THALES

TLS certificate loading tool

For EXSx2/TXx2/PLSx3/ELS62

www.thalesgroup.com

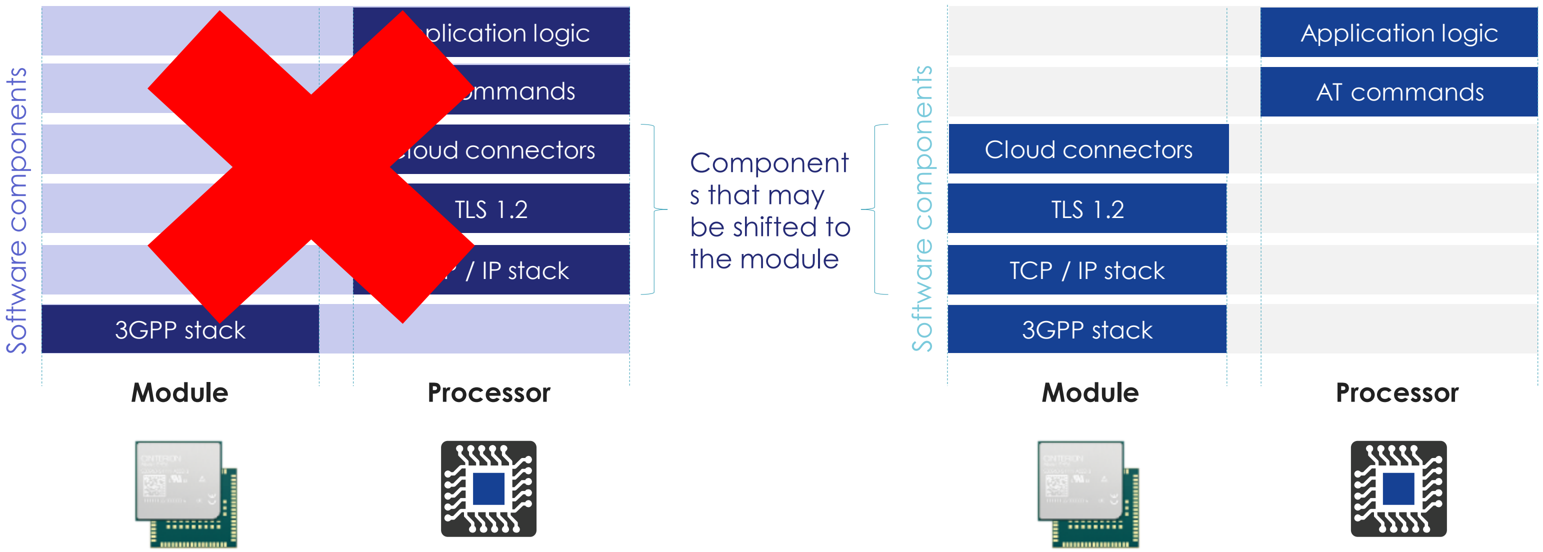
Agenda

- Server/Client certificate loading – unsecure mode
- Management certificate (required for secure mode)
- Server/Client certificate loading – secure mode
- Establish a secure connection
- Application certificate loading

Target group

Classical approach

Cinterion IP services



Software components

plication logic

mmands

loud connectors

TLS 1.2

/ IP stack

3GPP stack

Module

Processor

Components that may be shifted to the module

Software components

Application logic

AT commands

Cloud connectors

TLS 1.2

TCP / IP stack

3GPP stack

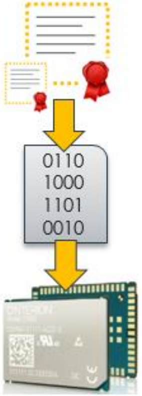
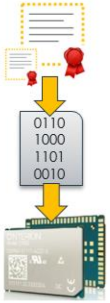
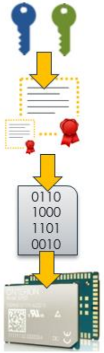
Module

Processor

General Information

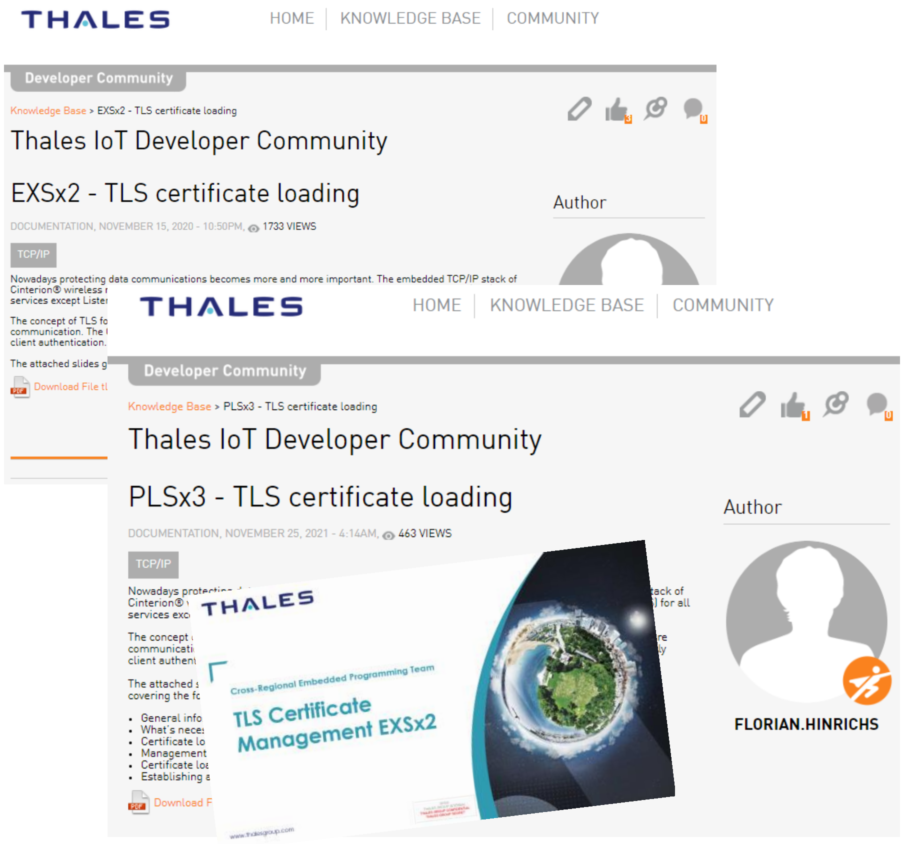
- **The embedded TCP/IP stack of Cinterion® wireless modules supports server and client authentication for Transport Layer Security (TLS) for all services except Listener services**
- **TLS certificates are stored in the NVRAM**
  - Max. 30 server certificates
  - Max. 1 client certificate & max. 1 “management certificate”
- **All certificates shall be coded in DER format**
- **AN62 describes TLS for Client TCP/IP services in detail**
  - Guidelines for loading certificates: Chapter 3
  - Basic information about generating certificates and key stores: Chapter 5
  - Secure AT commands: Chapter 8

