Digital Certificates
HOW TO GUIDE

July 2011

Revision 1.0

Table of Contents

1. Introduction:

1.1 Overview:

Security in 802.11 systems relies on digital certificates to provide mutual authentication and encryption. Mutual authentication or trust is provided by leveraging Public Key Infrastructure (PKI) which allows all parties in the security exchange to verify and validate digital certificates on each party. Authentication and encryption is provided using standard public key and private key algorithms to protect credentials exchanged over the air as well as exchange credentials.

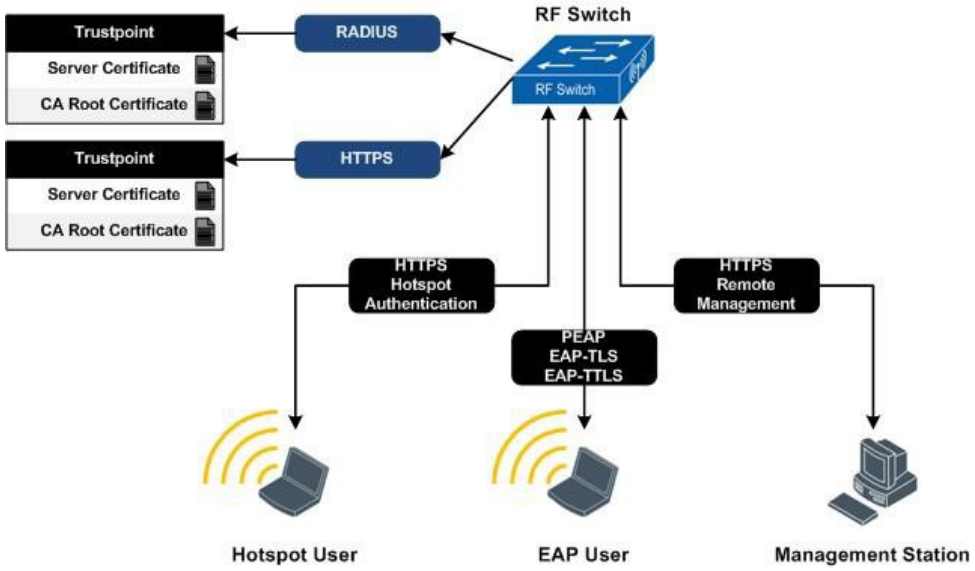


Figure 1.1 – Digital Certificates

1.1.1 Certification Authority:

To verify that a digital certificate is not forged, you need a mechanism to validate it which is provided by a certification authority (CA). The CA is a trusted third party that can be a private secure server deployed in an enterprise data center or a public server from a specialized company offering certificates such as Entrust, Go Daddy or, VeriSign.

The CA is charged with signing all user and server certificates and signs a certificate by running a hash of the certificate contents, encrypting the hash with its Private Key (creating a digital signature), then appending this signature to the end of the certificate. The CA also has a certificate of its own called a CA certificate or root certificate. The root certificate contains the CA's Public Key and can be freely distributed any party. Anyone that has the CA's root certificate installed can validate certificates issued from the CA.

Most operating systems include root certificates issued from top public certificate providers allowing secure transactions to be made on-line without having to manually install root certificates.

Using a CA to sign user and server certificates and validate them is the simplest form of Public Key Infrastructure (PKI). A certificate chain includes information about the CA or CA's involved in issuing certificates and the user or server certificates themselves. There are other PKI functions such as certificate revocation lists, cross-certification and certificate chaining that are used but are beyond the scope of a guide.

1.1.2 Trustpoints:

Server and CA certificates are installed in pairs on the RF Switch into trustpoints which are assigned to the local RADIUS and HTTPS services. Each service on the RF Switch supports a single trustpoint allowing separate server certificates to be used for RADIUS and HTTPS services.

WiNG provides a default trustpoint which includes a self-signed server certificate which is assigned to the local RADIUS and HTTPS services. However as the default server certificate is self-signed, no mutual authentication can be provided as no Certificate Authority (CA) root certificate exists to allow the end users to trust the self-signed certificate.

To provide mutual authentication and trust for management, EAP and Hotspot services a trustpoint needs to be created on the RF Switch and a certificate request generated to a public or enterprise CA. Once the certificate request has been signed by the CA, the server and CA certificate can be installed on the RF Switch. Once installed the RF Switch mutual authentication can occur between all parties with certificates issued from the CA.

1.1.2.1 Server Certificates:

Server certificates are digital identifications containing information about a server, service or organization. Server certificates contain a public key which is used to create a secure TLS connection between the service and end user device. In WLAN environments server certificates are used to provide secure encrypted HTTPS management connections to RF Switches and Access Points as well as protect credentials over the air for Hotspot and EAP authentication.

Server certificates are required for all external RADIUS servers providing EAP authentication as well as the RF Switches providing RADIUS, Hotspot or secure web based management. The RF Switch supports a single server certificate for local RADIUS services and a single server certificate to provide Hotspot and secure web based management.

1.1.2.2 Root Certificates:

A root certificate is a self-signed certificate or an unsigned public key certificate which forms the foundation of a public key infrastructure (PKI). A root certificate is the top-most certificate in the Certificate Authority (CA) tree, and its private key is used sign all certificates issued from the CA.

Root certificates are installed on end user devices to identify and verify digital certificates issued from CAs. Root certificates for common public CAs such as Entrust and VeriSign are typically pre-installed on most operating systems allowing the end user devices to automatically trust servers and applications using digital certificates issued from these CAs. However in enterprise environments, a private CA is often deployed and CA certificates are automatically or manually distributed to end user devices before certificate verification and trust can occur.

It's not mandatory that a CA root certificate be installed on the end user device for WLAN authentication as web browsers and 802.1X supplicants can establish a secure connection to a peer without a CA certificate being present. However in WLAN deployments it is strongly recommended that a CA root certificate be installed as the CA certificate provides the only mechanism for the end device to verify the identity of the presented digital certificate prior to credentials being exchanged. Without a CA certificate being installed, the device is susceptible to man-in-the-middle (MIN) attacks.

1.2 Applications:

Digital certificates are required to enable the following services on the RF Switch:

1) Secure Web UI Management – Provides secure remote web based management of the RF Switch. When enabled all web management configuration transactions are encrypted using Transactional Layered Services (TLS). In addition PKI allows the remote management station to verify the identity of the RF Switch prior to submitting management credentials.
2) EAP Authentication – When using the integrated RADIUS server, PKI allows the RF Switch to authenticate users using PEAP, EAP-TLS and EAP-TTLS. These EAP methods provide mutual authentication between the RF Switch and 802.1X supplicant as well as a secure TLS tunnel to exchange credentials over the air.
3) Hotspot Authentication – Provides web based authentication for users. When users authenticate to the RF Switch by presenting a username and password which is encrypted over the air using TLS. In addition PKI provides the ability to allow the end user to verify the identity of the RF Switch prior to submitting credentials.

1.3 Restrictions:

A single trustpoint can be assigned to the HTTPS service which is shared for both secure Web-UI management and Hotspot services.

If Hotspot authentication is required, Zebra recommends that the hostname for the CN field in the server certificate be defined to resolve to the IP address assigned to the Hotspot virtual interface. This will ensure compatibility with Mozilla Firefox and Microsoft Internet Explorer which uses the CN field to detect phishing attacks.

2. Pre-Requisites:

2.1 Requirements:

The following requirements must be met prior to attempting this configuration:

One (or more) RF Switches are installed and operational on the network.

One (or more) Access Ports configured and adopted by the RF Switch.

One (or more) WLAN profiles are configured and assigned to adopted radios.

