SET UP A CERTIFICATE AUTHORITY IN RHEL5

Security certificates are widely used for authentication. This article explores how to set up a Certificate Authority in RHEL5.

Security certificates are basically used for authentication purposes and you must have encountered a number of websites that use them. These digital certificates are issued by a Certificate Authority. Such certificates contain the public key of the applicants and various other information regarding their identity. In this article, we'll discuss the setting up of a Certificate Authority in RHEL and certificate signing.

Before we start, just make sure you have *openssl* installed on your system and follow the steps listed below:

1. Open the */etc/pki/tls/openssl.cnf* file in a text editor and write down the following lines under the [CA_default] section:

dir=/etc/pki/myCA

certificate=$dir/my-ca.crt

crl=$dir/my-ca.crl

private_key=$dir/private/my-ca.key

You can find the purpose of each of these objects in the */etc/pki/tls/openssl.cnf* file.

2. Under the *[req_distinguished_name]* section, you can specify the default values for several fields:

countryName_default=IN

stateOrProvinceName_default=West Bengal

localityName_default=Kolkata

These fields are used during the time of certificate creation.

3. Now it is time to create your working directories using the following command:

```
mkdir p /etc/pki/myCA/{certs,crl,newcerts,private}
```

4. Create a certificate index file using the command that follows:

```
touch /etc/pki/CA/index.txt
```

5. To create another file for the next certificate serial number to be issued, use the following command:

```
echo 01 > /etc/pki/myCA/serial
```

6. It’s time to generate a private key and a self-signed certificate for your Certificate Authority.

```
cd /etc/pki/myCA
openssl genrsa -out private/my-ca.key des3 2048
```

Do remember the passphrase you give at this step.

7. Now create your self-signed certificate using the command shown below:

openssl req 'new x509 key private/my-ca.key days 365 > my-ca.crt

This certificate will be distributed to your users.

With this, the process of setting up a Certificate Authority is complete. Now you can make your self-signed certificate downloadable by your users through a Web browser. Let us next check out the process of signing a certificate.

1. First of all, generate a private key using the *openssl genrsa 1024 > mykey.key* command.
2. Then create the Certificate Signing Request using the openssl req 'new'key mykey.key out mycsr.csr command.
3. Now, as the Certificate Authority, sign the certificate using the *openssl ca* in *mycsr.csr out mycert.crt* command.

Your certificate is now ready to be used across multiple applications including the Web and e-mail. You can view information regarding this certificate in the */etc/pki/myCA/newcerts/01.pem*file. Also, if you open */etc/pki/myCA/serial*, you'll see that its contents have been updated to 2, which is the serial number for the next certificate to be signed. As a Certificate Authority, you can also revoke a certificate using the openssl ca revoke */etc/pki/myCA/newcerts/01.pem* command. Here *01.pem* id is the file related to the first certificate that we've created.

So this was a brief overview of how to set up a Certificate Authority in RHEL5. You can use it for intranet applications management. And if you want to understand the functionality behind the Certificate Security, you can explore the cryptography concepts related to certificates like TLS/SSL handshakes, key distribution, cryptographic hashes, etc.[i]

Source : http://www.opensourceforu.com/2014/01/set-certificate-authority-rhel5/