Connection types

No Security	Encryption	Server Authentication	Mutual Authentication
• No additional steps required	• Create secure Internet service profile with disabled check of received server certificates	• Load server root certificate • Enable certificate check  Server certificates	• Load server root certificate • Load client certificate plus keys • Enable certificate check  Server certificates  Client certificates

Not covered by this document!

What’s different this time?



THALES HOME | KNOWLEDGE BASE | COMMUNITY

Developer Community

Knowledge Base > EXSx2 - TLS certificate loading

Thales IoT Developer Community

EXSx2 - TLS certificate loading

DOCUMENTATION, NOVEMBER 15, 2020 - 10:50PM, 1733 VIEWS

TCP/IP

Nowadays protecting data communications becomes more and more important. The embedded TCP/IP stack of Cinterion® wireless … services except Listen…

The concept of TLS fo… communication. The … client authentication.

The attached slides g…

Download File tl…

Author

THALES HOME | KNOWLEDGE BASE | COMMUNITY

Developer Community

Knowledge Base > PLSx3 - TLS certificate loading

Thales IoT Developer Community

PLSx3 - TLS certificate loading

DOCUMENTATION, NOVEMBER 25, 2021 - 4:14AM, 463 VIEWS

TCP/IP

Nowadays protectin… …ack of Cinterion® … …) for all services exc…

The concept … …re communicati… …ly client authent…

The attached s… covering the fo…

- General info…
- What’s neces…
- Certificate lo…
- Management…
- Certificate loa…
- Establishing a…

Download F…

THALES

Cross-Regional Embedded Programming Team

TLS Certificate Management EXSx2

www.thalesgroup.com

Author

FLORIAN.HINRICHS

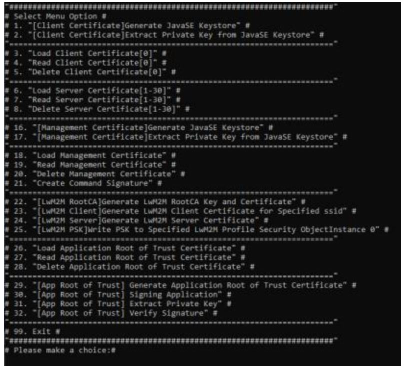
openssl

cmd_ipcertmgr.jar

AT commands

Keytool.exe

Hash_gen.jar



```
"##########################################################################"
# Select Menu Option #
# 1. "[Client Certificate]Generate JavaSE Keystore" #
# 2. "[Client Certificate]Extract Private Key from JavaSE Keystore" #
"--------------------------------------------------------------------------"
# 3. "Load Client Certificate[0]" #
# 4. "Read Client Certificate[0]" #
# 5. "Delete Client Certificate[0]" #
"--------------------------------------------------------------------------"
# 6. "Load Server Certificate[1-30]" #
# 7. "Read Server Certificate[1-30]" #
# 8. "Delete Server Certificate[1-30]" #
"--------------------------------------------------------------------------"
# 16. "[Management Certificate]Generate JavaSE Keystore" #
# 17. "[Management Certificate]Extract Private Key from JavaSE Keystore" #
"--------------------------------------------------------------------------"
# 18. "Load Management Certificate" #
# 19. "Read Management Certificate" #
# 20. "Delete Management Certificate" #
# 21. "Create Command Signature" #
"--------------------------------------------------------------------------"
# 22. "[LwM2M RootCA]Generate LwM2M RootCA Key and Certificate" #
# 23. "[LwM2M Client]Generate LwM2M Client Certificate for Specified ssid" #
# 24. "[LwM2M Server]Generate LwM2M Server Certificate" #
# 25. "[LwM2M PSK]Write PSK to Specified LwM2M Profile Security ObjectInstance 0" #
"--------------------------------------------------------------------------"
# 26. "Load Application Root of Trust Certificate" #
# 27. "Read Application Root of Trust Certificate" #
# 28. "Delete Application Root of Trust Certificate" #
"--------------------------------------------------------------------------"
# 29. "[App Root of Trust] Generate Application Root of Trust Certificate" #
# 30. "[App Root of Trust] Signing Application" #
# 31. "[App Root of Trust] Extract Private Key" #
# 32. "[App Root of Trust] Verify Signature" #
"--------------------------------------------------------------------------"
# 99. Exit #
"##########################################################################"
# Please make a choice:#
```

Bash script

What is necessary on server side

- **Server with public IP**
- **Certificates loaded for**
  - Server authentication
  - Client authentication

What is necessary on client side

What is needed to start:

- Module EXSs2/TXx2/PLSx3/ELS62
- Terminal program (e.g. Hterm, Zoc, teraterm)
- Application Note AN62 (TLS)
- Tools to have installed prior to start
  - Java (32 Bit version)
  - OpenSSL
  - Python

gemalto
a Thales company

Transport Layer Security for Client TCP/IP Services

Application Note 62

Version: 01
DocId: exs62-w_exs82-w_an62_tls_v01

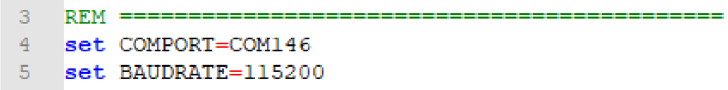
GEMALTO.COM/M2M

AN62

General configuration of the script

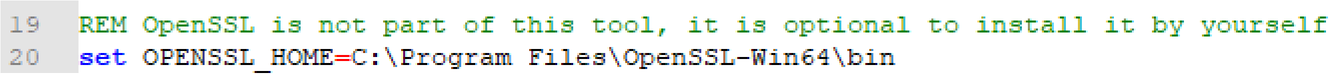
Make the script aware of where to find tools such as

