HOW TO CREATE SELF-SIGNED SERVER AND DEVICE CERTIFICATES FOR WEBLINK (WEBSOCKETS) CONNECTIONS

This article demonstrates the steps to create and sign a server certificate or a printer (device) certificate.

ISSUE / QUESTION

How can I use self-signed server and device certificates rather than a Zebra signed ones for weblink connections?

APPLICABLE TO

Server applications using a Link-OS printer weblink connection.

RESOLUTION / ANSWER

By default, a printer running Link-OS comes supplied with a generic Weblink device certificate and Zebra server certificate authority. These certificates can be used for connecting to a Weblink (Websockets) server with a Zebra signed server certificate. Starting with Link-OS v5, it is possible to supply and use your own certificates.

This article shows you the steps to create and sign a server certificate yourself and optionally printer (device) certificates. See our *PrintSecure Administration Guide* available at www.zebra.com/printsecure (https://www.zebra.com/printsecure) for further information and details on how certificates can be deployed to printers. As there are many application servers available, configuring the certificates on your server is beyond the scope of this article.

Requirements

- The latest version of OpenSSL, downloaded from the OpenSSL website (https://www.openssl.org/source/).
- All Zebra printers must be running Link-OS 5.2 or later.

NOTE The steps in this article were performed using OpenSSL 1.1.1d on a Windows 10 operating system.

Determine the Link-OS Version Running in Your Printer

- Send the following command to your printer to determine the Link-OS version that the printer is running.

```
{}{"appl.link_os_version" : null}
```

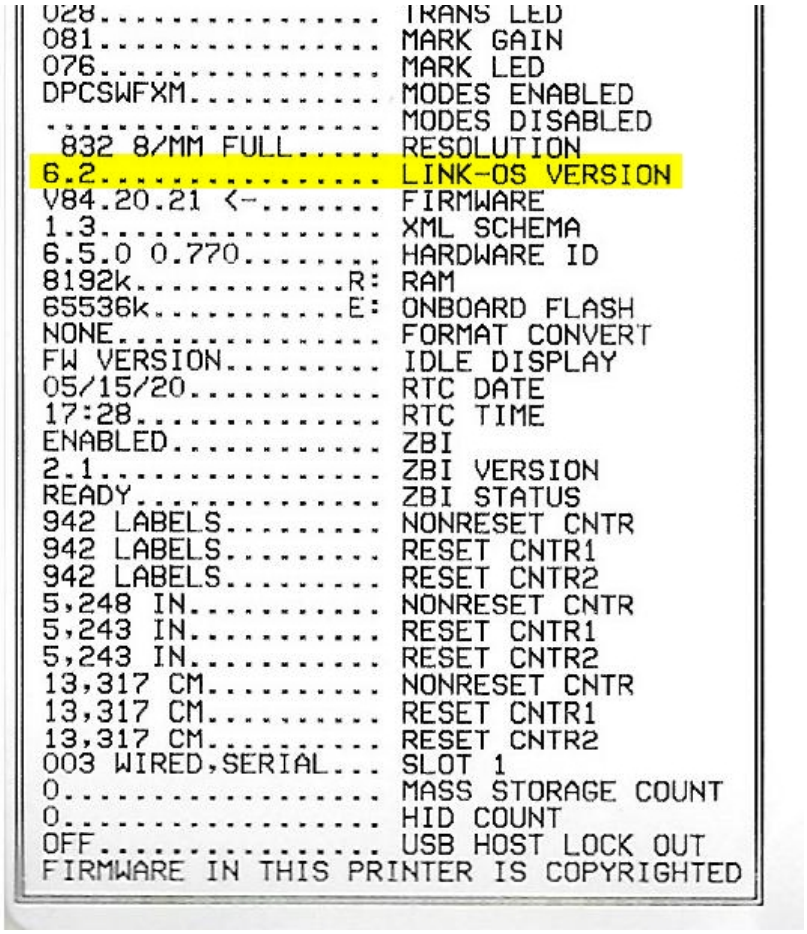
The printer will return the Link-OS version in the following format:

```
{"appl.link_os_version":"6.3"}
```

- Zebra Setup Utilities for Windows (http://www.zebra.com/setup) can be used to send the command above and receive the response. For more details on how to use the Communication Windows, read this article: Zebra Setup Utilities - Sending Printer Commands and Receiving Data (/s/article/Zebra-Setup-Utilities--Sending-Printer-Commands-and-Receiving-Data)

richText.RichText.getParsedRichTextValue=1&ui-communities-components-aura-components-forceCommunity-seoAssistant.SeoAssistant.getSeoData=1).

- The Configuration Label printout also reports the Link-OS version as shown below:



Create and Sign a SHA-256 Server Certificate

Refer to the OpenSSL documentation (https://www.openssl.org/docs/) for a more detailed command explanation where necessary.

