Obtaining Digital Certificates In IOS

Keith Bogart

CCIE #4923

- kbogart@ine.com
- @keithbogart1
- linkedin.com/in/keith-bogart-2a75042

CCIE Routing & Switching

Topic Overview

- Prerequisites For Creating Certificates Within IOS
- PKI Trustpoints
- Subject-Name
- Pointing To The Trustpoint
- Downloading The CA's Root Certificate
- Enrolling With The CA
- Verification

Requesting Identity Certificates

- The following steps need to be taken on a router (or firewall) in order to eventually obtain an Identity Certificate from a Root Authority;
  - Create RSA Keypair
  - Ensure IP reachability to the Root (or Intermediate) CA
  - Configure a Trustpoint
  - Authenticate the Trustpoint
  - Submit a CSR to the Trustpoint (also called, “enrolling”)
- Optional (but recommended) is to synchronize time with NTP.

CSR = Certificate Signing Request. Typically done by using SCEP (Simple Certificate Enrollment Protocol).

-

It’s important that devices containing Identity Certificates have their time synchronized with the Root CA. Otherwise, certificates may expire before devices are actually aware of this fact and have the opportunity to take some action. Or they may believe that Certificates are already expired from their peers when in reality…they are not.

PKI Trustpoints

- Trustpoint = Certificate Authority
- Cisco devices desiring an Identity Certificate must be configured to recognize/point-to a Trustpoint.
  - CSR will be sent to the Trustpoint.
  - This is called, “enrolling” the Certificate.
- Trustpoint must be configured in IOS specifying (at minimum);
  - RSA Keypair to Enroll
  - Enrollment method (such as HTTP, HTTPS, SCP, others)
  - Many other optional items could be included.

When selecting HTTP as the enrollment method, this means you’ll be using SCEP (Simple Certificate Enrollment Protocol) over HTTP.

Trustpoint Configuration

```
Router-2(config)#crypto pki trustpoint CSR-1
Router-2(ca-trustpoint)#rsakeypair Router2-Key
Router-2(ca-trustpoint)#enrollment url http://172.16.1.11
Router-2(ca-trustpoint)#
Router-2(ca-trustpoint)#
Router-2(ca-trustpoint)#subject-name ?
  LINE  Subject Name

Router-2(ca-trustpoint)#subject-name keith
"keith" is not a valid subject name
The subject name must be in X.500 (LDAP) format

Router-2(ca-trustpoint)#$e CN=Router2.ine.com OU=Lab O=INE L=RTP S=NC C=US
Router-2(ca-trustpoint)#
```


More on the “Subject-name” command in the next slide.

Subject-Name

- Required component of a Digital Signature
- By default, IOS devices populate this field with their Hostname.
- Should match the name remote devices will use to recognize the local device.
- Must follow X.500 “Distinguished Names” format:
  - CN=commonName (name of person or device)
  - OU=organizationUnit (small organization, department or division)
  - O=organizationName (large organization or company name)
  - L=localityName (locality, city, or municipality)
  - S=stateName (State name)
  - C=country (Two-letter Country code)

If you try to use HTTPS to securely access a website, and the “subject name” in the cert doesn’t match what you typed into the URL, the Certification will display as untrusted.

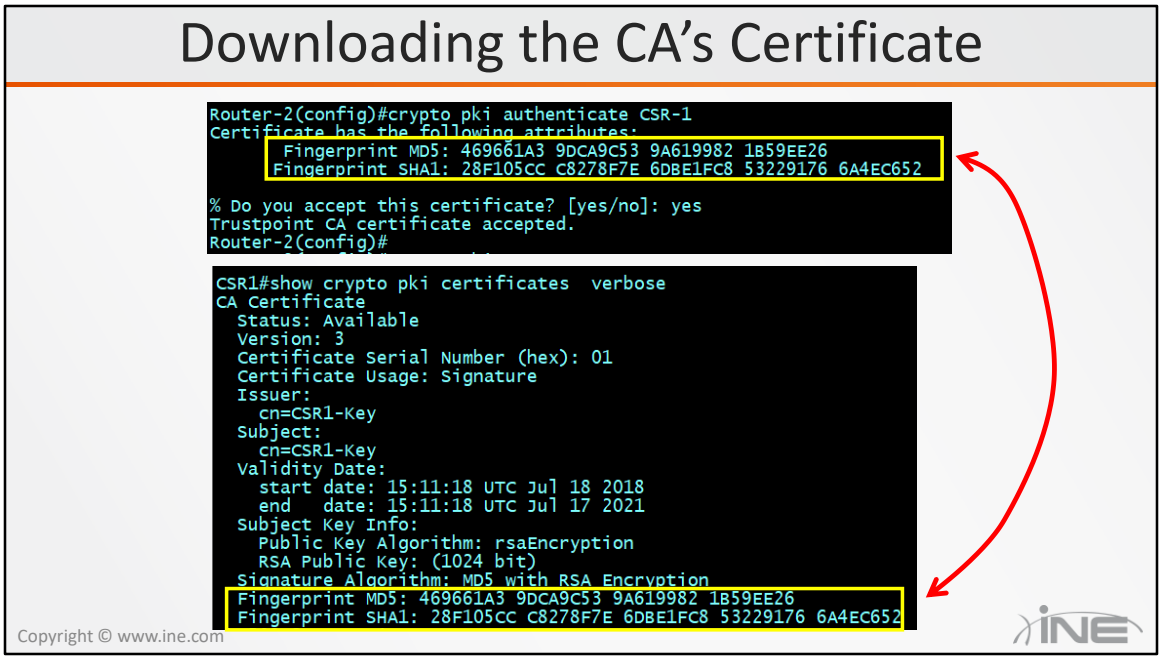
-

According to non-Cisco documents, the order of the X.500 elements does matter when manually typing a Subject-Name. Apparently this is not the case when configuring Cisco IOS devices.

