Over the Air Firmware Update

Application Note 17

80783NT12138A
Rev. 0
V 06
2024-4-2
Preliminary
Confidential

Technical Documentation

Contents

Tables

Figures

1 Applicability Table

Table 1: Applicability table

Products
Cinterion® EXS62-W
Cinterion® EXS82-W
Cinterion® TX62-W
Cinterion® TX82-W
Cinterion® TX62-W-B

2 Introduction

2.1 Scope

This Application Note[1] describes how to update a module's firmware over the air (so-called FOTA), i.e., via a wireless connection to an external FOTA server providing the firmware.

2.2 General Precautions

The firmware download over-the-air is only intended to install the same or a new firmware version. Installation of an older firmware version may lead to the module no longer being operational. The differential files could be downloaded which should be match exactly with the current firmware version.

2.3 Contact Information, Support

For technical support and general questions, e-mail:

- TS-EMEA@telit.com
- TS-AMERICAS@telit.com
- TS-APAC@telit.com
- TS-SRD@telit.com
- TS-ONEEDGE@telit.com

Alternatively, use: https://www.telit.com/contact-us/

Product information and technical documents are accessible 24/7 on our website: https://www.telit.com

2.4 Conventions

Note: Provide advice and suggestions that may be useful when integrating the module.

Danger: This information MUST be followed, or catastrophic equipment failure or personal injury may occur.

ESD Risk: Notifies the user to take proper grounding precautions before handling the product.

Warning: Alerts the user on important steps about the module integration.

All dates are in ISO 8601 format, that is YYYY-MM-DD.

1. The document is effective only if listed in the appropriate Release Notes as part of the technical documentation delivered with your Telit product.

2.5 Abbreviations

Table 2: **Abbreviations**

Abbreviation	Description
FFS	Flash File System
FOTA	Firmware update over-the-air
HTTP	Hypertext Transfer Protocol
PDP	Packet Data Protocol

2.6 Terms and Conditions

Refer to https://www.telit.com/hardware-terms-conditions/.

2.7 Disclaimer

THE MATERIAL IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. TELIT CINTERION RESERVES THE RIGHT TO MAKE CHANGES TO THE PRODUCTS DESCRIBED HEREIN. THE SPECIFICATIONS IN THIS DOCUMENT ARE SUBJECT TO CHANGE AT THE DISCRETION OF TELIT CINTERION WITHOUT PRIOR NOTICE. THIS DOCUMENT IS PROVIDED ON "AS IS" BASIS ONLY AND MAY CONTAIN DEFICIENCIES OR INADEQUACIES. TELIT CINTERION DOES NOT ASSUME ANY LIABILITY FOR INFORMATION PROVIDED IN THE DOCUMENT OR ARISING OUT OF THE APPLICATION OR USE OF ANY PRODUCT DESCRIBED HEREIN.

TELIT CINTERION GRANTS A NON-EXCLUSIVE RIGHT TO USE THE DOCUMENT. THE RECIPIENT SHALL NOT COPY, MODIFY, DISCLOSE, OR REPRODUCE THE DOCUMENT EXCEPT AS SPECIFICALLY AUTHORIZED BY TELIT CINTERION.

3 FOTA Application

To (automatically) update the module's firmware over-the-air, a possible external application has to complete the following basic steps:

1. **Connect to the Internet.** To prepare for a firmware download from the FOTA server, the user has to provide SIM PIN if needed, configuration of appropriate APN and define the PDP context.
2. **Download firmware.** To download a firmware package from the FOTA server to an internal FOTA partition on the module's flash file system (FFS), the AT command AT^SNFOTA="act",2 can be used.

   Before triggering the download, the user or application has to provide a server address, connection id and SHA256 checksum value via following subcommands AT^SNFOTA="url", AT^SNFOTA="conid" and AT^SNFOTA="crc".

   The AT command connects to the FOTA server via HTTP(s); download the firmware and verifies the firmware's integrity by SHA256 checksum. When using a resume download, the module checks whether the FFS fragment file is consistent with the server file, if they are consistent, continue to download, if not, restart the download.
3. **Report firmware download.** The module will report the progress of the firmware download at regular intervals. The success and failure will be reported by the module, success includes 100% file download and SHA256 integrity matching.
4. **Install firmware.** After download and data integrity verification, the firmware package can be installed with the AT command AT^SFDL=2. After firmware installation, the module will automatically restart to finish the firmware update. Afterwards, module is ready to be operated with the new firmware.