A Windows XP workstation is available with Microsoft Internet Explorer or Mozilla Firefox to perform Web UI configuration.

A public or private Certificate Authority available to issue server certificates to the RF Switch.

The reader has read the Zebra Solutions WiNG 5 System Reference

.

2.2 Components Used:

The information in this document is based on the following Zebra hardware and software versions:

1 x RFS6000 Version 5.1.0.0-074R.

1 x AP7131N.

Registered users may download the latest software and firmware from the Zebra Solutions Support Site http://support.symbol.com.

3. Configuration:

The following section outlines the configuration steps required to add a Digital Certificate issued from a Certification Authority onto a RF Switch. This guide describes the steps to create a trustpoint on an RFS6000 switch. But the same steps can be used for installing a trustpoint on any other controller or access point.

1) Generating Certificate Request [Section 3.1]:
2) Importing Signed Certificates [Section 3.2]:
3) Assigning Trustpoints [Section 3.3]:

3.1 Generating a Certificate Request:

Before a certificate can be installed into a trustpoint on the RF Switch, a certificate request must be generated. A certificate request will generate a new certificate key and prepare a certificate signing request (CSR) which can be entered into a Certificate Authority to generate a server certificate.

The CSR contains information identifying the RF Switch including information such as Company, Organization, Department, Country and Locality. The CSR also include specific network level information about the RF Switch such as IP Address, hostname and fully qualified domain name.

When a certificate signing request is generated, the RF Switch will generate a Base64 PKCS#10 binary encoded text which can be saved to a file. The PKCS#10 file can then be uploaded to a CA or the PKCS#10 file opened in a text editor and the content copied and pasted into a form on the CA.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBnTCCAQYCAQAwXTELMAkGA1UEBhMCU0cxETAPBgNVBAoTCE0yQ3J5cHRvMRIw
EAYDVQQDEwlsb2NhbGhvc3QxJzAlBgkqhkiG9w0BCQEWGGFkbWluQHNlcnZlci5l
eGFtcGxlLmRvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAr1nYY1Qrll1r
uB/FqlCRrr5nvupdIN+3wF7q915tvEQoc74bnu6b8IbbGRMhzdzmvQ4SzFfVEAuM
MuTHeybPq5th7YDrTNizKKxOBnqE2KYuX9X22A1Kh49soJJFg6kPb9MUgiZBiMlv
tb7K3CHfgw5WagWnLl8Lb+ccvKZZl+8CAwEAAaAAMA0GCSqGSIb3DQEBBAUAA4GB
AHpoRp5YS55CZpy+wdigQEwjL/wSluvo+WjtpvP0YoBMJu4VMKeZi405R7o8oEwi
PdlrrliKNknFmHKIaCKTLRcU59ScA6ADEIWUzqmUzP5Cs6jrSRo3NKfg1bd09D1K
9rsQkRc9Urv9mRBIsredGnYECNeRaK5R1yzpOowninXC
-----END CERTIFICATE REQUEST-----
```

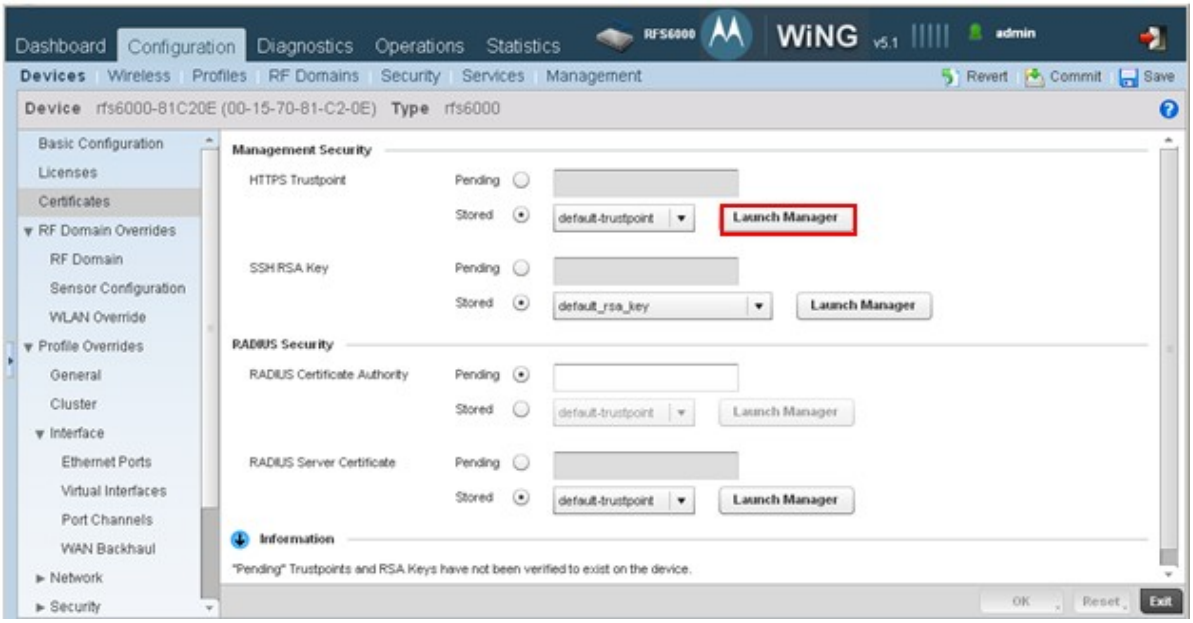
Figure 3.1 – Base64 Encoded CSR Generated from an RF Switch

Section 4.0 explains the process for issuing a server certificate using Microsoft Certificate services

3.1.1 Web UI Configuration Example:

The following configuration example will demonstrate how to create a trustpoint and generate a Certificate Signing Request on the RF Switch using the Web UI:

1) Navigate to the ***Configuration > Devices > RFS6000-81-C2-0E > Certificates*** window. Click "***Launch Manager"***.



2) In the ***Certificates Management,*** select ***Create CSR*** tab. Select the option ***Create New*** to generate a new RSA Key (private key) to be used with the trustpoint. Enter the key name ***rfs6000_rsa_key***. Set the key size to 1024 bits (default). Select the ***subject name*** as ***user-configured.*** Enter the required server certificate information that will be forwarded to the certificate authority in the certificate request. The certificate authority will use the information entered on this page to generate the server certificate. Click ***Generate CSR***.

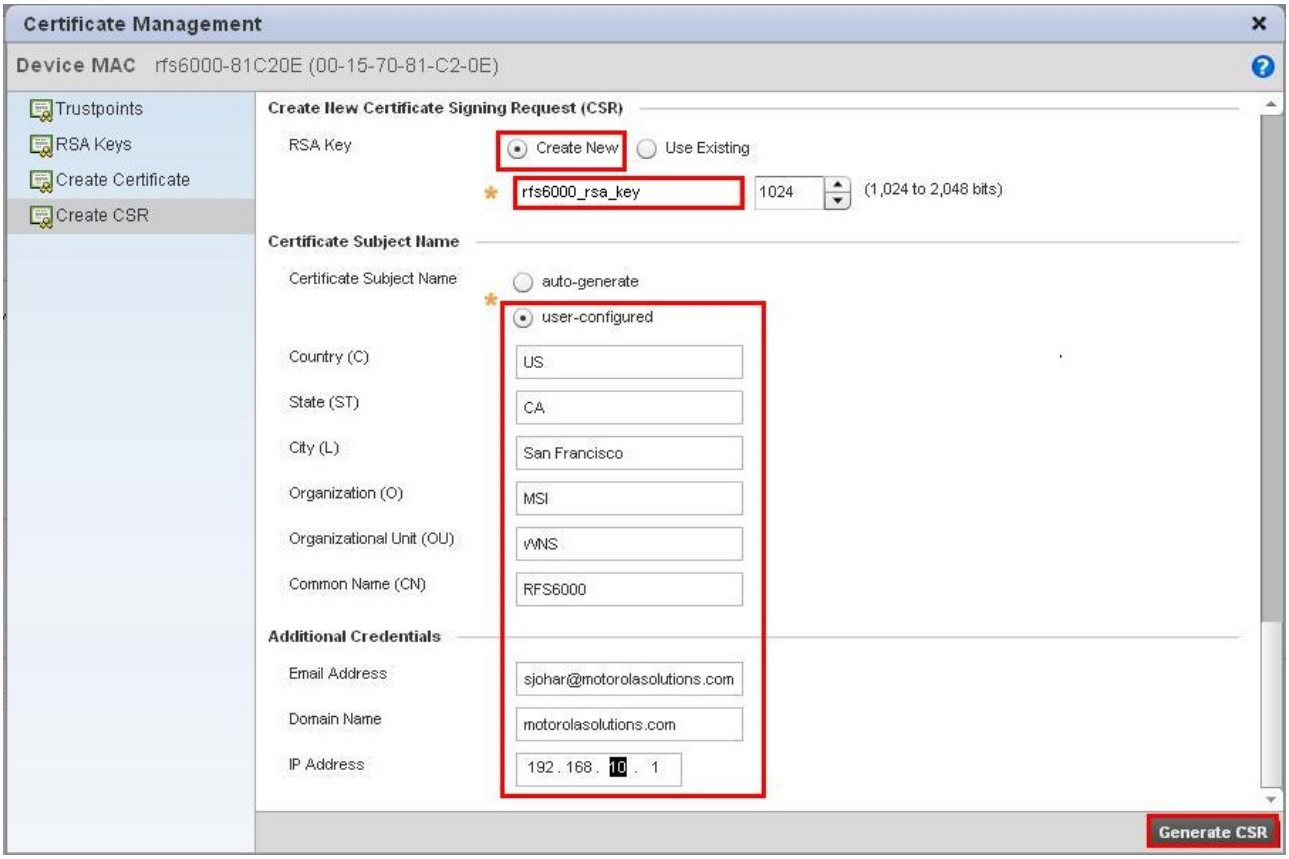
Country (C)	The country to be displayed in the server certificate for identification (example US).
State (ST)	The state or province to be displayed in the server certificate for identification (example CA).
City (L)	The locality or city to be displayed in the server certificate for identification (example San Francisco).
Organisation (O)	The company name or organisation to be displayed in the server certificate for identification (example MSI.).
Organisation Unit (OU)	The organisation or department to be displayed in the server certificate for identification (example WNS).

Common Name (CN) The hostname of the RF Switch (example rfs6000.Zebrasolutions.com). The common name must be resolvable by DNS to the management or Hotspot interface on RF Switch for the client to trust the certificate.

Email Address The email address to contact for issues related to the certificate request..

IP Address The IP Address on the device for the management or Hotspot interface using the certificate. The IP Address will be added to the Subject Alternative Name field in the server certificate (example 192.168.10.14).

FQDN The fully qualified domain name that specifies the node's position in the DNS tree hierarchy.



3) The RF Switch will generate a Base64 PCKS#10 encoded certificate request that can be entered into a Certificate Authority to generate the server certificate. The certificate request encoded text can be saved to a text file. Click ***Close***.

4) The server certificate request can now be injested by a Certificate Authority to generate a server certificate. An example using Microsoft Certificate services is provided in Section 4.

3.1.2 CLI Configuration Example:

1) Enter the following command to generate a certificate request with the parameters explained in step #2 above. The certificate request will be saved into a file csr_req.txt on the TFTP server. The server certificate request can now be injested by a Certificate Authority to generate a server certificate. An example using Microsoft Certificate services is provided in Section 4.

