APPENDIX C

Certificate Signing Request (CSR) Generation for a Third-Party Certificate on Cisco Prime Infrastructure

This appendix describes how to generate a Certificate Signing Request (CSR) to obtain a third-party certificate with Cisco Prime Infrastructure and how to import the certificate into Prime Infrastructure. It contains the following sections:

Prerequisites

Ensure that you meet these requirements before you attempt this configuration:

- Knowledge of how to install and configure Prime Infrastructure for basic operation
- Knowledge of self-signed and digital certificates, and other security mechanisms related to Public Key Infrastructure (PKI)

For more information about the supported hardware, see the Prime Infrastructure release notes at the following URL:

http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-release-notes-list.html

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Certificate Signing Request (CSR)

A certificate is an electronic document that you use to identify a server, a company, or some other entity and to associate that identity with a public key.

A self-signed certificate is an identity certificate that is signed by its own creator. That is, the person who created the certificate also signed off on its legitimacy.

Certificates can be self-signed or can be attested by a digital signature from a certificate authority (CA).

CAs are entities that validate identities and issue certificates. The certificate issued by the CA binds a particular public key to the name of the entity that the certificate identifies, such as the name of a server or device. Only the public key that the certificate certifies works with the corresponding private key possessed by the entity that the certificate identifies. Certificates help prevent the use of fake public keys for impersonation.

A CSR is a message that an applicant sends to a CA to apply for a digital identity certificate. Before a CSR is created, the applicant first generates a key pair, which keeps the private key secret. The CSR contains information that identifies the applicant, such as a directory name in the case of an X.509 certificate, and the public key chosen by the applicant. The corresponding private key is not included in the CSR, but is used to digitally sign the entire request.

The CSR can be accompanied by other credentials or proofs of identity required by the certificate authority, and the certificate authority can contact the applicant for further information. For the most part, a third-party CA company, such as Entrust or VeriSign, requires a CSR before the company can create a digital certificate.

CSR generation is independent of the device on which you plan to install an external certificate. Therefore, a CSR and a private key file can be generated on any individual machine which supports CSR generation. CSR generation is not switch-dependent or appliance-dependent in this case.

This appendix describes how to generate a CSR for a third-party certificate using the Cisco Prime Infrastructure.

Generating a Certificate Signing Request (CSR) File

An SSL certificate can be obtained from a third party. To set up this support, you must:

1. Generate a Certificate Signing Request file.
2. Submit the signing request to a Certificate Authority you choose.
3. Apply the signed Security Certificate file to the server.

Step 1 Generate a Certificate Signing Request (CSR) file for the Prime Infrastructure server:

a. At the Prime Infrastructure appliance, exit to the command line.

b. At the command line, log in using the administrator ID and password used to install Prime Infrastructure.

c. Enter the following command to generate the CSR file in the default backup repository:

- ncs key genkey -newdn -csr *CertName***.csr repository** *RepoName*

where:

– *CertName* is an arbitrary name of your choice (for example: MyCertificate.csr).

– *RepoName* is any previously configured backup repository (for example: defaultRepo).

Step 2 Copy the CSR file to a location you can access. For example:

copy disk:/*RepoName***/***CertName***.csr ftp://your.ftp.server**

Step 3 Send the CSR file to a Certificate Authority (CA) of your choice.

Note Once you have generated and sent the CSR file for certification, do *not* use the **genkey** command again to generate a new key on the same Prime Infrastructure server. If you do, importing the signed certificate file will result in mismatches between keys in the file and on the server.

Step 4 You will receive a signed certificate file with the same filename, but with the file extension CER, from the CA. Before continuing, ensure:

- There is only one CER file. In some cases, you may receive chain certificates as individual files.
- Any blank lines in the CER file are removed.

Step 5 At the command line, copy the CER file to the backup repository. For example:

- copy ftp://your.ftp.server/*CertName***.cer disk:***RepoName*

Step 6 Import the CER file into the Prime Infrastructure server using the following command:

- ncs key importsignedcert *CertName***.cer repository** *RepoName*

Step 7 Restart the Prime Infrastructure server by issuing the following commands in this order:

- ncs stop

- ncs start

Step 8 If the Certificate Authority who signed the certificate is not already a trusted CA: Instruct users to add the certificate to their browser trust store when accessing the Prime Infrastructure login page.