- Com port and baud rate



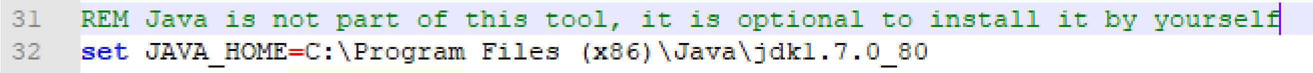
```
REM ==============================================
set COMPORT=COM146
set BAUDRATE=115200
```

- OpenSSL



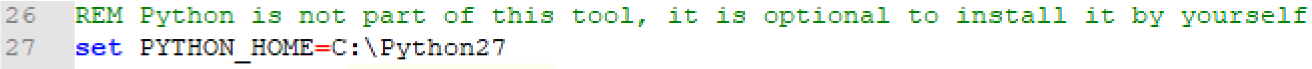
```
REM OpenSSL is not part of this tool, it is optional to install it by yourself
set OPENSSL_HOME=C:\Program Files\OpenSSL-Win64\bin
```

- Java



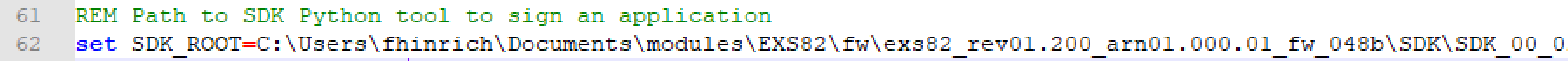
```
REM Java is not part of this tool, it is optional to install it by yourself
set JAVA_HOME=C:\Program Files (x86)\Java\jdk1.7.0_80
```

- Python



```
REM Python is not part of this tool, it is optional to install it by yourself
set PYTHON_HOME=C:\Python27
```

- Thales SDK



```
REM Path to SDK Python tool to sign an application
set SDK_ROOT=C:\Users\fhinrich\Documents\modules\EXS82\fw\exs82_rev01.200_arn01.000.01_fw_048b\SDK\SDK_00_0
```

Security Modes

Unsecure Mode	Secure Mode
• Everybody who has access to the module can manage the certificate store • **Enabled by default**	• AT commands and other means to access or modify security relevant configuration data, credentials and code shall be protected by a cryptographic signature based on the secure mode certificate loaded into the module. • Only authorised person can access and modify the certificate store • **“Management certificate” necessary to be loaded + AT command to activate secure mode**

THALES

TLS Certificate Loading – Unsecure Mode

Supported modules: EXSx2/TXx2/PLSx3/ELS62

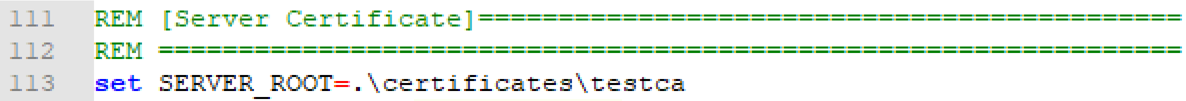
TLS Certificate Loading - Unsecure Mode

Server/Client certificate script functions

- Certificate Write
- Certificate Read
- Certificate Delete

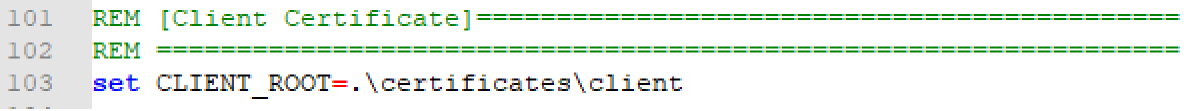
Before you launch the script, specify the certificate location

- Server certificate



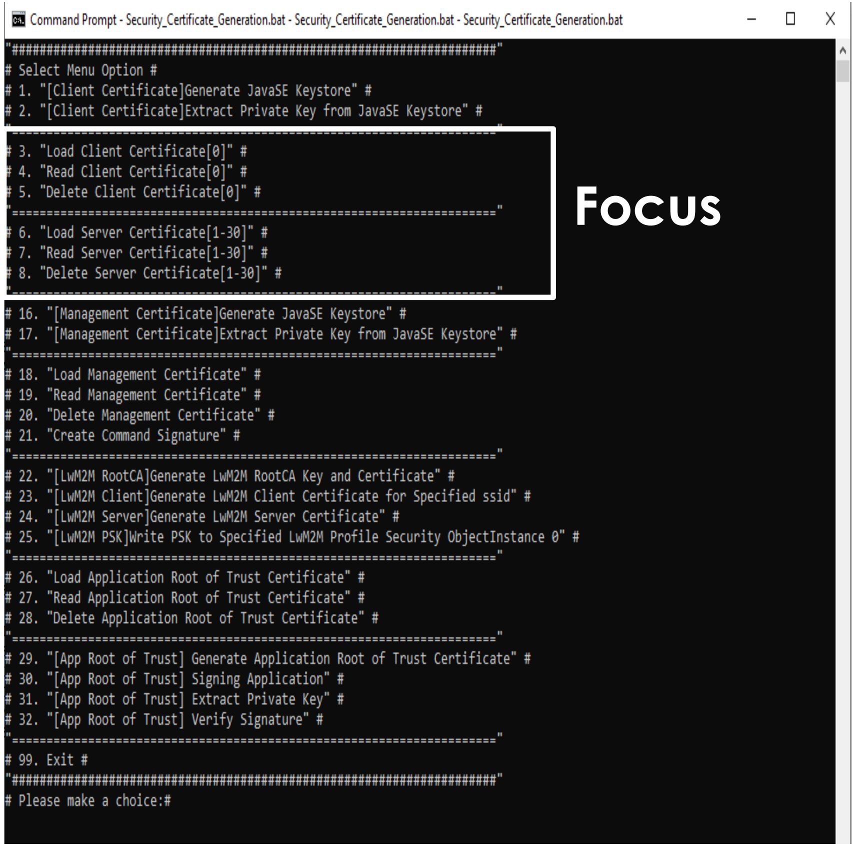
```
REM [Server Certificate]============================================
REM ================================================================
set SERVER_ROOT=.\certificates\testca
```

