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)

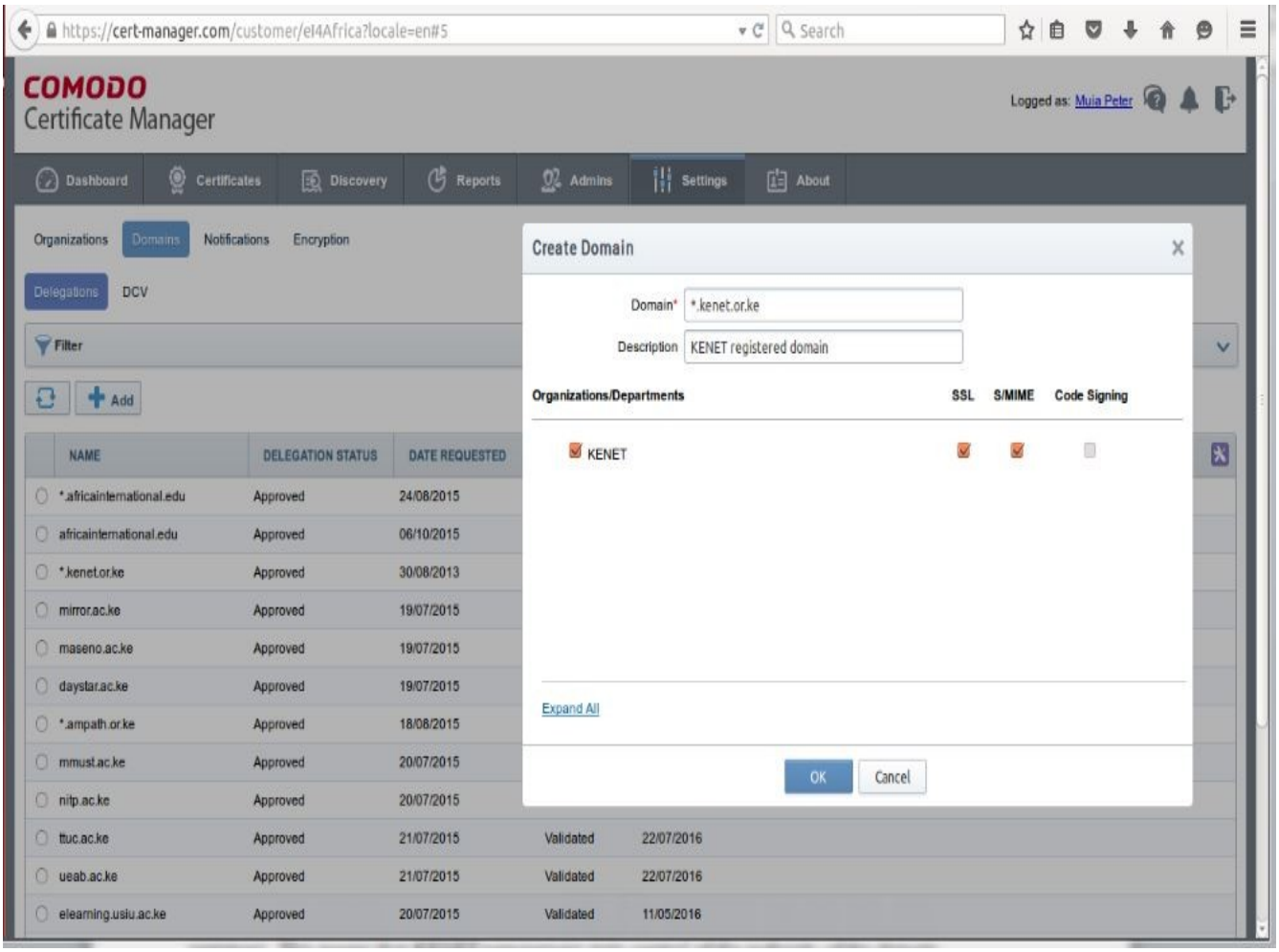
(ii) Domain Control Validation (DCV)
-CNAME record based DCV
-eMail-based DCV
-HTTP(S)-based DCV