Get a Signed Certificate for CSR from Microsoft Certificate Authority (CA)

You must take the CSR, load it into the Microsoft CA, and have it signed as an Internet certificate. Once you do this, you get a new *.csr file that shows a path where the Microsoft CA is the trusted root and not the Prime Infrastructure. Complete these steps in order to submit the CSR to CA if your CA is a Windows 2008 Server.

Step 1 Open the CSR file you downloaded in to Notepad and copy the entire contents including the ---BEGIN CERTIFICATE --- and ---END CERTIFICATE -- lines.

Step 2 Go to http://<certificate server address>/certsrv in order to open the Certificates Server web page.

Step 3 Enter your username and password.

Step 4 Click **Request a certificate**.

The Request a Certificate web page appears.

Step 5 Click **the advanced certificate request** link.

The Submit a Certificate Request or Renewal Request web page appears.

Step 6 Paste the content you copied in Step1 into the Saved Request field, choose **Web Server in the Certificate Template** drop-down list, and click **Submit**.

Step 7 On the Certificate Issued web page, click the **DER encoded** radio button, and then click **Download certificate**.

Step 8 Save the file to your local computer.

Importing a Certificate Authority (CA) Certificate and Key

Step 1 At the command line, log in using the administrator ID and password and enter the following command:

ncs key importcacert *aliasname ca-cert-filename* **repository** *repositoryname*

where

- *aliasname* is a short name given for this CA certificate.
- *ca-cert-filename* is the CA certificate file name.
- *repositoryname* is the repository name configured in Prime Infrastructure where the ca-cert-filename is hosted.

Step 2 To import an RSA key and signed certificate to Prime Infrastructure, enter the following command in admin mode:

ncs key importkey ***key-filename cert-filename*** **repository** ***repositoryname***

where

- *key-filename* is the RSA private key file name.
- *cert-filename* is the certificate file name.
- *repositoryname* is the repository name configured in Prime Infrastructure where the key-file and cert-file are hosted.

Step 3 Restart the Prime Infrastructure server by issuing the following commands in this order:

- ncs stop

- ncs start

Viewing the list of Certificates

To list all the CA certificates that exist in Prime Infrastructure trust store, use Prime Infrastructure **key listcacerts** command.

ncs key listcacerts

This example shows how to list all the CA certificates exist in Prime Infrastructure trust store:

```
admin# ncs key listcacerts

Certificate utnuserfirsthardwareca from CN=UTN-USERFirst-Hardware,
OU=http://www.example.com, O=The USERTRUST Network, L=Salt Lake City, ST=UT, C=US
```

```
Certificate gtecybertrust5ca from CN=GTE CyberTrust Root 5, OU="GTE CyberTrust Solutions,
Inc.", O=GTE Corporation, C=US
Certificate equifaxsecureebusinessca1 from CN=Equifax Secure eBusiness CA-1, O=Equifax
Secure Inc., C=US
Certificate thawtepersonalfreemailca from EMAILADDRESS=email@example.com, CN=Thawte
Personal Freemail CA, OU=Certification Services Division, O=Thawte Consulting, L=Cape
Town, ST=Western Cape, C=ZA
Certificate addtrustclass1ca from CN=AddTrust Class 1 CA Root, OU=AddTrust TTP Network,
O=AddTrust AB, C=SE
Certificate aolrootca1 from CN=America Online Root Certification Authority 1, O=America
Online Inc., C=US
Certificate geotrustuniversalca from CN=GeoTrust Universal CA, O=GeoTrust Inc., C=US
Certificate digicertglobalrootca from CN=DigiCert Global Root CA, OU=www.example.com,
O=DigiCert Inc, C=US
Certificate certumtrustednetworkca from CN=Certum Trusted Network CA, OU=Certum
Certification Authority, O=Unizeto Technologies S.A., C=PL
Certificate swisssignsilverg2ca from CN=SwissSign Silver CA - G2, O=SwissSign AG, C=CH
```

Deleting Certificates

To delete CA certificates that exist in Prime Infrastructure trust store, use Prime Infrastructure key deletecacert command.

ncs key deletecacert *aliasname*

This example shows how to delete CA certificates exist in Prime Infrastructure trust store:

```
admin# ncs key deletecacert certumtrustednetworkca
Deleting certificate from trust store
```

Related Publications

For more information about Prime Infrastructure, see the following URL:

http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/tsd-products-support-series-home.html