```
rfs6000-81C20E# crypto pki export request generate-rsa-key rfs6000_rsa_key subject-name
RFS6000 US CA  "San Francisco"  MSI  WNS   tftp://10.10.1.64/csr_req.txt
```

3.2 Importing Signed Certificates:

Once a certificate has been issued form a CA, it will need to be imported along with a CA root certificate into the trustpoint on the RF Switch. Most CAs provide the ability to save an issued certificate in numerous formats and care needs to be made to ensure that the issued server and CA root certificates are saved using Base64 encoding. The Base64 encoded server certificate and CA root certificate files can then be uploaded into the RF Switch.

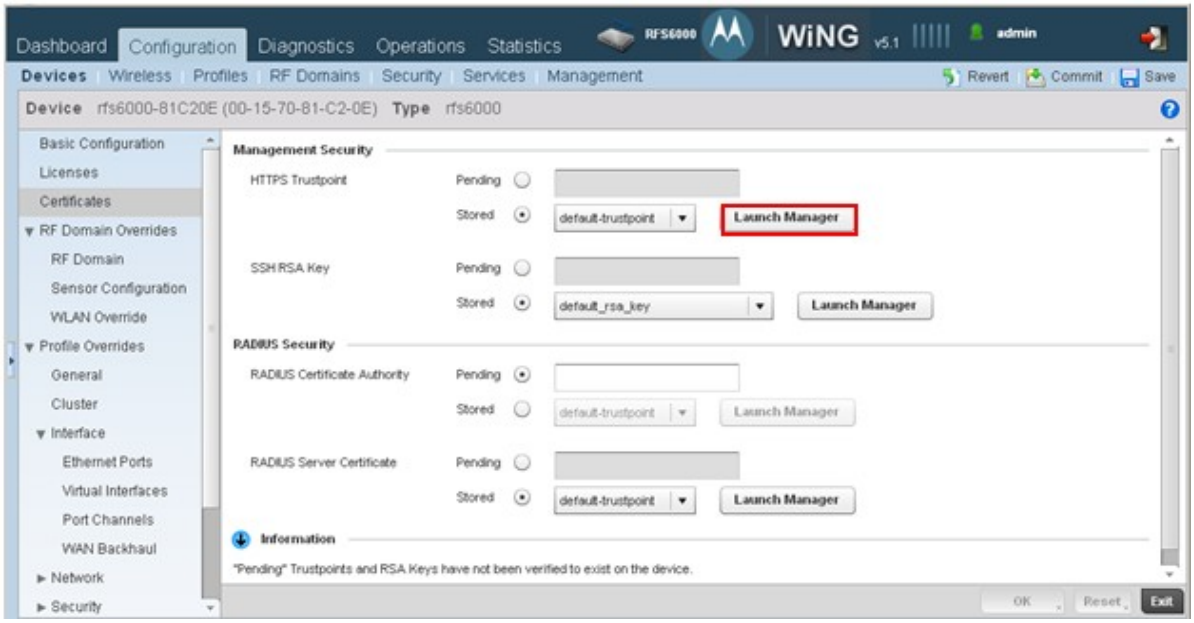
```
-----BEGIN CERTIFICATE-----
MIIF1zCCBL+gAwIBAgIKbHnDYwAAAAAAJzANBgkqhkiG9w0BAQUFADBBMRMwEQYK
CZImiZPyLGQBGRYDY29tMRYwFAYKCZImiZPyLGQBGRYGZXNlbGFiMRIwEAYDVQQD
EwlFU0VMQUIgQ0EwHhcNMDgwODE0MTg1MDI4WhcNMTAwODE0MTg1MDI4WjB9MQsw
CQYDVQQGEwJVUzELMAkGA1UECBMCVE4xFTATBgNVBAcTDEpvaG5zb24gQ2l0eTEW
MBQGA1UEChMNTW90b3JvbGEgSW5jLjEhMB8GA1UECxMYRW50ZXJwcmlzZSBXTEFO
IERpdmlzaW9uMQ8wDQYDVQQDEwZ3czYwMDAwgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBALZ+8aJWSJ7JjuVJ7f+iNffacvh+vN44raTFzRUTaDgR04jSqSgA6w8N
fPTUVcOxG8sq5Vwg19qiugcw2H8MDaAIlMAVqdbkccsoLm30ld6YyVIYf3CvfATW
s7p/AWWoIgFtFjc4rAtENPPvyqB/eMSTa8sidgeCCACN4XE1EUVzAgMBAAGjggMX
MIIDEzALBgNVHQ8EBAMCBaAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwIgYDVR0RBBsw
