THALES

payShield 10K

GENERATING & INSTALLING TLS CERTIFICATES

CPL Technical Training

Revision History

Revision	Date	Reason
A	5 June 2023	Initial release

Trademarks, Copyrights, and Third-Party Software

CPL Technical Training Documentation

The information contained in this document is intended solely for your personal reference and for learning purposes and is provided AS IS and with no warranties. Such information is subject to change without notice, its accuracy is not guaranteed, and it may not contain all material/information concerning Thales (the 'Company'). The Company makes no representation regarding, and assumes no responsibility or liability for, the accuracy or completeness of, or any errors or omissions in, any information contained herein. The Company may update or supplement the information at any time. In addition, the information contains projections and forward-looking statements that may reflect the Company's current views with respect to future events. These views are based on current assumptions which are subject to various risks and which may change over time.

Disclaimer

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

This document to be solely used for informational, non-commercial, internal and personal use only provided that: (a) The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies; (b) document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made; and (c) is not relied upon for any other reason other than use described above. Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Contents

This document covers how to generate and install TLS certificates for the HOST Port on payShield 10k using OpenSSL on Microsoft Windows.

Open SSL Installation and Configuration

1. Use the freely available OpenSSL to generate a CA. You can obtain a compiled version from: https://slproweb.com/products/Win32OpenSSL.html

   Use the following version: Win64 OpenSSL v3.1.0 Light on Windows 10 x64
2. Perform the installation using the default options.
3. Open a command line with elevated privileges, go to the default path where you find the binary of OpenSSL (C:\Program Files\OpenSSL-Win64\bin\).
4. Create a subdirectory to store your certificates and keys; name it **PC** (mkdir PC, to create it).
5. Create a file called **v3.ext** under the subdirectory PC containing the following lines:

```
authorityKeyIdentifier=keyid,issuer

basicConstraints=CA:FALSE

keyUsage = digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment
```

> **What is the purpose of step 5 above?** If this file extension is not used when creating the client certificate and payShield host port certificate, OpenSSL generates them in version v1 instead of version v3. payShield will not install certificates with version v1! Only v3 certificates are accepted.
>
> The other two essential parameters are **nonRepudiation** and **dataEncipherment** for client certificates to work with payShield.

Generating Certificates

1. Generate the CA key by entering the command:

   ```
   openssl genrsa -out PC\CADISprivate.key 2048
   ```

2. Generate the self-signed certificate for the CA, by entering the command:

   ```
   openssl req -new -x509 -key  PC\CADISprivate.key -out PC\CADIS.crt -days 365
   ```

3. Connect to the payShield Console or Virtual Console to obtain the certificate signing request.

   You need to be in **Secure mode** and issue the command SG

   > **NOTE:** If you are using the virtual console, reply NO when asked to save the certificate request, otherwise payShield tries to save it on a USB stick connected to the USB-A port on the rear of the appliance (generally used for printers).

4. Copy the command output and save it in a file with the extension **CSR** under the **PC** directory.
   For example: **10kDIS.csr**

5. Sign the payShield certificate request using the CA:

   ```
   openssl x509 -req -in PC\10kDIS.csr -CAcreateserial -extfile PC\v3.ext -out
   PC\10kDISv3.crt -days 365 -CA PC\CADIS.crt -CAkey PC\CADISprivate.key
   ```

Generating the Client Certificate

1. Create the KEY for your client and the certificate signature request:

   ```
   openssl genrsa -out PC\laptopPrivate.key 2048
   ```

   ```
   openssl req -new -key PC\laptopPrivate.key -out PC\laptopDIS.csr
   ```

2. Sign the request using your CA:

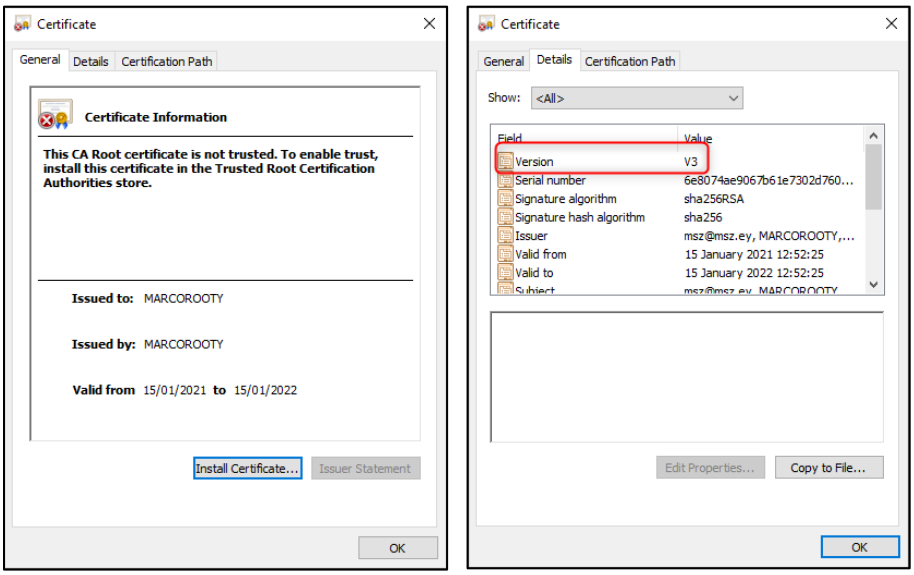
   ```
   openssl x509 -req -in PC\laptopDIS.csr -CA PC\CADIS.crt -CAkey
   PC\CADISprivate.key -CAcreateserial -extfile PC\v3.ext -out PC\laptopDISv3.crt
   ```