- Client certificate



```
REM [Client Certificate]============================================
REM ================================================================
set CLIENT_ROOT=.\certificates\client
```

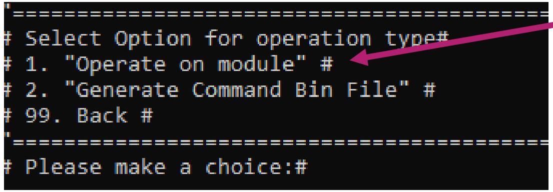
TLS Certificate Loading - Unsecure Mode


Command Prompt - Security_Certificate_Generation.bat - Security_Certificate_Generation.bat - Security_Certificate_Generation.bat

```
"#####################################################################"
# Select Menu Option #
# 1. "[Client Certificate]Generate JavaSE Keystore" #
# 2. "[Client Certificate]Extract Private Key from JavaSE Keystore" #
"====================================================================="
# 3. "Load Client Certificate[0]" #
# 4. "Read Client Certificate[0]" #
# 5. "Delete Client Certificate[0]" #
"====================================================================="
# 6. "Load Server Certificate[1-30]" #
# 7. "Read Server Certificate[1-30]" #
# 8. "Delete Server Certificate[1-30]" #
"====================================================================="
# 16. "[Management Certificate]Generate JavaSE Keystore" #
# 17. "[Management Certificate]Extract Private Key from JavaSE Keystore" #
"====================================================================="
# 18. "Load Management Certificate" #
# 19. "Read Management Certificate" #
# 20. "Delete Management Certificate" #
# 21. "Create Command Signature" #
"====================================================================="
# 22. "[LwM2M RootCA]Generate LwM2M RootCA Key and Certificate" #
# 23. "[LwM2M Client]Generate LwM2M Client Certificate for Specified ssid" #
# 24. "[LwM2M Server]Generate LwM2M Server Certificate" #
# 25. "[LwM2M PSK]Write PSK to Specified LwM2M Profile Security ObjectInstance 0" #
"====================================================================="
# 26. "Load Application Root of Trust Certificate" #
# 27. "Read Application Root of Trust Certificate" #
# 28. "Delete Application Root of Trust Certificate" #
"====================================================================="
# 29. "[App Root of Trust] Generate Application Root of Trust Certificate" #
# 30. "[App Root of Trust] Signing Application" #
# 31. "[App Root of Trust] Extract Private Key" #
# 32. "[App Root of Trust] Verify Signature" #
"====================================================================="
# 99. Exit #
"#####################################################################"
# Please make a choice:#
```

Focus

- Script can be controlled intuitively
- Simply type in the menu option of your desired action
- Dependent on the action, the script prompts additional questions
- Generally the user has two ways to load certificates
  - Automatically via the tool (configure Com port in the script prior to launch)
  - Manually via AT commands



```
"==========================================="
# Select Option for operation type#
# 1. "Operate on module" #
# 2. "Generate Command Bin File" #
# 99. Back #
"==========================================="
# Please make a choice:#
```

more convenient

“Management Certificate” – Secure Mode Activation

Note: Management Certificate required for secure mode

Supported modules: EXSx2/TXx2/PLSx3

Secure Mode

- The module supports uploading digital certificates for local module management. The certificate is then used to validate authentication of dedicated set of AT commands (these commands have to be signed by management certificate). List of commands:
  - AT^SBNW
  - AT^SSECUC
  - AT^SSECUA
- Activation with AT^SSECUC="SEC/MODE"
- Once activated, above AT commands require a valid signature to be provided in order to authenticate command issuer and command integrity. Signature is the SHA256 checksum of all the command data encrypted with module management private RSA key.

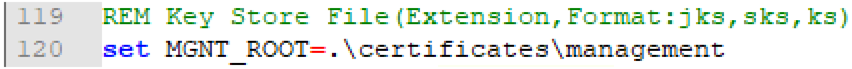
Management Certificate – Generating & Loading

Management certificate script functions

- Generate management certificate
- Certificate Write
- Certificate Read
- Certificate Delete

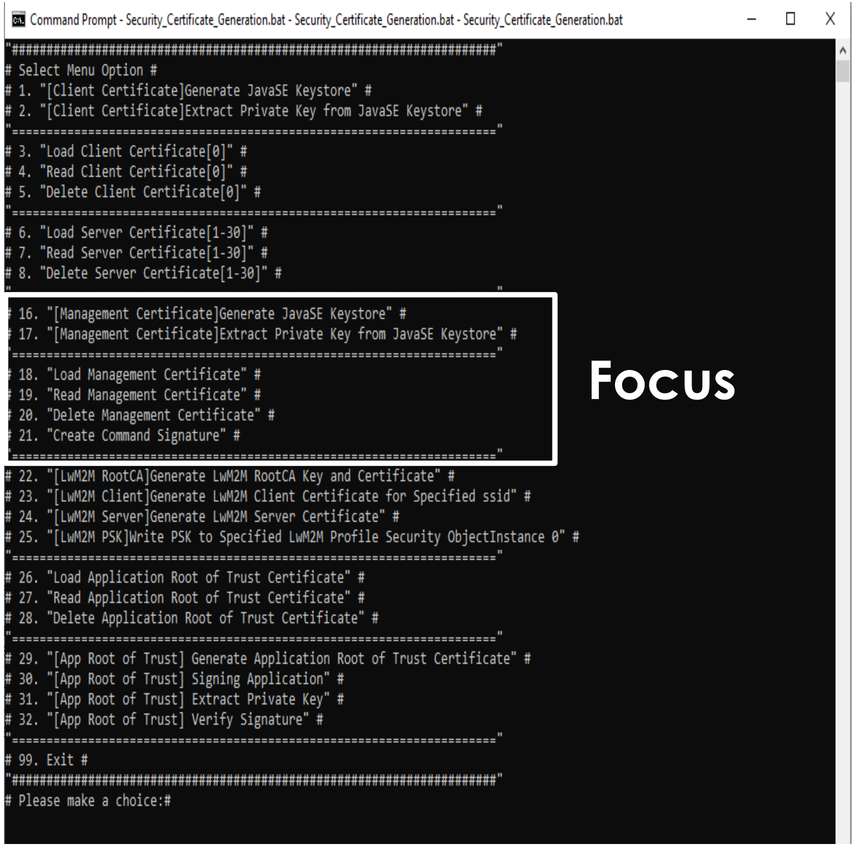
Before you launch the script, specify the certificate location or use the script to create a management certificate