(iii) Submit your CSR (Certificate Signing Request)

(iv) Generate your SSL certificate

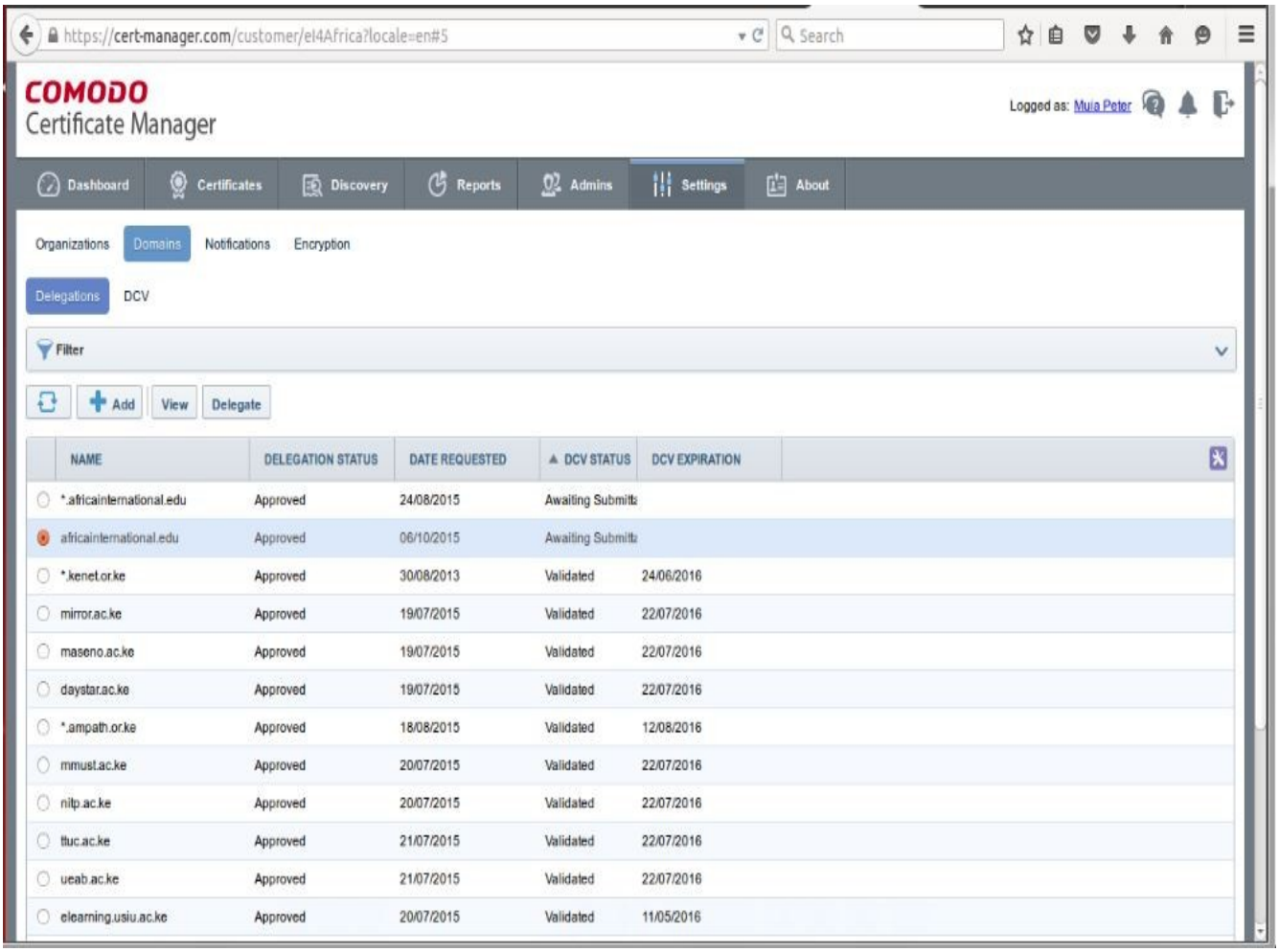
1. Create your domain zone on the CA (Certification Authority) certificate manager