Figure 1 shows a flow chart for such an external FOTA application. Chapter 3 describes a FOTA application in more detail, and Chapter 4 details the HTTP(S) based protocol used to communicate with the FOTA server. All FOTA operations are controlled by AT commands. For more information on the AT commands mentioned throughout the document please refer to [2].

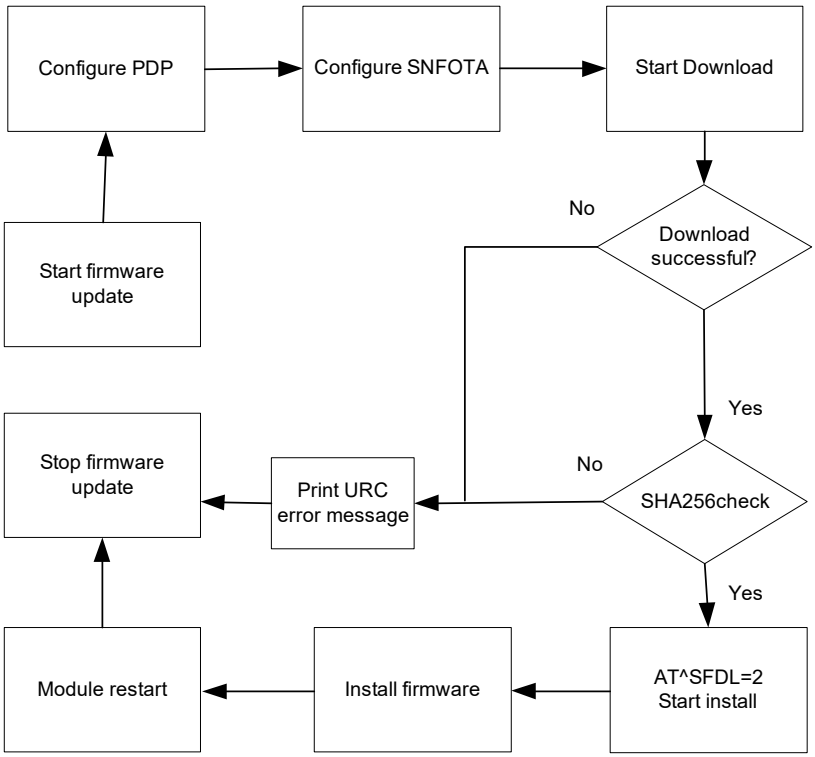


Figure 1: FOTA application

4 FOTA Application Example

This chapter gives a FOTA application sample, thereby explaining the basic steps as outlined in Chapter 2 in somewhat more detail.

Internet connection setup

`AT+CGDCONT=1,"IP","internet"` `OK`	// Define Internet context.

`AT+CGDCONT?`
`+CGDCONT: 1,"IP","internet","0.0.0.0",0,0,0,0,0,0`
`OK`
	// Query current PDP contexts.

`AT^SGAUTH=1,2,<password>,<username>`	//In case of using private APN with PDN authentication, which need to set type of Authentication for PDP-IP Connection and the corresponding <password> and <username> both need to be specified.

`AT+COPS?`
`+COPS: 0,0,"CHINA MOBILE",7`
`OK`
	// Module is started and attached to the network.

Configure FOTA connection and procedure

```
AT^SNFOTA=url,"http://
192.168.1.xxx:8008/ diff.usf"
OK

AT^SNFOTA=conid,"1"
OK

AT^SNFOTA=crc,ba168491fb-
ca78e11144d40576143d94604f75c2b
0124ae8a1b2c9aff3023527
OK

AT^SNFOTA=urc,1
OK

AT^SNFOTA?
^SNFOTA: "url","http://
192.168.1.xxx:8008/diff.usf"
^SNFOTA: "crc","ba168491fb-
ca78e11144d40576143d94604f75c2b
0124ae8a1b2c9aff3023527"
^SNFOTA: "urc","1"
^SNFOTA: "conid","1"
^SNFOTA: "act,"0","0","0"
OK
```

// Set FOTA server address, firmware path and file name.

// Set conID for AT+CGDCONT configuration

// set SHA256[1]

// Enable URCs.

// Check configuration settings
//Note: FOTA configuration settings are non volatile

1. For Windows, type the below command into console in order to calculate the SHA256 hash:
certutil -hashfile .\diff.usf SHA256
SHA256 hash of .\diff.usf:
ba168491fbca78e11144d40576143d94604f75c2b0124ae8a1b2c9aff3023527
CertUtil: -hashfile command completed successfully.