- Management certificate



```
REM Key Store File(Extension,Format:jks,sks,ks)
set MGNT_ROOT=.\certificates\management
```

Management Certificate – Generating & Loading

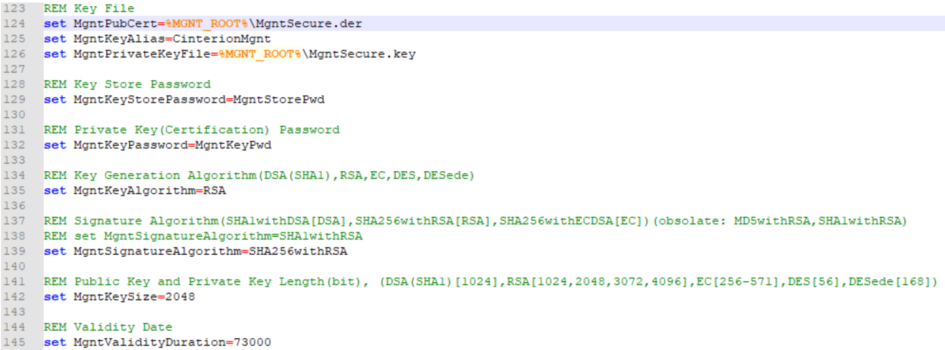

Command Prompt - Security_Certificate_Generation.bat - Security_Certificate_Generation.bat - Security_Certificate_Generation.bat

```
"##################################################################"
# Select Menu Option #
# 1. "[Client Certificate]Generate JavaSE Keystore" #
# 2. "[Client Certificate]Extract Private Key from JavaSE Keystore" #
"=================================================================="
# 3. "Load Client Certificate[0]" #
# 4. "Read Client Certificate[0]" #
# 5. "Delete Client Certificate[0]" #
"=================================================================="
# 6. "Load Server Certificate[1-30]" #
# 7. "Read Server Certificate[1-30]" #
# 8. "Delete Server Certificate[1-30]" #
"                                                                  "
# 16. "[Management Certificate]Generate JavaSE Keystore" #
# 17. "[Management Certificate]Extract Private Key from JavaSE Keystore" #
"=================================================================="
# 18. "Load Management Certificate" #
# 19. "Read Management Certificate" #
# 20. "Delete Management Certificate" #
# 21. "Create Command Signature" #
"=================================================================="
# 22. "[LwM2M RootCA]Generate LwM2M RootCA Key and Certificate" #
# 23. "[LwM2M Client]Generate LwM2M Client Certificate for Specified ssid" #
# 24. "[LwM2M Server]Generate LwM2M Server Certificate" #
# 25. "[LwM2M PSK]Write PSK to Specified LwM2M Profile Security ObjectInstance 0" #
"=================================================================="
# 26. "Load Application Root of Trust Certificate" #
# 27. "Read Application Root of Trust Certificate" #
# 28. "Delete Application Root of Trust Certificate" #
"=================================================================="
# 29. "[App Root of Trust] Generate Application Root of Trust Certificate" #
# 30. "[App Root of Trust] Signing Application" #
# 31. "[App Root of Trust] Extract Private Key" #
# 32. "[App Root of Trust] Verify Signature" #
"=================================================================="
# 99. Exit #
"##################################################################"
# Please make a choice:#
```

Focus

- Loading the management certificate onto the module works similar to loading server/client certificates

- For generating a management certificate the user can utilize either default or customized configuration parameter

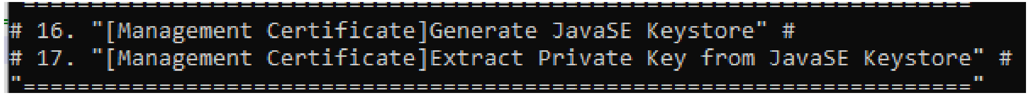


```
REM Key File
set MgntPubCert=%MGNT_ROOT%\MgntSecure.der
set MgntKeyAlias=CinterionMgnt
set MgntPrivateKeyFile=%MGNT_ROOT%\MgntSecure.key

REM Key Store Password
set MgntKeyStorePassword=MgntStorePwd

REM Private Key(Certification) Password
set MgntKeyPassword=MgntKeyPwd

REM Key Generation Algorithm(DSA(SHA1),RSA,EC,DES,DESede)
set MgntKeyAlgorithm=RSA

REM Signature Algorithm(SHA1withDSA[DSA],SHA256withRSA[RSA],SHA256withECDSA[EC])(obsolate: MD5withRSA,SHA1withRSA)
REM set MgntSignatureAlgorithm=SHA1withRSA
set MgntSignatureAlgorithm=SHA256withRSA

REM Public Key and Private Key Length(bit), (DSA(SHA1)[1024],RSA[1024,2048,3072,4096],EC[256-571],DES[56],DESede[168])
set MgntKeySize=2048

REM Validity Date
set MgntValidityDuration=73000
```

Management Certificate – Generating & Loading

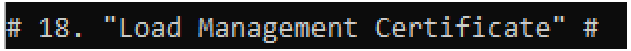
Steps to activate a management certificate on the module

- Generate a management certificate



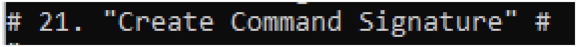
```
=====================================================================
# 16. "[Management Certificate]Generate JavaSE Keystore" #
# 17. "[Management Certificate]Extract Private Key from JavaSE Keystore" #
"==================================================================="
```

- Load the management certificate onto the module



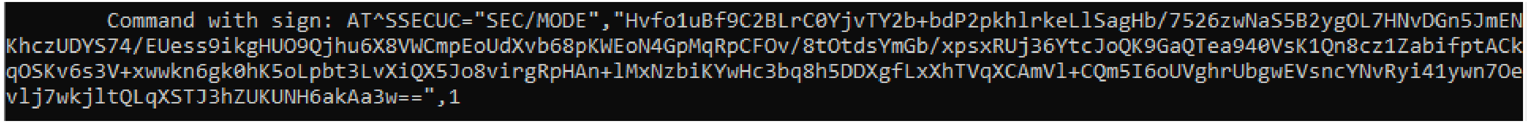
```
# 18. "Load Management Certificate" #
```