1. Create a new folder (for example, "zebra-certs").
2. Open a Command Prompt using **Run as Administrator** and navigate to the folder created in step 1. Execute the following commands:

```
mkdir demoCA\newcerts
mkdir demoCA\private
echo 1000 > .\demoCA\serial"
copy nul .\demoCA\index.txt
echo basicConstraints=critical,CA:true > constraints.cnf
echo basicConstraints=critical,CA:false > constraints-noca.cnf
```

3. Create self-signed root by using the following two OpenSSL commands:

```
openssl req -new -keyout "ROOTNAME.key" -sha256 -out "ROOTNAME.csr" -verify -subj "/C=xx/ST=yyyy/L=zz
openssl ca -days cccc -out "ROOTNAME.crt" -keyfile "ROOTNAME.key" -batch -extfile constraints.cnf -in
```

```
Where
  xx: 2-character country code
  yyyy: State name
  zzzz: City name
  aaaa: Organization
  bbbb: The name of your root certificate (ROOTNAME)
  cccc: Number of days to certify the certificate for
```

4. Create a server CSR by using the following OpenSSL command:

```
openssl req -newkey rsa:2048 -new -keyout "SERVERNAME.key" -sha256 -out "SERVERNAME.csr" -verify -sub
```

```
Where the letter variables are defined in step 3, and
  dddd: The actual FQDN of your server (e.g. "weblink.mydomain.com (http://weblink.mydomain.com)")
```

5. Sign it with the root by using the following OpenSSL command:

```
openssl ca -days cccc -md sha256 -out "SERVERNAME.crt" -keyfile "ROOTNAME.key" -cert "ROOTNAME.crt" -
```

```
Where
  cccc: Number of days to certify the certificate for
```

This should produce an output similar to the following:

```
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4097 (0x1001)
        Validity
            Not Before: Apr 23 19:26:32 2020 GMT
            Not After : Jul 22 19:26:32 2020 GMT
        Subject:
            countryName               = XX
            stateOrProvinceName       = XXXXXXXX
            organizationName          = XXXXX
            commonName                = XXXXXXXX
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
Certificate is to be certified until Jul 22 19:26:32 2020 GMT (90 days)

Write out database with 1 new entries
Data Base Updated
```

You now have a self-signed server certificate.

6. Execute the following command to create the CA file that will be deployed to all your printers.

```
copy ROOTNAME.crt WEBLINK1_CA.NRD
```

IMPORTANT! The filename must correspond to the weblink connection you are using (weblink ip conn[1|2] location).

- Use WEBLINK1_CA.NRD if you are using weblink ip conn1 location.
- Use WEBLINK2_CA.NRD if you are using weblink ip conn2 location.

NOTE The printer must be restarted after deploying any WEBLINKx.NRD files for them to take effect.

7. Add your root CA from step 3 to your trust store.
8. Continue with the following steps if mutual authentication is enabled in your environment.

NOTE Although optional, Zebra strongly recommends the use of mutual authentication, especially if there is any sensitive data that resides, or is used by the Weblink server. This implies that the Zebra device and the Weblink server both have certificates they use to authenticate each other and prevent unrecognized devices and servers from connecting.

On Tomcat this can be enabled by modifying the server.xml configuration file and setting clientAuth="true".

When mutual authentication is enabled, every device that connects to a Weblink server must have a certificate to identify itself with the server that the server can trust.

9. If you are *not* using your own device certificates, the Zebra device (printer) certificate will be used and so it is necessary to import the following Zebra CA certificates into your trust store. If you wish to use your own device certificates, continue to step 10.

    Zebra Root.crt
    AIT.crt
    Printer.crt

    Click this link (http://www.zebra.com/content/dam/zebra_new_ia/en-us/knowledge-articles-community/000019334/Zebra CA Certificates.zip) to download the Zebra CA certificates listed above.

Create and Sign a SHA-256 Device Certificate

10. Create a device CSR by using the following OpenSSL command.

NOTE While a general device certificate can be deployed to all printers with care, unique device certificates are recommended.

```
openssl req -newkey rsa:2048 -new -keyout "PRINTER.key" -out "PRINTER.csr" -verify -subj "/C=xx/ST=yy
```

```
Where the letter variables are defined in step 3.
```

11. Sign it with the root by using the following OpenSSL command:

```
openssl ca -days cccc -out "PRINTER.crt" -keyfile "ROOTNAME.key" -cert "ROOTNAME.crt" -batch -extfile
```

```
Where
  cccc: Number of days to certify the certificate for
```

12. Execute the following commands to create the files that will be deployed to all your printers.

```
copy PRINTER.crt WEBLINK1_CERT.NRD
copy PRINTER.key WEBLINK1_KEY.NRD
```

IMPORTANT! The filename must correspond to the Weblink connection you are using (weblink.ip.conn[1|2].location).

- Use WEBLINK1_CERT.NRD and WEBLINK1_KEY.NRD if you are using weblink.ip.conn1.location
- Use WEBLINK2_CERT.NRD and WEBLINK2_KEY.NRD if you are using weblink.ip.conn2.location

NOTE The printer must be restarted after deploying any WEBLINKx.NRD files for them to take effect.

RELATED ARTICLES

PowerPrecision Console and Device Tracker with Self-Signed Certificate Installation (/s/article/PowerPrecision-Console-Device-Tracker-with-Self-Signed-Certificate-Installation) 138

Installing the ZDVC 2.3.1 with Self-signed Certificates (/s/article/installing-zvdc-with-self-signed-certificates) 80

Remote Desktop Connection Troubleshooting and Terminal Services Server Common Issues and Fixes (/s/article/Remote-Desktop-Connection-Troubleshooting-and-Terminal-Services-Server-Common-Issues-and-Fixes) 33.73K

Enabling Logging on a Link OS Weblink compatible printer (/s/article/Enabling-Logging-on-a-Link-OS-Weblink-compatible-printer) 1.08K

How do i check if my certificate is SHA2 or SHA256 based? (/s/article/How-do-i-check-if-my-certificate-is-SHA2-or-SHA256-based) 3.74K

Didn't find exactly what you're looking for?

SUBMIT A CASE

Site Feedback