Verifying Certificates

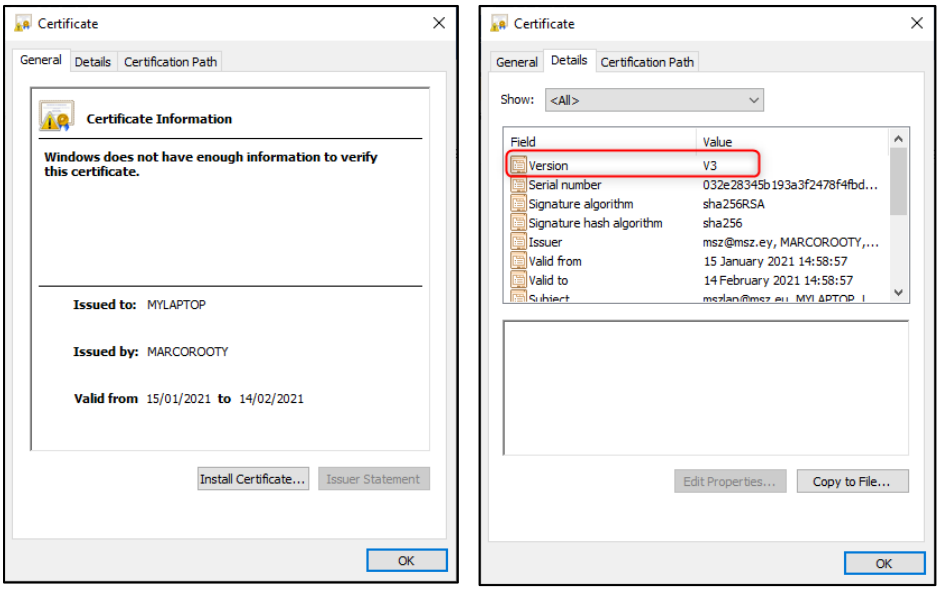
In this section, you will verify that all your certificates are version v3.