- Generate signed activation AT command



```
# 21. "Create Command Signature" #
```

- Activate secure mode by sending the signed AT command to the module

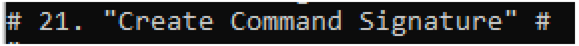


```
        Command with sign: AT^SSECUC="SEC/MODE","Hvfo1uBf9C2BLrC0YjvTY2b+bdP2pkhlrkeLlSagHb/7526zwNaS5B2ygOL7HNvDGn5JmEN
KhczUDYS74/EUess9ikgHUO9Qjhu6X8VWCmpEoUdXvb68pKWEoN4GpMqRpCFOv/8tOtdsYmGb/xpsxRUj36YtcJoQK9GaQTea940VsK1Qn8cz1ZabifptACk
qOSKv6s3V+xwwkn6gk0hK5oLpbt3LvXiQX5Jo8virgRpHAn+lMxNzbiKYwHc3bq8h5DDXgfLxXhTVqXCAmVl+CQm5I6oUVghrUbgwEVsncYNvRyi41ywn7Oe
vlj7wkjltQLqXSTJ3hZUKUNH6akAa3w==",1
```

Management Certificate – Deactivation

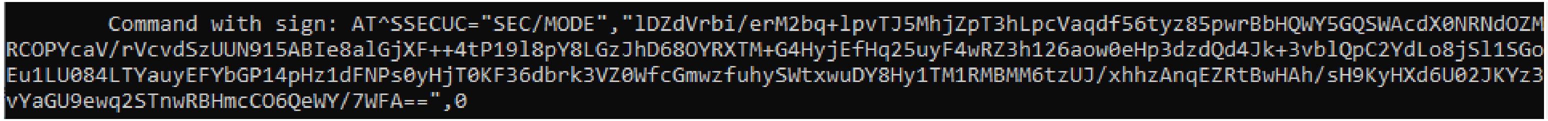
Steps to deactivate a management certificate on the module

- Generate signed activation AT command



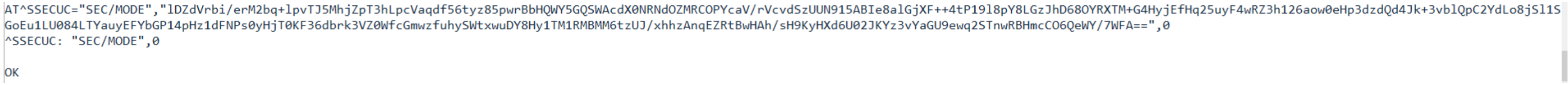
```
# 21. "Create Command Signature" #
```

- Deactivate secure mode by sending the signed AT command to the module



```
       Command with sign: AT^SSECUC="SEC/MODE","lDZdVrbi/erM2bq+lpvTJ5MhjZpT3hLpcVaqdf56tyz85pwrBbHQWY5GQSWAcdX0NRNdOZM
RCOPYcaV/rVcvdSzUUN915ABIe8alGjXF++4tP19l8pY8LGzJhD68OYRXTM+G4HyjEfHq25uyF4wRZ3h126aow0eHp3dzdQd4Jk+3vblQpC2YdLo8jSl1SGo
Eu1LU084LTYauyEFYbGP14pHz1dFNPs0yHjT0KF36dbrk3VZ0WfcGmwzfuhySWtxwuDY8Hy1TM1RMBMM6tzUJ/xhhzAnqEZRtBwHAh/sH9KyHXd6U02JKYz3
vYaGU9ewq2STnwRBHmcCO6QeWY/7WFA==",0
```

- AT command sent to the module



```
AT^SSECUC="SEC/MODE","lDZdVrbi/erM2bq+lpvTJ5MhjZpT3hLpcVaqdf56tyz85pwrBbHQWY5GQSWAcdX0NRNdOZMRCOPYcaV/rVcvdSzUUN915ABIe8alGjXF++4tP19l8pY8LGzJhD68OYRXTM+G4HyjEfHq25uyF4wRZ3h126aow0eHp3dzdQd4Jk+3vblQpC2YdLo8jSl1S
GoEu1LU084LTYauyEFYbGP14pHz1dFNPs0yHjT0KF36dbrk3VZ0WfcGmwzfuhySWtxwuDY8Hy1TM1RMBMM6tzUJ/xhhzAnqEZRtBwHAh/sH9KyHXd6U02JKYz3vYaGU9ewq2STnwRBHmcCO6QeWY/7WFA==",0
^SSECUC: "SEC/MODE",0

OK
```

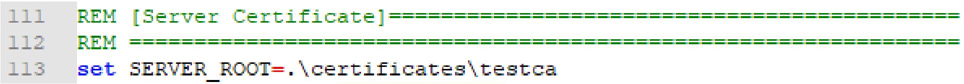
Certificate Loading – Secure Mode

Note: Management Certificate needs to be loaded

Supported modules: EXSx2/TXx2/PLSx3/ELS62

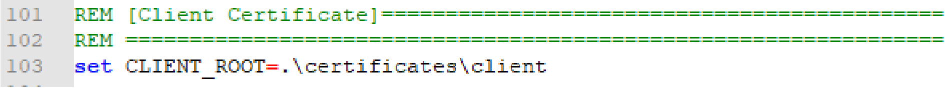
TLS Certificate Loading - Secure Mode

- Server/Client certificate script functions are equivalent to unsecure mode
- Difference between secure and unsecure mode, the module accepts properly signed commands only
- The beauty of the tool, it will automatically sign the commands
- Before you launch the script, specify the certificate location
  - Server certificate



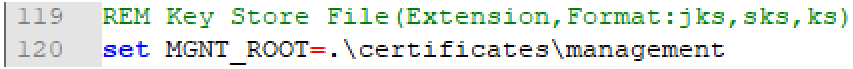
```
REM [Server Certificate]============================================
REM ================================================================
set SERVER_ROOT=.\certificates\testca
```