-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



-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



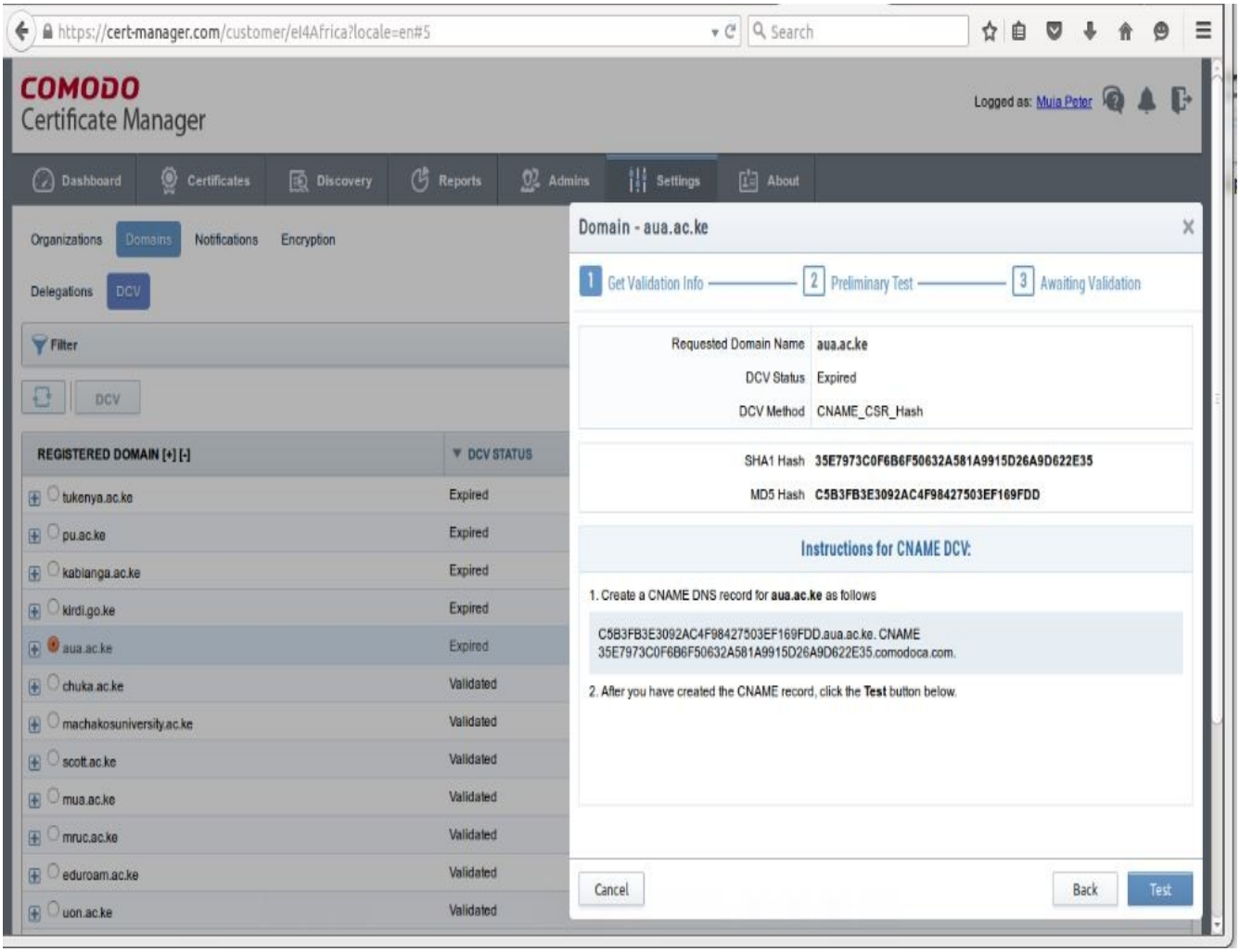
2. Domain Control Validation (DCV)