For Linux, use:
sha256sum ./diff.usf

FOTA URC error explanation

In case any error occurs after the download has started, it will be reported by an ^SNFOTA: "act", 2,<error>,0 URC, where <error> in (numeric) code represents as following possible FOTA errors:

0 No error

1 Error unknown

3 Server error

5 Socket error

6 Timeout error

7 File error

8 Not enough space

10 Firmware not available

11 integrity check mismatch

12 User break

13 Activate PDP error

14 Config parameter error

Examples:

- In case of ^SNFOTA:act,0,6,0 URC, (6 timeout error), there are following possibilities representing this kind of this an error;

  - It might be caused by missing the server CA certificate installation with AT^SBNR=is_cert command, while connecting to secure https FOTA file server;
  - Wrong server address or port configured. It can also be cause by the destination URL not pointing to correct incremental USF file.

- In case of ^SNFOTA:act,0,8,0 URC (8 Not enough space), which indicates the firmware USF file size is larger than the FOTA partition size (11MB) during downloading phase.

  This indicates the full firmware USF file has been uploaded into FOTA server instead of the expected incremental firmware USF file.

FOTA secure connection setup

```
AT^SNFOTA=url,https://
192.168.1.xxx:443/diff.usf                  // Set FOTA server secure address, firmware path and file name.
OK

AT^SBNW=is_cert,1                           // Load Server Certificate into module to ensure check certificates received from the server against the local certificate store
CONNECT
SECURE CMD READY: SEND COMMAND
...
SECURE CMD END OK
```

Note:

To load Server Certificate into a module, the Security_Certificate_Generation.bat script tool from SecurityCertMgr_Public package has to be used. Then, convert the X.509 format certificate file in ASN.1 encoded (der file extension) into binary transfer format file (bin file extension).

For example:

1.Place server certificate (X.509 format with ASN.1 encoded) with the specified name ServerCert{n}.der (n represent slot idx in is_cert store where certificate will be placed) under the root directory of SecurityCertMgr_Public tool package. Rename the certificate file to ServerCert1.der in order to place it into the first idx slot of is_cert store.

2. Using windows command console, launch the Security_Certificate_Generation.bat. A menu with multiple options will pop up;

```
"#################################################################
#####"
# Select Menu Option #
# 1. "[Client Certificate]Generate KeyTool Keystore, Certificate and
Private Key" #
# 2. "[Client Certificate:Optional]Generate Openssl Certificate and
Private Key" #
"=================================================================
====="
# 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 KeyTool Keystore, Certifi-
cate and Private Key" #
# 17. "[Application Root of Trust Certificate]Generate Openssl Cer-
tificate and Private Key" #
```

```
"================================================================
====="
# 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 Ob-
jectInstance 0" #
"================================================================
====="
# 26. "Load Application Root of Trust Certificate" #
# 27. "Read Application Root of Trust Certificate" #
# 28. "Delete Application Root of Trust Certificate" #
"================================================================
====="
# 99. Exit #
"################################################################
#####"
# Please make a choice:#
```

3. Execute option # 6 from the menu mentioned above ("Load Server Certificate[1-30]" #). It provides following options:

```
"################################################################
#####"
"Load Server Certificate[1-30]"
"################################################################
#####"
"================================================================
====="
```

```
# Please Input Server Certificate Index Number (1-30)#
# 99. Back #
"================================================================="
```

4. Choose Input 1 to select the ServerCert1.der as specified certificate to be loaded into No.1 idx slot of is_cert store, it provides additional options:

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

5. There are two ways of loading a certificate into a module:
   - Select # 1 "Operate on module" # to install the certificate ServerCert1.der into module directly, if module connected PC.

     For example:

     ```
     D:\SecurityCertMgr_Public>"C:\SoftDepot\DevSoft\Java\jdk1.7.0_71"\bin\java.exe -jar.\Tools\bin\win-x86\cmd_IpCertMgr.jar -serialPort COM5 -serialSpd 115200 -cmd writecert -certfile ServerCert1.der -certIndex 1 -sigType NONE
     Java version: 32-bit
     1.7.0_71
     Stable Library
     =========================================
     Native lib Version = RXTX-2.1-7
     Java lib Version   = RXTX-2.1-7
     CTS_RTS flow control enabled.
     AT:AT+CGSN
     Response:004401083356430
     IMEI:004401083356430
     signature skipped
     CTS_RTS flow control enabled.
     ```

```
nullAT

OK

AT

OK

AT^SBNW=is_cert,1

CONNECT

SECURE CMD READY: SEND COMMAND ...

SECURE CMD END OK

OK
```

- Select # 2. "Generate Command Bin File" # to generate the binary command bin file, which will use to load the certificate file in bin format.