  - Client certificate



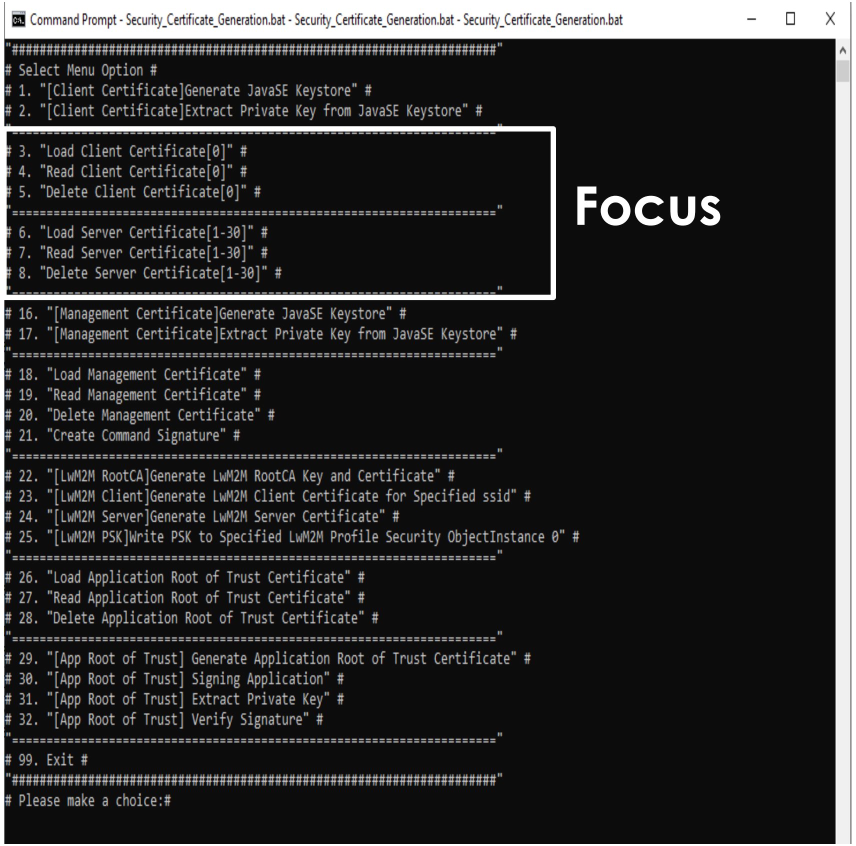
```
REM [Client Certificate]==========================================
REM =============================================================
set CLIENT_ROOT=.\certificates\client
```

  - Management certificate



```
REM Key Store File(Extension,Format:jks,sks,ks)
set MGNT_ROOT=.\certificates\management
```

TLS Certificate Loading - Secure Mode

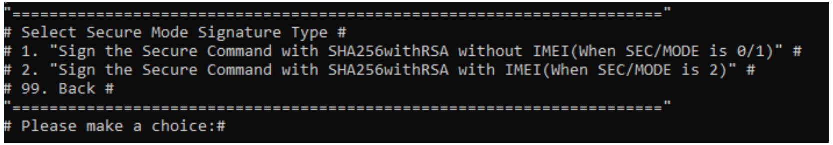


Command Prompt - Security_Certificate_Generation.bat - Security_Certificate_Generation.bat - Security_Certificate_Generation.bat

```
"######################################################################"
# Select Menu Option #
# 1. "[Client Certificate]Generate JavaSE Keystore" #
# 2. "[Client Certificate]Extract Private Key from JavaSE Keystore" #
"======================================================================"
# 3. "Load Client Certificate[0]" #
# 4. "Read Client Certificate[0]" #
# 5. "Delete Client Certificate[0]" #
"======================================================================"
# 6. "Load Server Certificate[1-30]" #
# 7. "Read Server Certificate[1-30]" #
# 8. "Delete Server Certificate[1-30]" #
"======================================================================"
# 16. "[Management Certificate]Generate JavaSE Keystore" #
# 17. "[Management Certificate]Extract Private Key from JavaSE Keystore" #
"======================================================================"
# 18. "Load Management Certificate" #
# 19. "Read Management Certificate" #
# 20. "Delete Management Certificate" #
# 21. "Create Command Signature" #
"======================================================================"
# 22. "[LwM2M RootCA]Generate LwM2M RootCA Key and Certificate" #
# 23. "[LwM2M Client]Generate LwM2M Client Certificate for Specified ssid" #
# 24. "[LwM2M Server]Generate LwM2M Server Certificate" #
# 25. "[LwM2M PSK]Write PSK to Specified LwM2M Profile Security ObjectInstance 0" #
"======================================================================"
# 26. "Load Application Root of Trust Certificate" #
# 27. "Read Application Root of Trust Certificate" #
# 28. "Delete Application Root of Trust Certificate" #
"======================================================================"
# 29. "[App Root of Trust] Generate Application Root of Trust Certificate" #
# 30. "[App Root of Trust] Signing Application" #
# 31. "[App Root of Trust] Extract Private Key" #
# 32. "[App Root of Trust] Verify Signature" #
"======================================================================"
# 99. Exit #
"######################################################################"
# Please make a choice:#
```

Focus

- Script can be controlled intuitively
- Simply type in the menu option of your desired action
- Dependent on the action, the script prompts additional questions
- In case the script detects a management certificate, it offers the user to sign the commands automatically



```
"======================================================================"
# Select Secure Mode Signature Type #
# 1. "Sign the Secure Command with SHA256withRSA without IMEI(When SEC/MODE is 0/1)" #
# 2. "Sign the Secure Command with SHA256withRSA with IMEI(When SEC/MODE is 2)" #
# 99. Back #
"======================================================================"
# Please make a choice:#
```

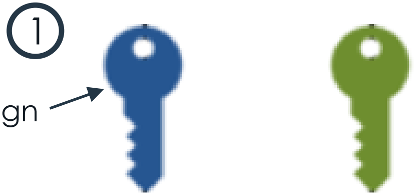
ThreadX Application Root of Trust

Note: Application root of trust mandatory to execute ThreadX application on the module

Supported modules: EXSx2/TXx2/PLSx3

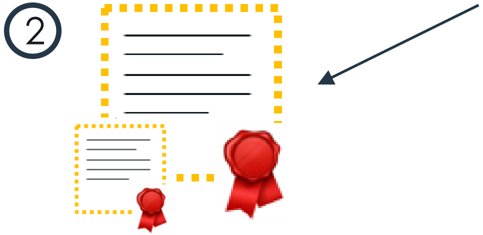
Why do we need to sign the ThreadX application…

