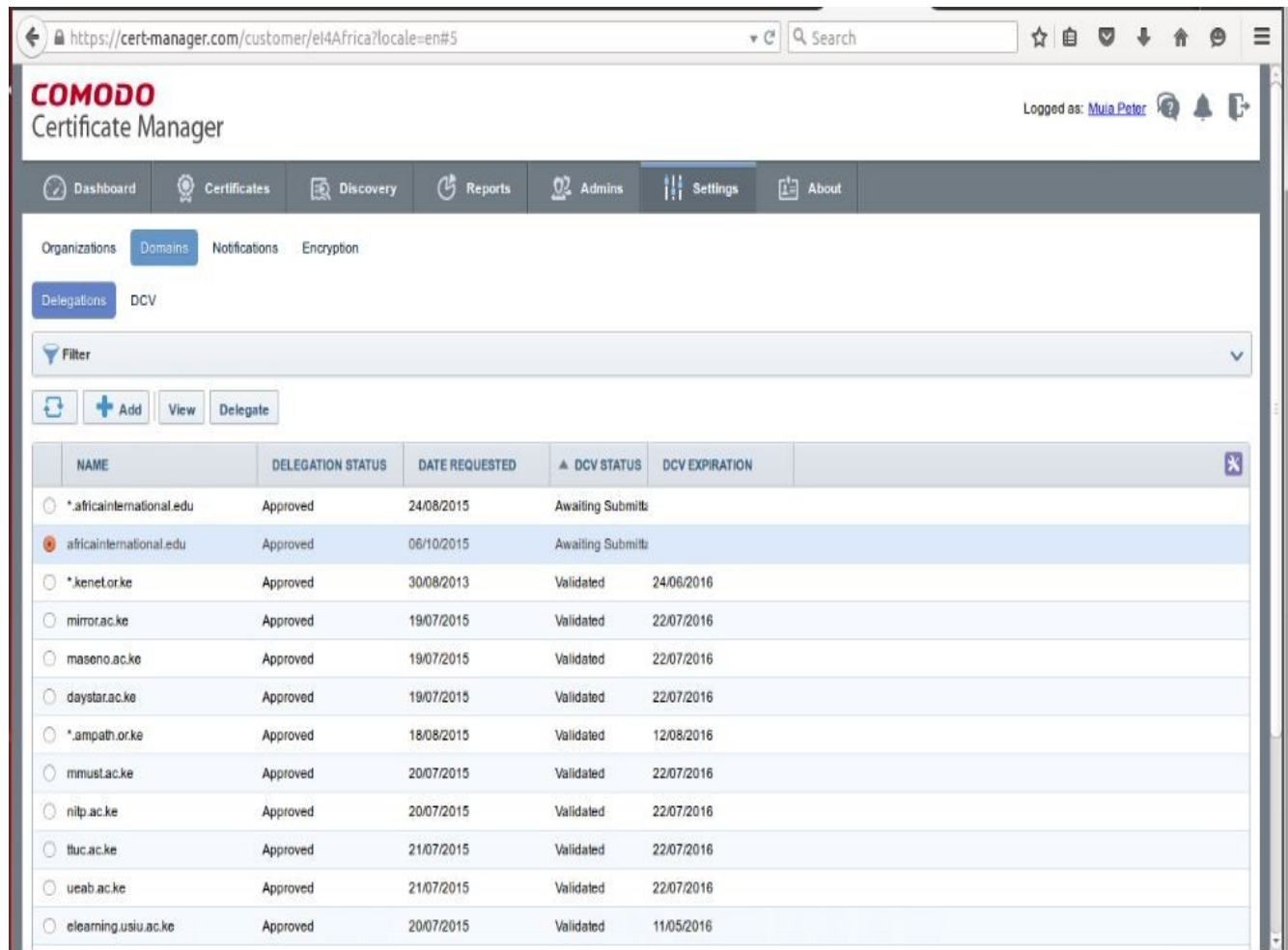
NAME	DELEGATION STATUS	DATE REQUESTED
<input type="radio"/> *.africainternational.edu	Approved	24/08/2015
<input type="radio"/> africainternational.edu	Approved	06/10/2015
<input type="radio"/> *.kenet.or.ke	Approved	30/08/2013
<input type="radio"/> mirror.ac.ke	Approved	19/07/2015
<input type="radio"/> 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"/> ntp.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