GYcEwKgKDoIRd3M2MDAwLmVzZWxhYi5jb20wHQYDVR0OBBYEFLZMmzIBZjRRUr+o
/W3ZVxIRZhA2MB8GA1UdIwQYMBaAFPq5zcZQepfvVBYM8C+DAifE03XUMIIBBAYD
VR0fBIH8MIH5MIH2oIHzoIHwhoG0bGRhcDovLy9DTj1FU0VMQUIlMjBDQSxDTj13
M2tzZXJ2ZXIxLENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1T
ZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWVzZWxhYixEQz1jb20/Y2VydGlm
aWNhdGVSZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1
dGlvblBvaW50hjdodHRwOi8vdzNrc2VydmVyMS5lc2VsYWIuY29tL0NlcnRFbnJv
bGwvRVNFTEFCJTIwQ0EuY3JsMIIBGQYIKwYBBQUHAQEEggELMIIBBzCBqQYIKwYB
BQUHMAKGgZxsZGFwOi8vL0NOPUVTRUxBQiUyMENBLENOPUFJQSxDTj1QdWJsaWMl
MjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERD
PWVzZWxhYixEQz1jb20/Y0FDZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNl
cnRpZmljYXRpb25BdXRob3JpdHkwWQYIKwYBBQUHMAKGTWh0dHA6Ly93M2tzZXJ2
ZXIxLmVzZWxhYi5jb20vQ2VydEVucm9sbC93M2tzZXJ2ZXIxLmVzZWxhYi5jb21f
RVNFTEFCJTIwQ0EuY3J0MAwGA1UdEwEB/wQCMAAwOwYJKwYBBAGCNxUHBC4wLAYk
KwYBBAGCNxUInfYig5iFL4flkyuZ1FSErMwMgRSEtrkpt5s4AgFkAgEDMBsGCSsG
AQQBgjcVCgQOMAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQEFBQADggEBAGmLi8TT
R2fj83zBKIrbED30f+lZvU6MmotL4OPjdNiStvVxCFpCWzYuneVYpdRXAYaby4H5
5XKlzgxOn/FJuIXv5mjGG7M4mIvLF1CAfXjYAIcqBK2U9no9bf5g9ySPocCGEbK/
mB64HHAeYEVcCHiHr4Qcq6XtKWE6SL2mYZxTB8a3abNAy0zcqpIs9GkcW1miViIX
g1RpwRYX5wi8QlEPtFO8jcqUbGjwBx0tI6TzkB+UOpPp8ik2TXg+nNGKExzxFD7V
KiSen5RS3YyCAStrQCUzzfjH8WZ6Aq7hgiBSbJMte2W/JzH0hwhmuexX3g9K6OhH