-

If you choose to supply a subject-name, you can choose how many of these elements you wish to utilize.

Downloading the CA's Certificate



We want to verify that the fingerprints match otherwise we could be downloading a cert from an imposter.

-

What is the difference between "Signature Algorithm" and "Fingerprint"? Signature Algorithm is what the CA used to hash-and-encrypt the Digital Signature. Fingerprint is a hashed version of the CA's public key. Rather than providing the full Public Key in this output which would be very long…it is presented as both an MD5 and SHA1 hash so we can easily locate, and verify it.

Manually Enrolling With The CA

```
Router-2(config)#crypto pki enroll CSR-1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: Router-2
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: FTX1405A063
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CSR-1' commandwill show the fingerprint.

Router-2(config)#
```


Serial Number: The serial number is not used by IP Security or Internet Key Exchange but may be used by the CA to either authenticate certificates or to later associate a certificate with a particular router. (Note that the serial number stored is the serial number of the internal board, not the one on the enclosure.) Ask your CA administrator if serial numbers should be included. If you are in doubt, include the serial number.

-

IP Address: Normally, you would not include the IP address because the IP address binds the certificate more tightly to a specific entity. Also, if the router is moved, you would need to issue a new certificate. Finally, a router has multiple IP addresses, any of which might be used with IPSec. If you indicate that the IP address should be included, you will then be prompted to specify the interface of the IP address. This interface should correspond to the interface that you apply your crypto map set to.

-

If you are enrolling with a Certificate Authority that requires a password, then you would input that password at the prompts. If you have configured a Cisco IOS device (router) as a CA Server, by default that device is not looking for (nor cares about) any password. So you can supply whatever password you wish here…and it will just be ignored.

-

If you desire the Cisco IOS CA Server to enforce secure Certificate Enrollment (via SCEP) then you must configure the command, “crypto pki server <name> password generate <minutes>” on the CA Server. This will cause a temporary one-time password to be generated which you would then provide to the PKI Clients. The PKI Clients would then insert that password when given the prompts to do so during enrollment.

Auto-Enrolling With The CA

```
crypto pki trustpoint R1-CA
 enrollment url
 revocation-check crl
 rsakeypair Router-4.ine.com
 auto-enroll 75 regenerate
```

- Auto-enrollment provides several benefits over manual enrollment:
  - As soon as Root CA (i.e. Trustpoint) is authenticated, router will automatically (dynamically) transmit a Certificate Signing Request
  - When the lifetime of the Root CA's Certificate is about to expire, Client will automatically ask for a new Root Certificate
  - When the lifetime of the current Identity Certificate is about to expire, this feature will automatically request a new Identity Certificate

The value after the "auto-enroll" keyword is optional. If entered, specifies a percentage of time. For example, 75 means after the currently-active Identity Certificate has been alive/active for 75% of its lifetime, auto-enroll to obtain a new Cert.

-

Regenerate is also optional. If specified, it means this router will auto-generate a new RSA keypair each time it perform auto-enrollment.

-

Couldn't find any documents to state what the default value was for percentage, but in lab tests, auto-enroll seems to default to about 2-minutes prior to expiration of current Identity Certificate.

Confirming Certificate Enrollment

```
Router-4#sho crypto pki certificates
Router Certificate (Rollover)
  Status: Available
  Certificate Serial Number (hex): 0E
  Certificate Usage: General Purpose
  Issuer:
    cn=R1-CA
  Subject:
    Name: Router-4.ine.com
    hostname=Router-4.ine.com
  Validity Date:
    start date: 14:23:53 UTC Oct 22 2018
    end   date: 14:35:02 UTC Oct 22 2018
  Associated Trustpoints: R1-CA
```

```
Certificate
  Status: Available
  Certificate Serial Number (hex): 0D
  Certificate Usage: General Purpose
  Issuer:
    cn=R1-CA
  Subject:
    Name: Router-4.ine.com
    hostname=Router-4.ine.com
  Validity Date:
    start date: 14:15:02 UTC Oct 22 2018
    end   date: 14:23:53 UTC Oct 22 2018
  Associated Trustpoints: R1-CA
```


The “rollover” keyword indicates that auto-enrollment has been configured and, because the Active Certificate is near its expiration date, a new (i.e. Rollover) certificate has been enrolled-and-downloaded.

-

Notice the differences between the start/end dates-and-times…and the serial number of the current certificate (0xD) as compared to the Rollover Certificate (0xE) that hasn’t become active yet.