- …because our ThreadX modules are demanding!
- They would not allow ThreadX applications entrance without permission
- ThreadX applications can only be executed if the application comes with a signature matching the application root of trust stored on the module
- By default modules come without application root of trust, it needs to be installed by the user
- What we need…



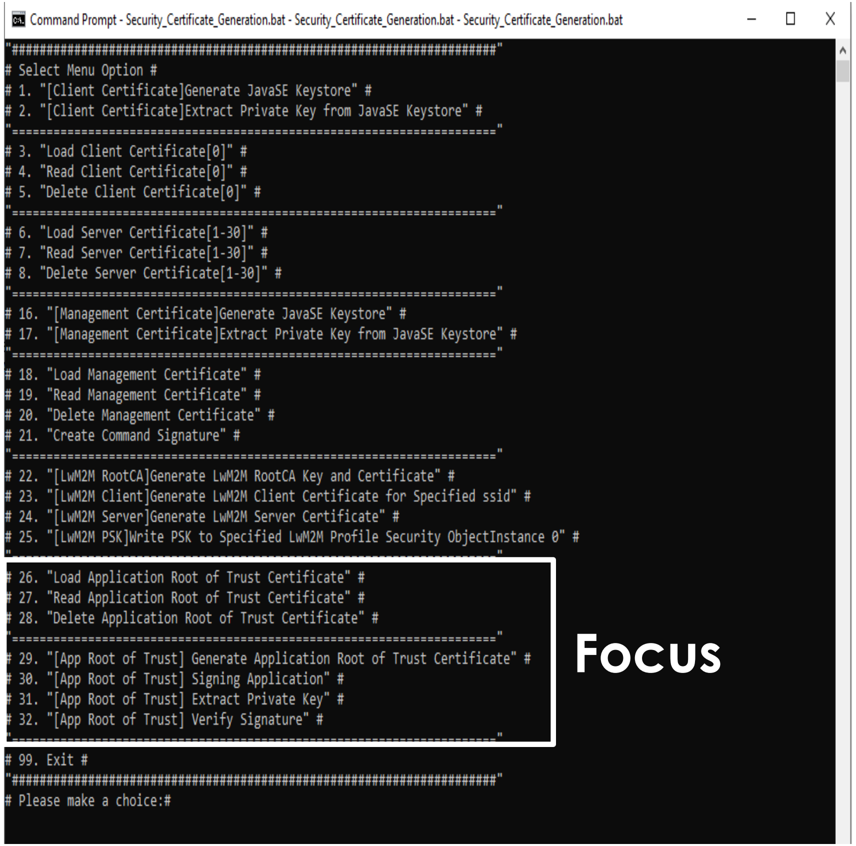
app_rot.key
(private)

app_rot.pem
(public)



app_rot.der
(certificate containing public key)

Application Root of Trust - Generating & Loading


Command Prompt - Security_Certificate_Generation.bat - Security_Certificate_Generation.bat - Security_Certificate_Generation.bat
Focus

```
"##################################################################"
# Select Menu Option #
# 1. "[Client Certificate]Generate JavaSE Keystore" #
# 2. "[Client Certificate]Extract Private Key from JavaSE Keystore" #
"=================================================================="
# 3. "Load Client Certificate[0]" #
# 4. "Read Client Certificate[0]" #
# 5. "Delete Client Certificate[0]" #
"=================================================================="
# 6. "Load Server Certificate[1-30]" #
# 7. "Read Server Certificate[1-30]" #
# 8. "Delete Server Certificate[1-30]" #
"=================================================================="
# 16. "[Management Certificate]Generate JavaSE Keystore" #
# 17. "[Management Certificate]Extract Private Key from JavaSE Keystore" #
"=================================================================="
# 18. "Load Management Certificate" #
# 19. "Read Management Certificate" #
# 20. "Delete Management Certificate" #
# 21. "Create Command Signature" #
"=================================================================="
# 22. "[LwM2M RootCA]Generate LwM2M RootCA Key and Certificate" #
# 23. "[LwM2M Client]Generate LwM2M Client Certificate for Specified ssid" #
# 24. "[LwM2M Server]Generate LwM2M Server Certificate" #
# 25. "[LwM2M PSK]Write PSK to Specified LwM2M Profile Security ObjectInstance 0" #
"=================================================================="
# 26. "Load Application Root of Trust Certificate" #
# 27. "Read Application Root of Trust Certificate" #
# 28. "Delete Application Root of Trust Certificate" #
"=================================================================="
# 29. "[App Root of Trust] Generate Application Root of Trust Certificate" #
# 30. "[App Root of Trust] Signing Application" #
# 31. "[App Root of Trust] Extract Private Key" #
# 32. "[App Root of Trust] Verify Signature" #
"=================================================================="
# 99. Exit #
"##################################################################"
# Please make a choice:#
```

- Script can be controlled intuitively
- Menu option 26-32 are ThreadX application signing related
- Dependent on the action, the script prompts additional questions

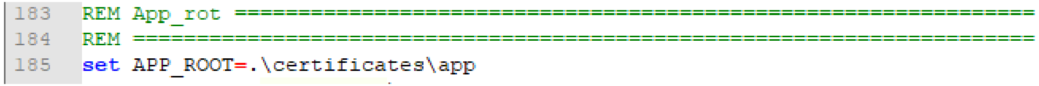
Application Root of Trust – Generating & Loading

Application Root of Trust script functions

- Load/Read/Delete application root of trust
- Generate application root of trust
- Signing application
- Verify signed application

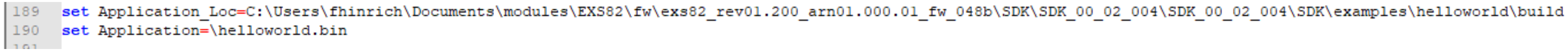
Before you launch the script, specify the certificate location or use the script to create a application root of trust

- Application root of trust



```
REM App_rot ===============================================================
REM =======================================================================
set APP_ROOT=.\certificates\app
```

- Application location and name



```
set Application_Loc=C:\Users\fhinrich\Documents\modules\EXS82\fw\exs82_rev01.200_arn01.000.01_fw_048b\SDK\SDK_00_02_004\SDK_00_02_004\SDK\examples\helloworld\build
set Application=\helloworld.bin
```

THALES

THANK YOU !