04xZS4gHWO3qc8Y=
-----END CERTIFICATE-----
```

Figure 3.2 – Base64 Encoded Certificate Issued from a CA

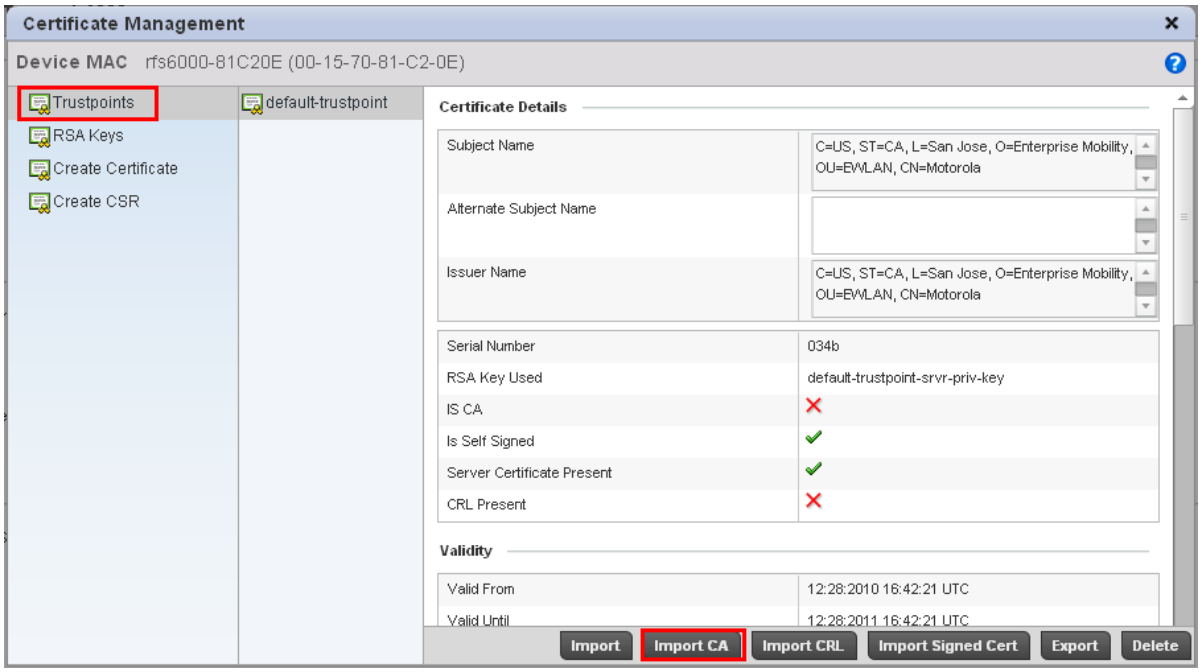
3.2.1 Web UI Configuration Example:

The following configuration example will demonstrate how to ingest a server and CA root certificate issued from a CA into a trustpoint on an RF Switch using the Web UI:

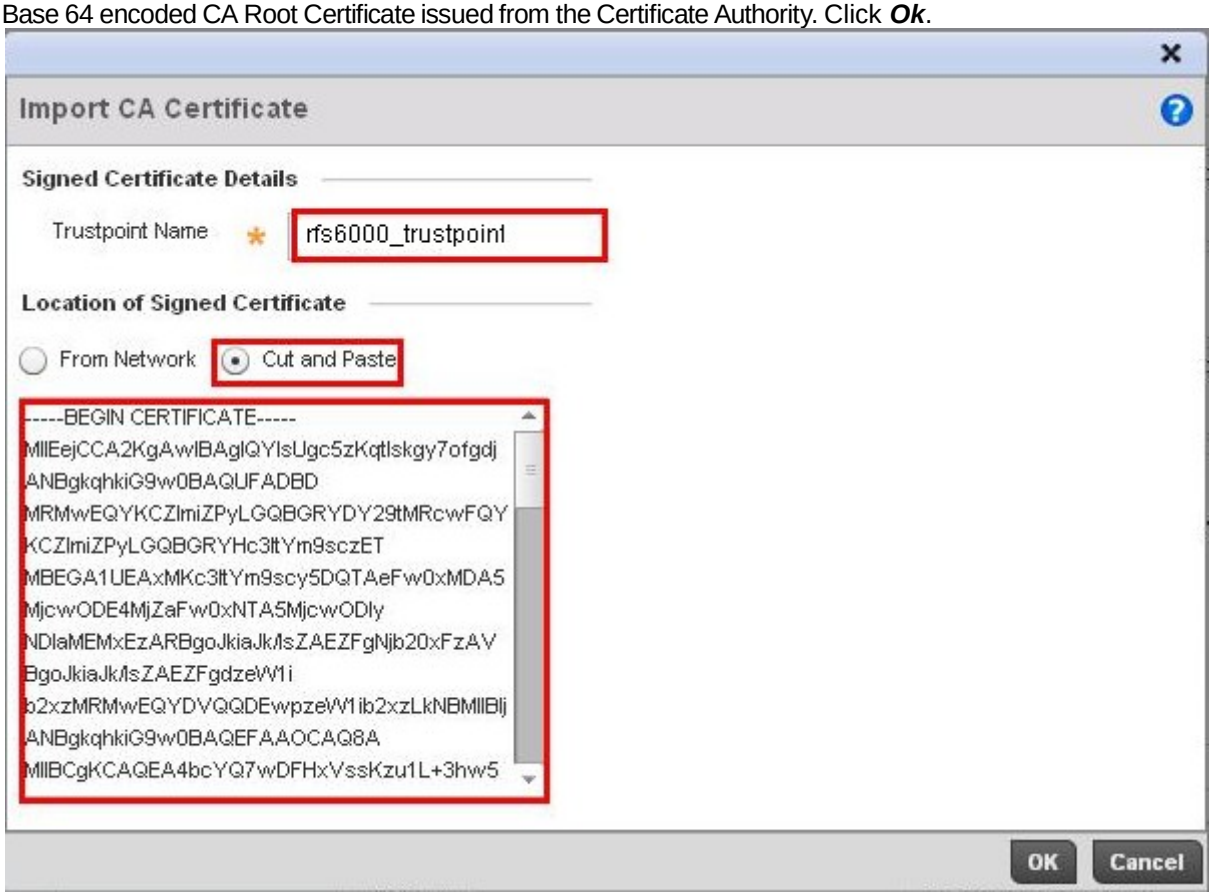
1) Navigate to the ***Configuration > Devices > RFS6000-81C2 > Certificates*** *window.* Click ***Launch Manager***.



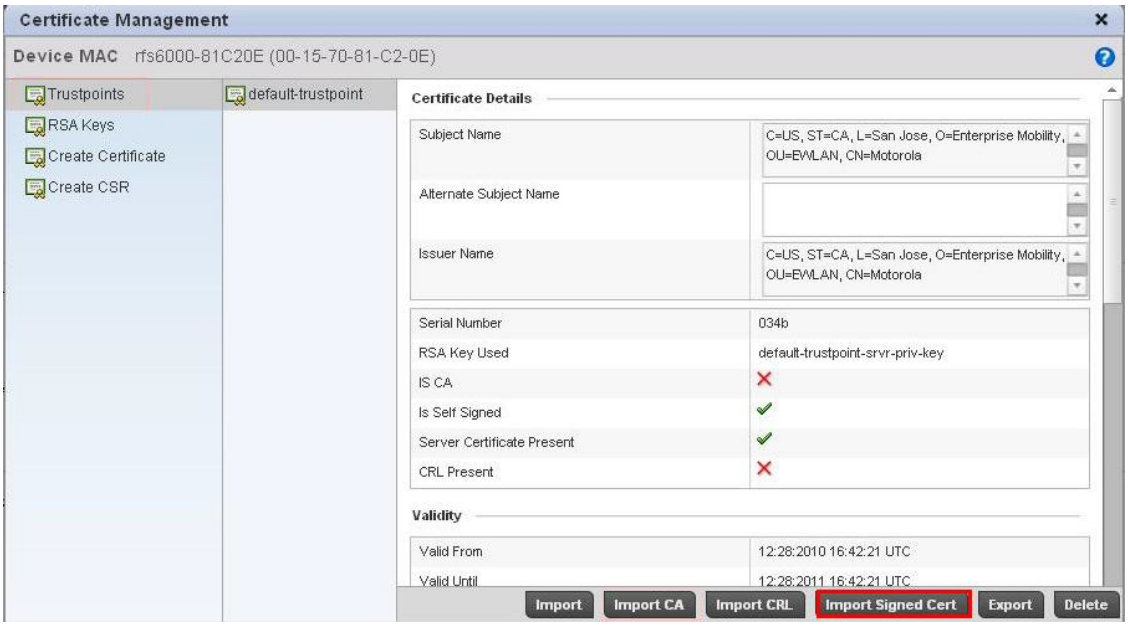
2) To create a new trustpoint, select the ***Trustpoints*** tab and click ***Import CA***.



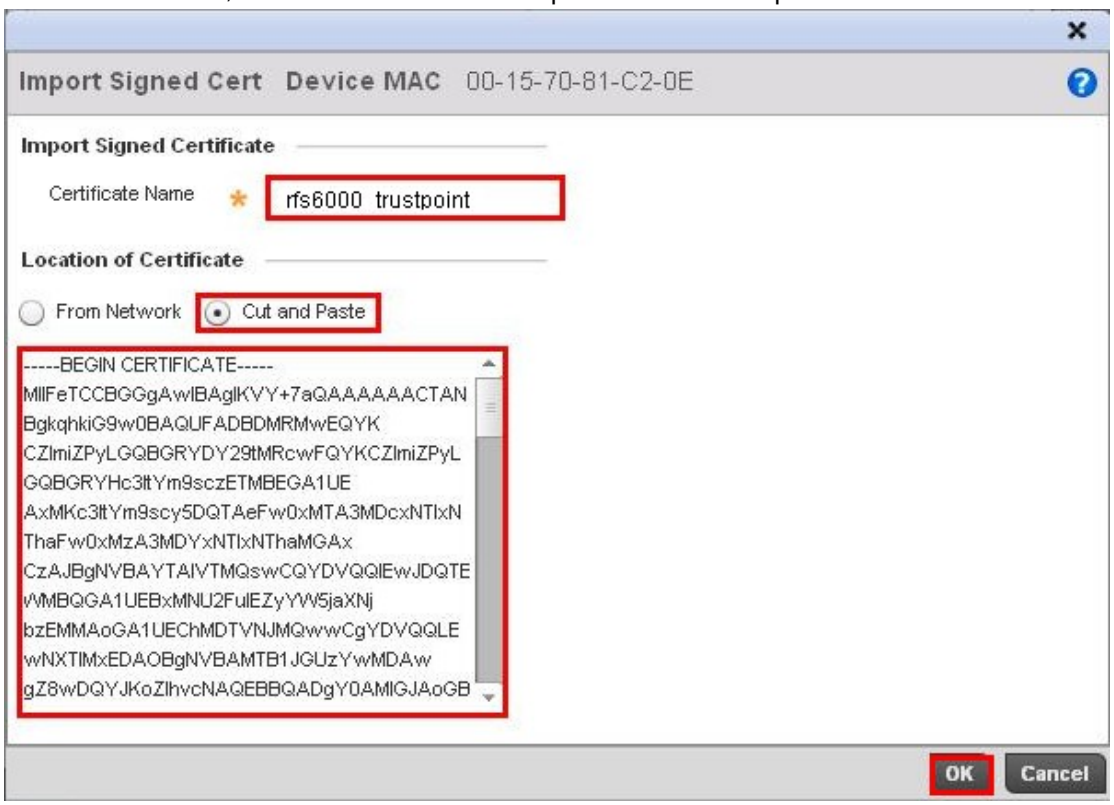
3) In the Trustpoint name enter a unique trustpoint name ***rfs6000_trustpoint*** for the trustpoint where the server certificate and the CA certificates will be associated. Select the ***Cut and Paste*** button to copy the Base 64 encoded CA Root Certificate issued from the Certificate Authority. Click ***Ok***.



4) To import the signed certificate, click ***Import Signed Certificate.***



5) In Certificate name, enter the name of the trustpoint created in step 3.



6) The ***CA Root Certificate*** and the ***signed server certificate*** is now installed in the trustpoint ***rfs6000_trustpoint***. Click ***Commit*** and ***Save*** to apply and save changes.

3.2.2 CLI Configuration:

