Technical Bulletin CS-13-06

Using custom certificates with Spectralink 8400 Series Handsets

This technical bulletin explains how to create and use custom certificates with the Spectralink 8400 Series Handset.

This technical bulletin applies to Spectralink 8400 Series handsets

Introduction

If you intend to provision the Spectralink 8400 Series Handsets with HTTPS, digital certificates must exist on the phones. Certificates issued by widely recognized certificate authorities (CAs) are pre-loaded on all Spectralink 8400 Series Handsets and a custom certificate can be added.

The trusted CAs can be found on the Trusted Certificate Authority List in the Spectralink 8400 Series Administrator's Guide at Spectralink Support under the 8400 Series Product Guide at http://support.spectralink.com.

You can create and use your own CA to issue certificates. This is done by using scripts provided by OpenSSL (http://www.openssl.org) and downloading the created files to the phone using the SSL Security menu to provide the URL of the custom certificates.

Note Make sure OpenSSL is installed and in your PATH.

This technical bulletin includes information on:

- Creating a Certificate Authority
- Issuing Certificates
- Downloading CA Certificates to Phones

Note This technical bulletin covers generating certificates with OpenSSL only. Configuration of the HTTPS server is beyond the scope of this document.

Note Every server vendor uses certificates in different ways and the server documentation should be consulted to properly configure the server.

Creating a Certificate Authority

Note You can also create a CA by using the `CA.sh` or `CA.pl` script provided by OpenSSL.

The following definitions may assist you in your understanding of the steps described below:

- A digital certificate is a certificate that uses a digital signature to bind together a public key with an identity.
- An RSA private key is one part of a key pair used to encrypt and decrypt information. RSA private key generation essentially involves the generation of two prime numbers and, because key generation is a random process, the time taken to generate a key may vary somewhat.
- Triple-DES is the algorithm used to encrypt the RSA private key.
- X.509 is an ITU Telecommunication Standardization Sector standard that specifies standard formats for certificates.

For more introductory information on public key infrastructure (PKI) and RSA keys, go to http://www.rsa.com/rsalabs/node.asp?id=2152.

To create a CA:

1. Create a RSA private key for your CA by typing the following at the command prompt:

```
openssl genrsa -des3 -out ca.key 2048
```

You will be prompted to enter a password during the command processing and each time the CA is used to generate and sign a new server certificate.

The key is output to the **ca.key** file.

2048 is the key size.

You can see the details of this RSA private key by typing the following command:

```
openssl rsa -noout -text -in ca.key
```

2. Backup the **ca.key** file and make note of the password you entered in step 1 at a secure location.
3. Create a self-signed CA certificate with the RSA private key by typing the following command:

```
openssl req -new -x509 -days 2555 -key ca.key -out ca.crt
```

You will be prompted to enter the password you entered in step 1.

You will also be prompted to enter the following:

- Country — US, for example
- State or Province — Colorado
- Locality (city or town) — Boulder
- Organization Name — Spectralink Corporation
- Organizational Unit Name — Service
- Common Name — Root CA
- E-mail address — admin@spectralink.com

The certificate is output to the **ca.crt** file.

The created certificate expires in 2555 days or seven years. The default value is 365 days if not specified.

Warning Make the CA certificate's lifetime in accordance with your organization's certificate policy statement (CPS). The longer the lifetime the less often you will need to reissue certificates to your company's phones.

You can see the details of this certificate by typing the following command:

```
openssl x509 -noout -text -in ca.crt
```

Issuing Certificates

The following definitions may assist you in your understanding of the steps described below:

- A certificate signing request (CSR) for the boot server is signed by the CA you created in the previous section.
- A server certificate, issued to the boot server, can be used to authenticate itself to the phone when new software needs to be downloaded or log files uploaded.

Note The following steps should be performed on the boot server except where noted.

Warning Do not transmit the server key (created in the following procedure) between servers. Copy the CSR to the CA signing server only.

To issue a server certificate:

1. Create a RSA private key for your boot server by typing the following at the command prompt:

```
openssl genrsa -out server.key 2048
```

The key is output to the **server.key** file.

2048 is the key size.

You will be prompted to enter a password. The password entry is optional, however it is more secure if you use one.

2. Backup the **server.key** file at a secure location.
3. Create a CSR with the server RSA private key by typing the following command:

```
openssl req -new -key server.key -out server.csr
```

You will also be prompted to enter information similar to that requested for the CA.

Warning

The 'Common Name' must match the name supplied as the boot server. In other words, if the 'Common Name' is a fully qualified domain name (FQDN), then the boot server as defined through the phone's user interface or by DHCP must be a matching FQDN. This is because the phone's application does not perform a DNS lookup (forward or reverse), only a simple string comparison.

For example, bootserver1.spectralink.com is a FQDN. The use of an IP address is also valid here.

4. On the CA server, issue the server certificate by typing the following command:

```
openssl x509 -days 365 -CA ca.crt -CAkey ca.key -req -
CAcreateserial -CAserial ca.srl -in server.csr -out server.crt
```

The certificate is output to the **server.crt** file.

The created certificate expires in 365 days. This is the default value if not specified.

When you use this command to issue more certificates, omit the `-Cacreateserial` option.

You can view your issued certificate with by typing the following command:

```
openssl x509 -text -in server.crt | more
```

The Issuer and Subject in the certificate should not be the same.

Downloading CA Certificates to Phones

You must now add the certificate of your Root CA generated to the phone, specifically the **ca.crt** file.

To load the Root CA certificate on the phone:

1. Select **Settings>Advanced**.
2. Enter the Administrator's password.

The default password is 456.

3. Select **Administration Settings>TLS Security>Custom CA Certificates**.
4. Select **Install Custom CA Certs>Configure CA Cert...**
5. Enter the URL for the certificate and press the **Enter** soft key.

For example:

```
http://bootserver1.spectralink.com/ca.crt
```

or

```
ftp://PlcmSpIp:PlcmSpIp@bootserver1.spectralink.com/ca.crt
```

You can edit the 'http://' portion of the URL. All character are entered as lower case.

The certificate loads onto the phone.

6. Select **Configure TLS Profiles,** select the profile you installed the certificate into.
7. Select **CA Certificate** then select **All Certificates**, and then press the **End** key.

The phone now includes the custom certificates when doing its verification.

Trademarks

Disclaimer

While SpectraLink uses reasonable efforts to include accurate and up-to-date information in this document, SpectraLink makes no warranties or representations as to its accuracy. SpectraLink assumes no liability or responsibility for any typographical or other errors or omissions in the content of this document.

Limitation of Liability

SpectraLink and/or its respective suppliers make no representations about the suitability of the information contained in this document for any purpose. Information is provided "as is" without warranty of any kind and is subject to change without notice. The entire risk arising out of its use remains with the recipient. In no event shall SpectraLink and/or its respective suppliers be liable for any direct, consequential, incidental, special, punitive or other damages whatsoever (including without limitation, damages for loss of business profits, business interruption, or loss of business information), even if SpectraLink has been advised of the possibility of such damages.

Customer Feedback

We are constantly working to improve the quality of our documentation, and we would appreciate your feedback. Please send email to info@SpectraLink.com.

Technical Support

Visit support.SpectraLink.com for software downloads, product document, product licenses, troubleshooting tips, service requests, and more.