1. Double-click the CRT files. They should appear as in the images below.

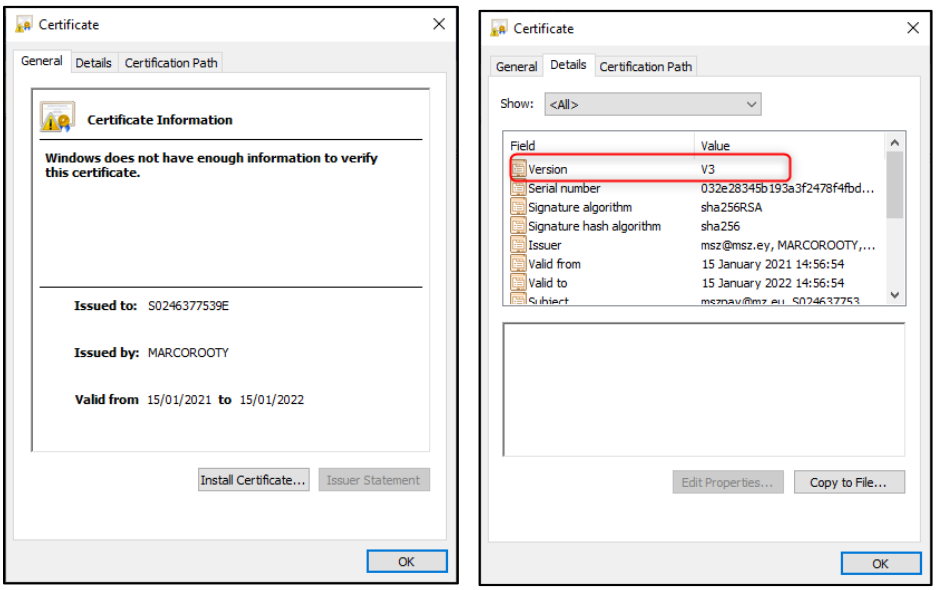
CADIS.CRT



10KDISv3.CRT



laptopDISv3.CRT



Installing Certificates on payShield

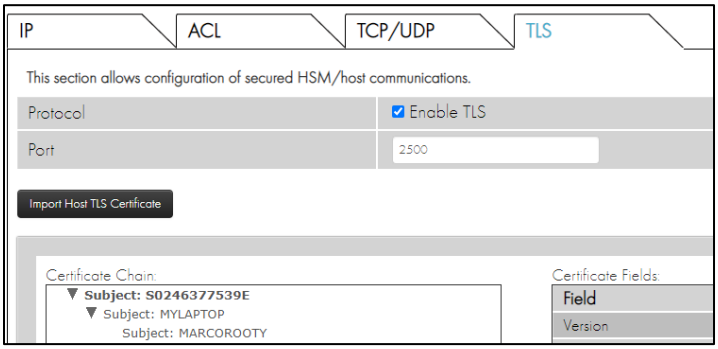
In this section, you will install certificates on payShield using the payShield Manager.

1. Log in using both the **L** and **R RACC** cards, and then enter Secure mode.
2. Go to **Configuration> Host Settings> TLS**, enable **TLS**, and then click **Import Host TLS Certificate**.

3. Import the certificates one by one in the following order:
   - **CADIS.crt** - your CA
   - **10kDISv3.crt** - the appliance certificate signed using your CA
   - **laptopDISv3.crt** - the client certificate signed by your CA

> **NOTE:** Every time a certificate is imported, you must reconnect to the payShield Manager.

4. After installing the last certificate, reconnect to the appliance, go to **Configuration> Host Settings> TLS**. If the certificates are installed correctly, you should see this:



Using the payShield Console or Virtual Console

1. Format a USB stick using the FAT file system (not ext3 or NTFS).
2. Copy all the **.CRT** files onto the USB stick.
3. Plug the USB stick into the USB-A port at the back of the appliance.
4. Enter Secure mode and issue the `SI` command.
5. Import the files in the following order:
   - **CADIS.crt** - your CA
   - **10kDISv3.crt** - the appliance certificate signed using your CA
   - **laptopDISv3.crt** - the client certificate signed by your CA
6. Use the `SV` command to verify that the certificates have been installed correctly. Remember to remove the USB stick from the port.

How to Test the TLS Host Connection

Using PayShieldPressureTest

> **PayShieldPressureTest** is a free Open Source tool written in Python to test the host port connectivity and to create a workload on the payShield 10k and 9k.

> The tool is freely available here: https://github.com/mszeu/PayShieldPressureTest

> A binary version for Microsoft Windows is also available on the same page.

> To test the connectivity, enable the host command **B2** and use the tool with the following parameters:

```
pressureTest.exe 192.168.0.36 --proto tls --keyfile PC\laptopPrivate.key  --
crtfile PC\laptopDISv3.crt --port 2500 --times 1 --b2 --echo TEST
```

If all is ok, the expected output is similar to the following:

Return code: 00 No error

Command sent/received: B2 ==> B3

sent data (ASCII) : HEADB20004TEST

sent data (HEX) : 000e484541444232303030454455354

received data (ASCII): HEADB300TEST

received data (HEX) : 000c48454144233303054455354DONE

Using OpenSSL

> Test if the connection can be established correctly through TLS with payShield. Use OpenSSL with the following parameters:

```
openssl s_client -connect 192.168.0.36:2500 -CAfile pc\CADIS.crt -key
pc\laptopPrivate.key -cert pc\laptopDISv3.crt -debug
```

> Verify that the certificate chain displayed is ok and that there are no evident errors.

The output should look similar to this:

```
SSL handshake has read 4232 bytes and written 2936 bytes
Verification: OK
---
New, TLSv1.2, Cipher is DHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : DHE-RSA-AES256-GCM-SHA384
    Session-ID: C2CD4159B669DED54FF57858C5F81D015B627744CEE2FD2E72BAE3D073B142F8
    Session-ID-ctx:
    Master-Key: BEA8EABE308FEE8EF2CE225949C1718B3E03AA9D83EECC34E333979C299C1B9A9530240368DD9C305F38F75F866E78CF
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 7200 (seconds)
    TLS session ticket:
    0000 - bc e2 9d 3a f2 e9 bc c5-58 0e 7c fe 9c ef 03 ee   ...:....X.|.....
```

```
   Start Time: 1684323590
   Timeout   : 7200 (sec)
   Verify return code: 0 (ok)
   Extended master secret: yes
---
```

If all is ok, the connection is established. To terminate it and return to the command prompt, press Ctrl-C.