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:



(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 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

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

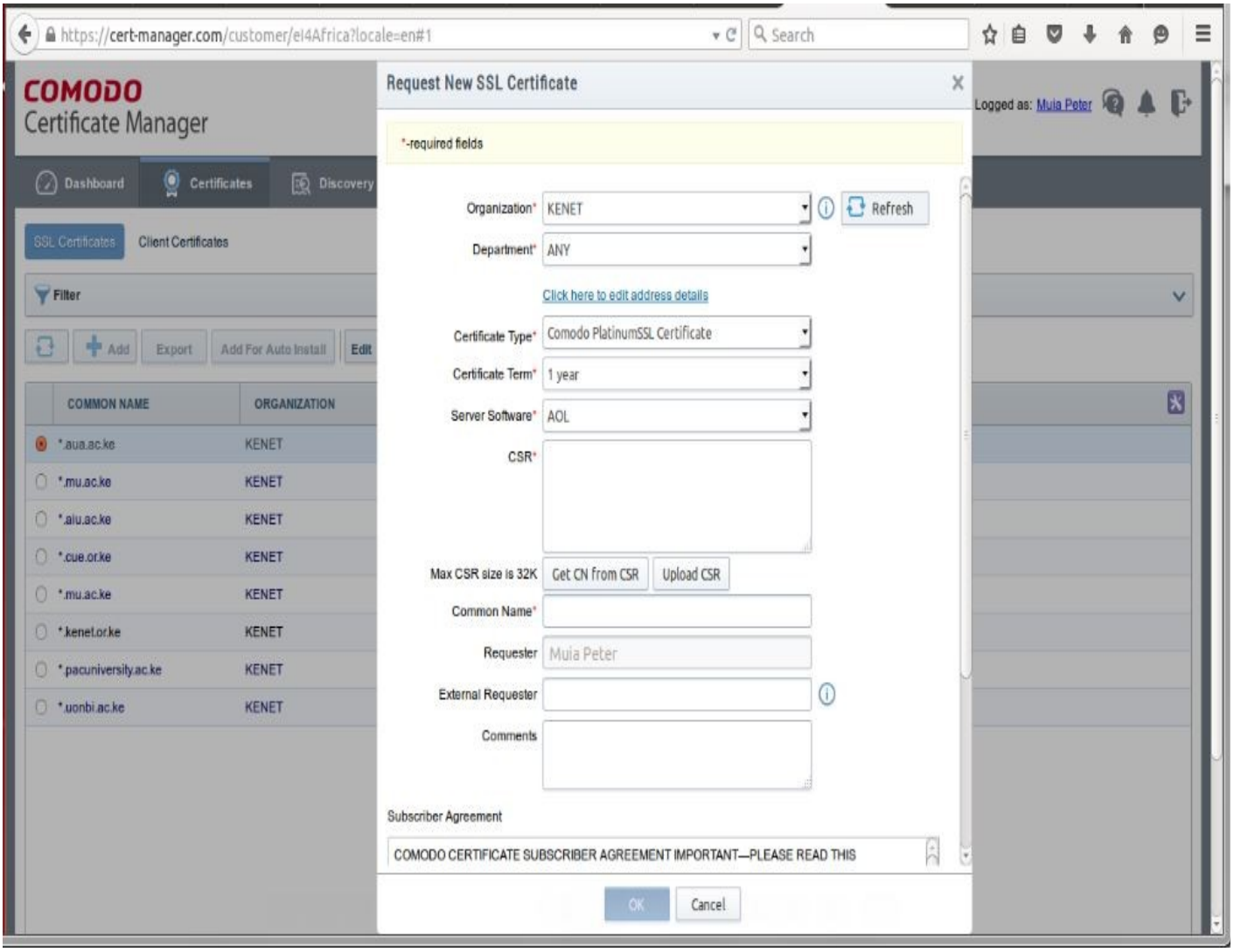
(c) Generate the RSA key (private key)
> openssl genrsa -out MYSSL.key 2048

(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:



- 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