Expand All

OK Cancel

-Perform domain delegation: In this case, the domain will be delegated to KENET (an authorized registrar). This means that KENET nameservers 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



The screenshot shows the Comodo Certificate Manager web interface. The browser address bar displays <https://cert-manager.com/customer/ei4Africa?locale=en#5>. The page header includes the Comodo logo and 'Certificate Manager'. A navigation bar contains links for Dashboard, Certificates, Discovery, Reports, Admins, Settings (active), and About. Below this, a sub-navigation bar shows Organizations, Domains (active), Notifications, and Encryption. The 'Delegations' tab is selected, and the 'DCV' (Domain Control Validation) section is active. A filter bar is present above a table of delegations. The table has columns for NAME, DELEGATION STATUS, DATE REQUESTED, DCV STATUS, and DCV EXPIRATION. The table lists several domains, including \*.africaninternational.edu, africaninternational.edu, \*.kenet.or.ke, and others, all with a status of 'Approved'.

NAME	DELEGATION STATUS	DATE REQUESTED	DCV STATUS	DCV EXPIRATION
*.africaninternational.edu	Approved	24/08/2015	Awaiting Submit	
africaninternational.edu	Approved	06/10/2015	Awaiting Submit	
*.kenet.or.ke	Approved	30/08/2013	Validated	24/06/2016
mirror.ac.ke	Approved	19/07/2015	Validated	22/07/2016
maseno.ac.ke	Approved	19/07/2015	Validated	22/07/2016
daystar.ac.ke	Approved	19/07/2015	Validated	22/07/2016
*.ampath.or.ke	Approved	18/08/2015	Validated	12/08/2016
mmust.ac.ke	Approved	20/07/2015	Validated	22/07/2016
nitp.ac.ke	Approved	20/07/2015	Validated	22/07/2016
ltuc.ac.ke	Approved	21/07/2015	Validated	22/07/2016
ueab.ac.ke	Approved	21/07/2015	Validated	22/07/2016
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:

The screenshot shows the Comodo Certificate Manager interface. The sidebar on the left has tabs for Organizations, Domains, Notifications, and Encryption. Under Domains, there are tabs for Delegations and DCV. A table lists registered domains with their DCV status. The domain 'aua.ac.ke' is selected, and a modal window titled 'Domain - aua.ac.ke' is open. The modal shows the DCV process steps: 1. Get Validation Info, 2. Preliminary Test, and 3. Awaiting Validation. It also displays the requested domain name, DCV status (Expired), DCV method (CNAME\_CSR\_Hash), and the SHA1 and MD5 hashes. Instructions for CNAME DCV are provided, including a CNAME record example and a 'Test' button.

REGISTERED DOMAIN [+]	DCV STATUS
tukenya.ac.ke	Expired
pu.ac.ke	Expired
kablanga.ac.ke	Expired
kirdi.go.ke	Expired
aua.ac.ke	Expired
chuka.ac.ke	Validated
machakosuniversity.ac.ke	Validated
scott.ac.ke	Validated
mua.ac.ke	Validated
mruc.ac.ke	Validated
eduroam.ac.ke	Validated
uon.ac.ke	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.

Buttons: 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/<Upper case value of MD5 hash of CSR>.txt`

**Note:** The DCV will fail if any redirection is in place.

-After the DCV has been validated by the CA, proceed to generate your certificate using the CSR created as in the steps below.

### 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

(d) Create a CSR using the above RSA key

> openssl req -new -sha256 -key MYSSL.key -out MYSSL.csr

(e) Verify your CSR

> openssl req -noout -text -in MYSSL.csr

### 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:

https://cert-manager.com/customer/ei4Africa?locale=en#1

COMODO Certificate Manager

Dashboard Certificates Discovery

SSL Certificates Client Certificates

Filter

+ Add Export Add For Auto Install Edit

COMMON NAME	ORGANIZATION
*.aia.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 Mula 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)