```
// Import the CA certificate cacert.cer into rfs6000_trustpoint
rfs6000-81C20E#crypto pki authenticate rfs600_trustpoint tftp://10.106.6.143/cacert.cer

// Import the signed certificate server_cert.cer into rfs6000_trustpoint
rfs6000-81C20E#crypto pki import certificate rfs6000_trustpoint
tftp://10.106.6.143/server_cert.cer
```

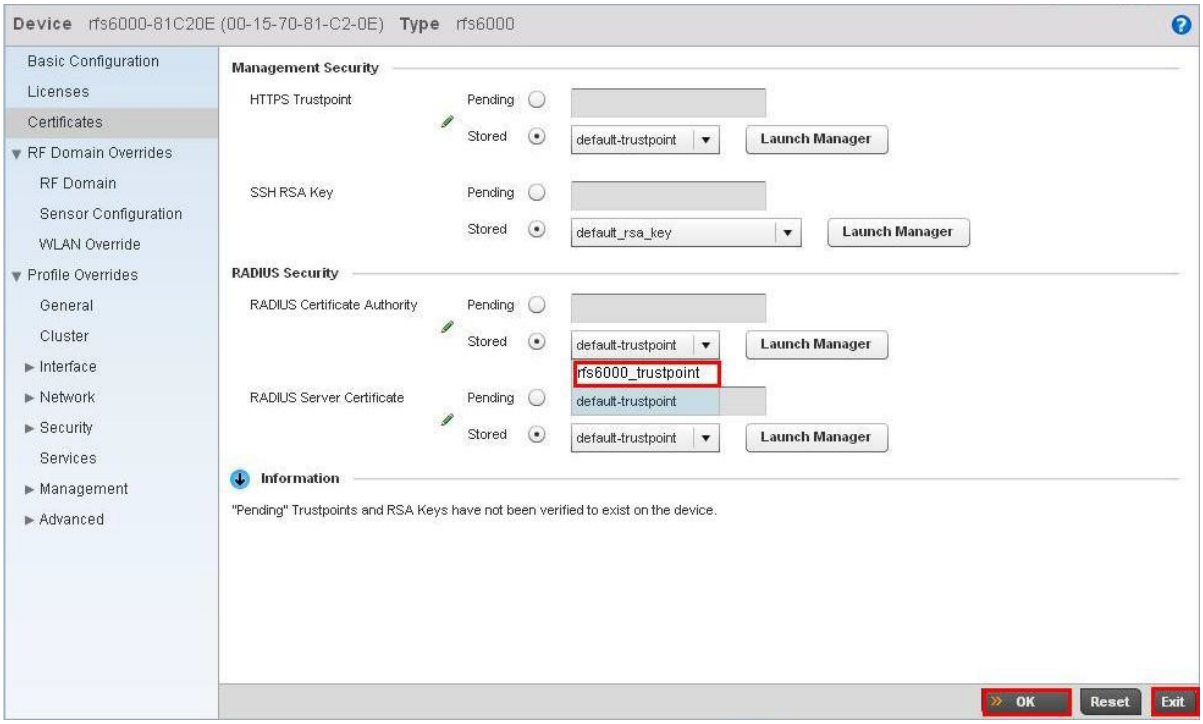
3.3 Assigning Trustpoints:

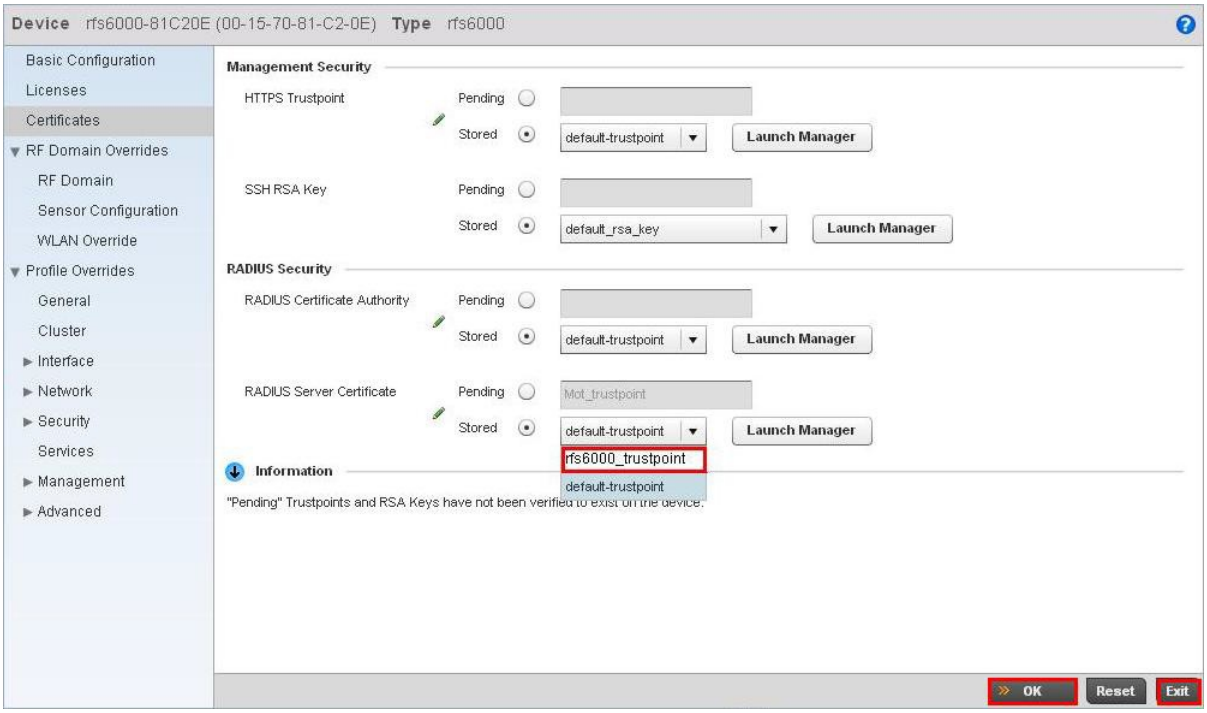
Trustpoints contain both the server and CA root certificates and can be assigned to the internal RADIUS and HTTPS services on the RF Switch. Flexibility is provided allowing the RF Switch to use a single trustpoint for management, RADIUS and Hotspot services, or two trustpoints can be used with one trustpoint servicing RADIUS and the second trustpoint servicing management and Hotspot users.

3.3.1 Web UI Configuration Example:

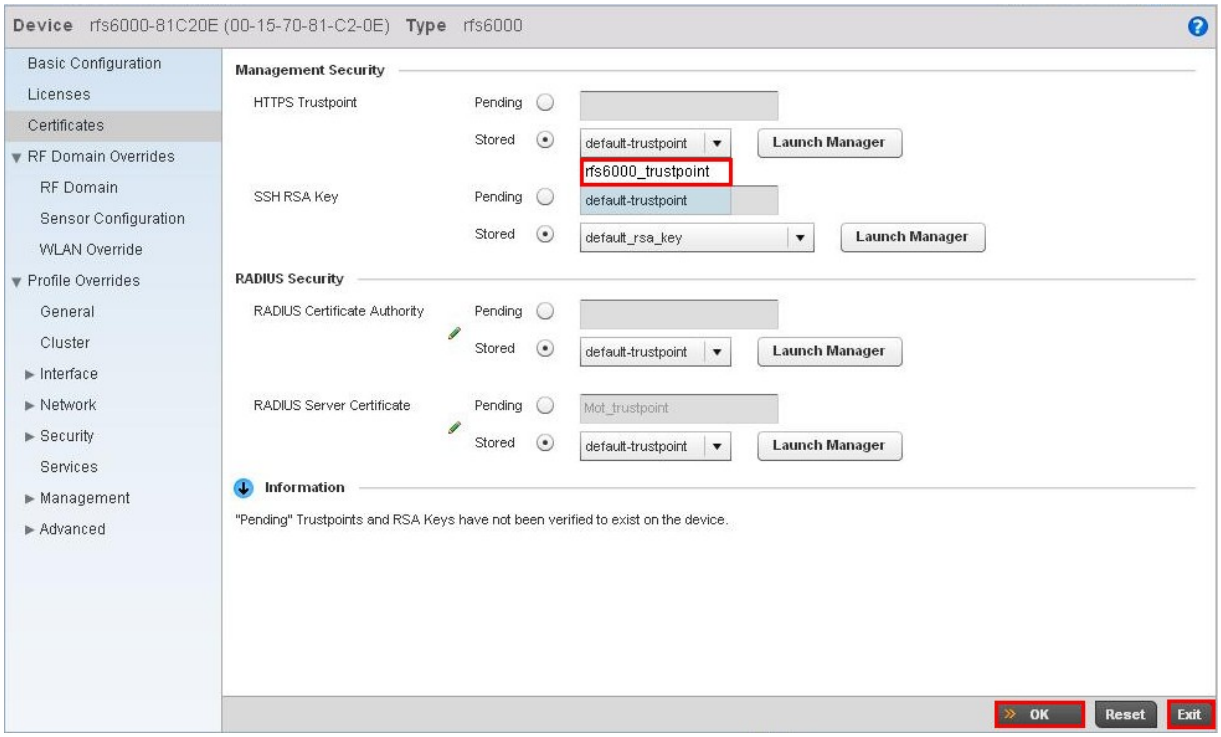
The following configuration example will demonstrate how to configure the RF Switch to use the trustpoint configured in sections 3.1 for RADIUS and HTTPS services using the Web UI:

1) Navigate to the ***Configuration > Devices > RFS6000-C20E > Certificates*** window. Select the ***rfs6000_trustpoint*** for Radius Certificate Authority and Radius Server Certificate to be used by the local RADIUS server on the device for EAP Authentication. Click ***OK*** and ***Exit***.





2) Navigate to the ***Configuration > Devices > RFS6000-C20E > Certificates*** window. Select the ***rfs6000_trustpoint*** to be used for HTTPS, for management access and Hotspot authentication. Click ***OK*** and ***Exit***.



3) Click **Commit** and ***Save*** *to* Apply and save changes.

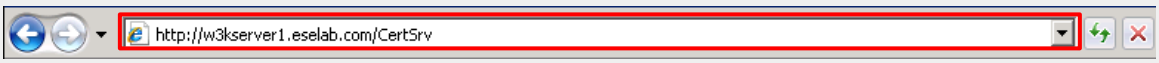
3.3.2 CLI Configuration:

