**Router is the CA Server.**

**onePK Box is where application runs.**

Create a CA cert on the onePK box.

Follow instructions from

<http://acidx.net/wordpress/2012/09/creating-a-certification-authority-and-a-server-certificate-on-ubuntu/>

Before you start, make sure to have openssl installed. This however should be the case by default on Ubuntu.

Preparations

*# Become root (you might have to set a password first: sudo passwd)*  
su -  
  
*# Create a directory for the CA and switch to it*  
mkdir /root/ca  
cd /root/ca  
  
*# Create some (necessary) directories*  
mkdir newcerts certs crl private requests  
  
*# Get a copy of the standard SSL configuration*  
cp /etc/ssl/openssl.cnf ./config.txt  
  
*# Create some necessary files*  
touch index.txt  
echo '01' > serial

#### Generate the CA’s Private Key

Now that all the files and folders are prepared, the CA’s private key can be generated:

openssl genrsa -des3 -out private/cakey.pem 4096

The output should look like this:

root@acidx:~/ca# openssl genrsa -des3 -out private/cakey.pem 4096  
Generating RSA private key, 4096 bit long modulus  
............++  
..................................................................................++  
e is 65537 (0x10001)  
Enter pass phrase for private/cakey.pem:  
Verifying - Enter pass phrase for private/cakey.pem:

#### Create the CA Root Certificate

To create the certificate, enter:

openssl req -new -x509 -key private/cakey.pem -out cacert.pem -days 3650 -set\_serial 0

The output should look like this:

root@acidx:~/ca# openssl req -new -x509 -key private/cakey.pem -out cacert.pem -days 3650 -set\_serial 0  
Enter pass phrase for private/cakey.pem:  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----

Install CA cert on router

configure terminal

crypto pki trustpoint rtrca

enrollment terminal pem

subject-name CN=ec2-54-187-124-97.us-west-2.compute.amazonaws.com

revocation-check none

crypto pki authenticate rtrca

<copy ca cert contents form the CA server when it asks >

Then press enter and y to accept it

Create a cert request on the router

ip-10-0-0-254#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

ip-10-0-0-254(config)#crypto pki trustpoint rtrca

ip-10-0-0-254(ca-trustpoint)#crypto pki enroll rtrca

% Start certificate enrollment ..

% The subject name in the certificate will include: CN=ec2-54-187-124-97.us-west-2.compute.amazonaws.com

% The subject name in the certificate will include: ip-10-0-0-254.us-west-2.compute.internal

% Include the router serial number in the subject name? [yes/no]: yes

% The serial number in the certificate will be: 9VQZFDOVYXG

% Include an IP address in the subject name? [no]: yes

Enter Interface name or IP Address[]: 10.0.0.254

Display Certificate Request to terminal? [yes/no]: ye

Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----

MIIBfzCCASkCAQAwgaIxOjA4BgNVBAMTMWVjMi01NC0xODctMTI0LTk3LnVzLXdl

c3QtMi5jb21wdXRlLmFtYXpvbmF3cy5jb20xZDASBgNVBAUTCzlWUVpGRE9WWVhH

MBcGCSqGSIb3DQEJCBMKMTAuMC4wLjI1NDA1BgkqhkiG9w0BCQIWKGlwLTEwLTAt

MC0yNTQudXMtd2VzdC0yLmNvbXB1dGUuaW50ZXJuYWwwXDANBgkqhkiG9w0BAQEF

AANLADBIAkEAsS3xcU78vEKHnYRDbHpjbH3AXOoRKGqJ0L577+6+EDCEaZWdqDkc

5DHHmvGeiPSm31aaFQVuEfLSgymnO9MwlQIDAQABoCEwHwYJKoZIhvcNAQkOMRIw

EDAOBgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQEFBQADQQCfg5UP8+8SDagCHa6J

iE/UaiMhCdUzsv2iLiwh8a4w+iq3VWpbQxRXUa6CatPadrixmTpN0upfJMl8OaCw

k52b

-----END CERTIFICATE REQUEST-----

Sign Cert request from router on onePK box

Go to the CA box in sudo mode and copy the above request into a pem file

ubuntu@ip-10-0-1-190:~$ su -

Password:

root@ip-10-0-1-190:~# cd /ca

-su: cd: /ca: No such file or directory

root@ip-10-0-1-190:~# cd /root/ca

root@ip-10-0-1-190:~/ca# clear

root@ip-10-0-1-190:~/ca# cd requests/

root@ip-10-0-1-190:~/ca/requests# vi Sprint1.pem

root@ip-10-0-1-190:~/ca# openssl x509 -days 3650 -CA cacert2.pem -CAkey private/cakey2.pem -req -in Sprint1.pem -outform PEM -out Sprint1Cert.pem -CAserial serial

Signature ok

subject=/CN=ec2-54-187-124-97.us-west-2.compute.amazonaws.com/serialNumber=9VQZFDOVYXG/unstructuredAddress=10.0.0.254/unstructuredName=ip-10-0-0-254.us-west-2.compute.internal

Getting CA Private Key

Enter pass phrase for private/cakey2.pem:

Install sign request cert on the router.

crypto pki import rtrca certificate

copy the signed certificate from Sprint1Cert.pem when asked.

Setup TLS on router

ip-10-0-0-254(config)#onep

ip-10-0-0-254(config-onep)#transport type tls disable-remotecert-validation

ip-10-0-0-254(config-onep)#transport type tls remotecert rtrca

ip-10-0-0-254(config-onep)# service set vty

Run the program

On the onePK box, run

source ./setupOnePK

setup config.txt with router ips(comma separated), username, password and ca cert location.

./bin/onePKRouterConfigurator -c config.txt -i 10.0.0.21 -a a