**Certification**

[SSL Description](#_SSL_Description) **----------------------------------------------------------------------------------------------------------1**

[**KeyStore and Trust Stroe configuration**](#_How_to_check) **------------------------------------------------------------------------------2**

[**How to check the expiry date time for the SSL certificate**](#_How_to_convert) **------------------------------------------------------3**

[**How to convert the .ca certificate to JKS file**](#_How_to_convert) **-----------------------------------------------------------------------4**

# SSL Description

we have two different types of mutual Authentication.

1. One way SSL
2. Two-way SSL

🡪In Service side we use key store (listener)

🡪In client side we use Trust Store (Requester)

For one-way SSL we only use service side certificate (KeyStore)

For Two-way SSL we use Both Certificate (KeyStore & Trust Store)

# **How to check KeyStore and Trust Stroe configuration details**

Step1: -

Keystore Explore Tool, which is available from Google, is required to examine the

certificate information.

Step2: - once install KeyStore Explore Tool in the machine click on the open an existing KeyStore.

A screenshot of a computer

Description automatically generated

->Now select the certificates

-> provide the password to open the certificate

->now we can be able to see the certificate details as below and in the same screenshot we can

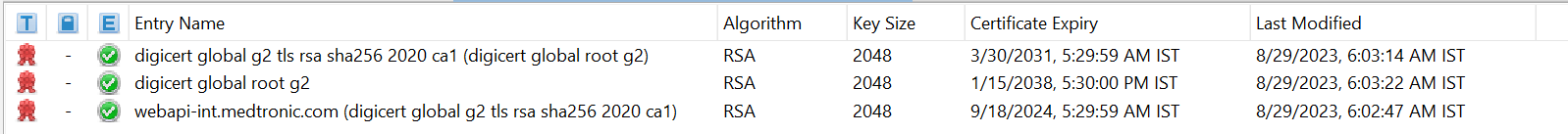
see the time of certification modified and certification Expiry.

Example: - KeyStore

A screenshot of a computer

Description automatically generated

Example: - Trust Store



**Trust Store Configuration details in the KeyStore**

Click on the key store certificate.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**🡪** In the Above screenshot we can be able to see the root and leaf certificates.

once you click the one-by-one certificate, we can be able to see the certificate details.

* If the same details were matching with the trust certificate, then the certificates were valid.

# **How to check the expiry date time for the SSL certificate on the google.**

**🡪** How to check the expiry date time for the SSL certificate on the google

Step 1: - Key Store Explorer from google.

Step 2: - upload the certificate, now we can be able to see the expiry of the certificate.

**🡪** search the host in the google exp: - “test.login.medtronic.com"

* Then click on the lock button as below.

A close-up of a website

Description automatically generated

* Click on the **connection is secure** -> certification **is valid.**

A screenshot of a computer

Description automatically generated

* Now in general we can see the certificate details like expiry date issue date host name

A screenshot of a certificate

Description automatically generated

# **How to convert the .ca certificate to JKS file**

* Search the Host Name on the google.
* Click on the lock icon on the tool bar.
* Click on the **connection is secure** -> certification **is valid**
* In Detail section we can see the certificate Hierarchy

1---> Root certificate

2---> mid certificate

3---> Leafe certificate

A screenshot of a computer

Description automatically generated

🡪 Now select the certificate you want to export and click on the Export Button Below (4)

🡪Once you download the certificate, we can see the certificate as below

A screen shot of a computer

Description automatically generated

🡪Now use the below commands to convert the certificate (.ca) to the jks

* cert conversion: keytool -import -v -trustcacerts -alias mule -file C:\Users\jayark4\Documents\wmcloud-int-it2.medtronic.com.cer -keystore wmcloud-int-it2.medtronic.com.jks