```
rfs6000-81C20E*#configure terminal
        Enter configuration commands, one per line.  End with CNTL/Z.
rfs6000-81C20E(config)*#rfs6000 00-15-70-81-C2-0E
rfs6000-81C20E(config-device-00-15-70-81-C2-0E)#trustpoint ?
          https           Assign the trustpoint to HTTPS
          radius-ca       Assign the trustpoint to be used as certificate authority,
                          for validating client certificates in EAP
          radius-server   Assign the trustpoint for radius server certificate

 rfs6000-81C20E(config-device-00-15-70-81-C2-0E)#trustpoint https ?
          WORD  Trustpoint name; this should be installed on the device using PKI
                                 commands in enable mode

 rfs6000-81C20E(config-device-00-15-70-81-C2-0E)#trustpoint radius-ca  rfs6000_trustpoint
 rfs6000-81C20E(config-device-00-15-70-81-C2-0E)#trustpoint radius-server rfs6000_trustpoint
 rfs6000-81C20E(config-device-00-15-70-81-C2-0E)#trustpoint https rfs6000_trustpoint
```

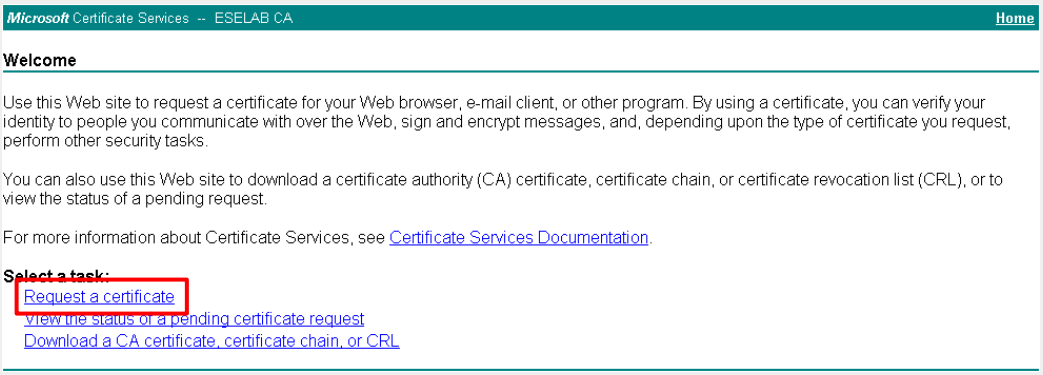
4. Microsoft CA Certificate Request:

The following demonstrates the certificate request process on a Microsoft Windows Server 2003 Enterpriser Edition Server running Microsoft Certificate Services as an Enterprise Root CA:

1) Using Microsoft Internet Explorer connect to the Certificate Services web enrollment tool and authenticate using the administrator username and password. The default URL to access the web enrollment tool is ***http://servername/CertSrv***.

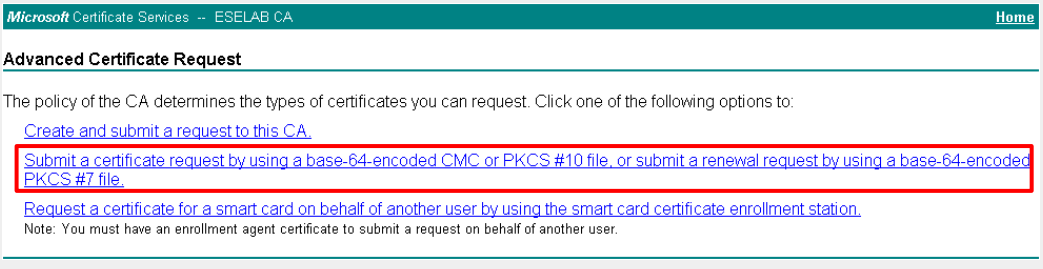


2) Select ***Request a certificate***.

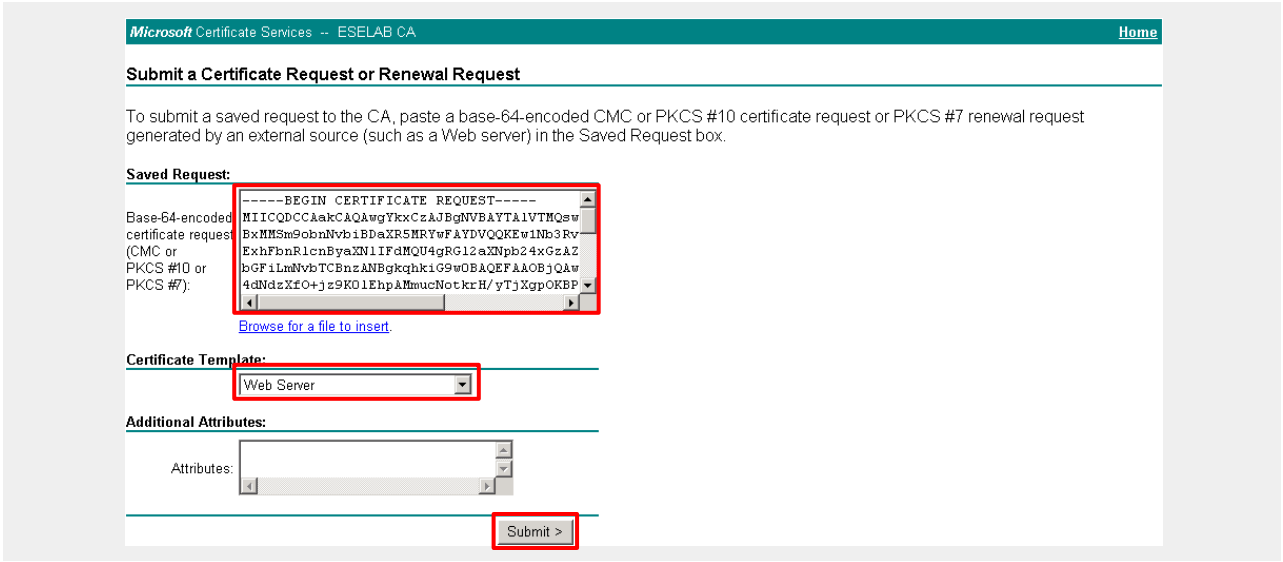


3) Select ***advanced certificate request***.

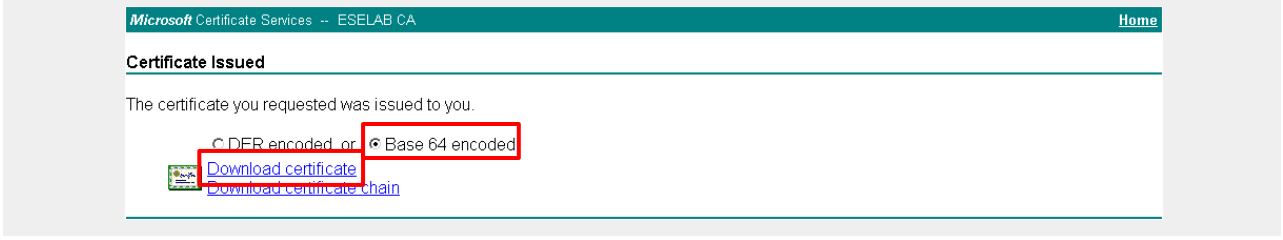
4) Select ***Submit a certificate request by using a base-64-encoded CMC or PKCS#10 file, or submit a renewal request by using a base-64-encoded PKCS#7 file***.



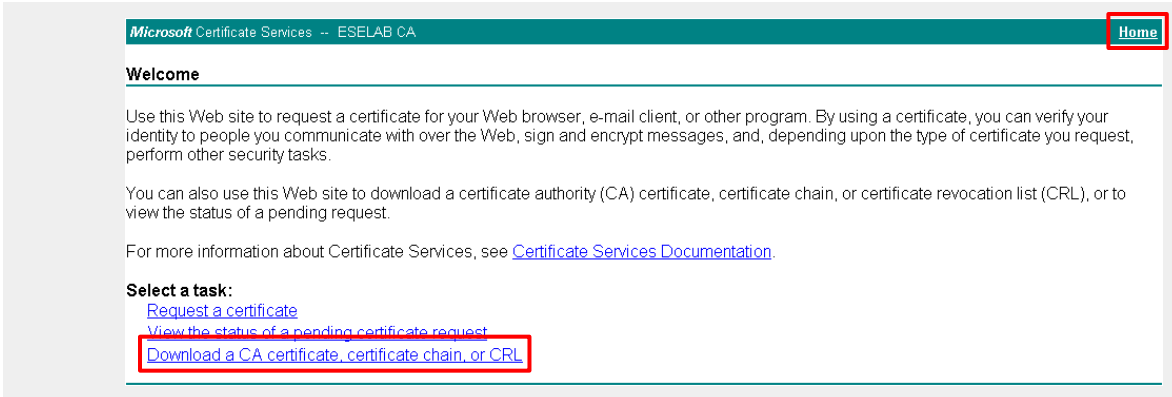
5) In the ***Base-64-encoded certificate request (CMC or PKCS#10 or PKCS#7)*** field, paste the base64 encoded text contained in the certificate request file generated by the RF Switch. In the ***Certificate Template*** window select a template to use to generate the Server Certificate. In this example a pre-installed template named ***Web Server*** is used. Click ***Submit***.



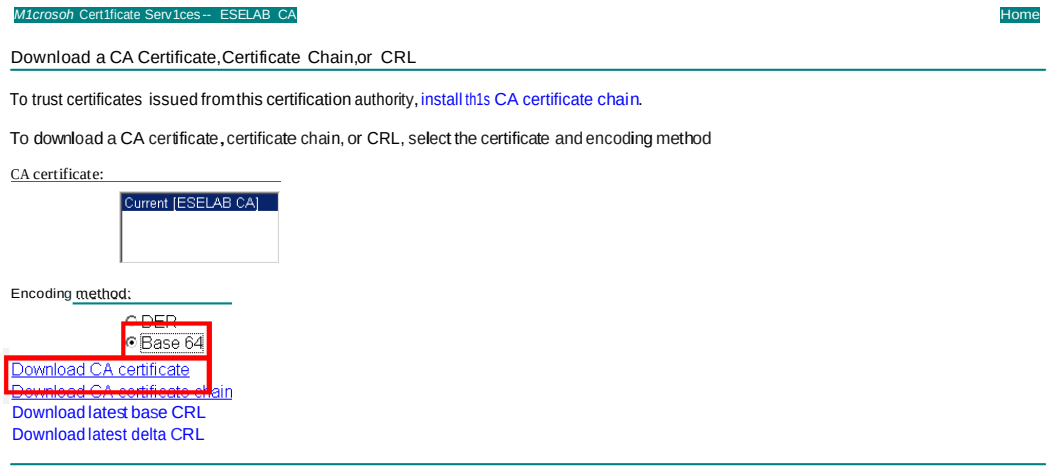
6) Select the certificate format ***Base 64 encoded*** then click ***Download certificate***. Name the certificate ***servercer.cer*** and save the Server Certificate to a location that can be easily accessed so it can be installed on the RF Switch.



7) Click ***Home*** to access the web enrollment home page then click ***Download a CA certificate, certificate chain or CRL***.



8) Select the Encoding method *Base 64* then click *Download CA certificate.* Name the certificate *caroot.cer* and save the CA Certificate to a location that can be easily accessed so it can be installed on the RF Switch.



5. Reference Documentation:

Description	Location
Zebra Solutions WiNG 5 System Reference Guide	http://support.symbol.com
Zebra Solutions WiNG 5 CLI Reference Guide	http://support.symbol.com