  For example: the LoadServerCert1_insecure.bin is generated:

```
D:\SecurityCertMgr_Public>"C:\SoftDepot\DevSoft\Java\jdk1.7.0_71"\bin\java.exe -jar .\Tools\bin\win-x86\cmd_IpCertMgr.jar -cmd writecert -certfile ServerCert1.der -certIndex 1 -sigType NONE -file .\LoadServerCert1_insecure.bin

Java version: 32-bit

1.7.0_71

signature skipped
```

  After `LoadServerCert1_insecure.bin` has been generated, use `AT^SBNW=is_cert,1` to transfer the bin file to load certificate into module.

```
AT^SBNW=is_cert,1

CONNECT

SECURE CMD READY: SEND COMMAND ...

SECURE CMD END OK

OK
```

Download firmware and verify firmware integrity

```
AT^SNFOTA=act,2                    // Start firmware download.
OK


^SNFOTA: "act",2,0,10              // Downloading progress notifications
^SNFOTA: "act",2,0,20              with // download progress indications
^SNFOTA: "act",2,0,30              every 10% // (default setting).
^SNFOTA: "act",2,0,40
^SNFOTA: "act",2,0,50
^SNFOTA: "act",2,0,60
^SNFOTA: "act",2,0,70
^SNFOTA: "act",2,0,80
^SNFOTA: "act",2,0,90
^SNFOTA: "act",2,0,100             // Firmware download is complete.
                                   // If a problem is detected during down-
                                   load
                                   // (e.g., connection problems, SHA256
                                   check
                                   //failed, no more space on FFS, etc.), an
                                   error
                                   //code is presented in the URC, for
                                   example:
                                   // ^SNFOTA: "act",2,11,100 --> SHA256
                                   check
                                   // failed
                                   // ^SNFOTA: "act",2,8,0 --> not enough
                                   space
                                   // on FFS to hold the binary image file
                                   // For further error codes see [2].
```

Install firmware from FFS

```
AT^SFDL=2                                   // Start firmware installation.
OK



FOTA START
Checksum OK
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................
...............................             PHASE 1 OK!
...............................
.Please Wait for PHASE 2 to com-
plete...

^SYSSTART

+CIEV: prov,0,"fallb3gpp"
```

Note: If a disruption (e.g. through power down) occurs while the firmware is being installed after sending the AT^SFDL=2 command, the firmware update process will automatically be restarted from the beginning after module reboot, signalized with the FOTA START URC.

However, the module needs to finish the initial installation phase. Otherwise, the module reboots with ^SYSSTART URC.

Notes:

- Details on the above mentioned AT commands can be found in [2].
- All network related FOTA operations based on AT^SNFOTA can be aborted at any time with AT^SNFOTA=act,0 and be restarted later.
- Configuration settings done with AT^SNFOTA are non-volatile.
- After downloading the firmware update file from the FOTA server, if the SHA256 checksum verification failed as shown by URC ^SNFOTA: "act", "2","11","100" firmware update is unable to start.
- For Unsolicited Result Codes format of ^SNFOTA: "act", <action>,<error>,<progress>
- Each parameter definition and range as following

<action>

(numeric)

Sends request for FOTA action.

Results of FOTA <action>s 0 and 2 are reported by URCs.

0	Stop downloading process and communication with server.
2	Start/resume download firmware USF file.
""(P)	Default is empty string.

<error>

(numeric)

Possible FOTA errors reported by URCs

0(P)	No error
1	Error unknown
3	Server error
5	Socket error
6	Timeout error
7	File error
8	Not enough space

10	Firmware not available
11	Integrity check mismatch
12	User break
13	Active PDP error
14	config parameter error

<progress>

(numeric)

$0^{(P)}$ ... 100	Download progress in percent in steps of 10%.

5 FOTA Protocol

This chapter describes the protocol required for FOTA communication between module and server. The protocol is based on HTTP, and a possible FOTA server has to implement it. Note that parameters and values in the protocol description are just examples. Please contact Telit for more information on possible FOTA server access.

5.1 FOTA Server Queries

This section assembles possible FOTA server queries as well as a subsection explaining the various parameters mentioned in the queries.

5.1.1 Firmware Download

The following table shows the query for the description of the current firmware image on the FOTA server, and lists possible responses by FOTA server:

Query	Response
GET <dynamic URI of firmware image> (for more information about parameters see also Section 4.1.2	If information is available: HTTP 200 (OK) Header fields settings: Content-Type: application/octet-stream Content-Length: 4406083 If information is not available: HTTP 404 (Not Found)

6 General LwM2M FOTA

FOTA also allows updating the module's firmware by downloading the new firmware from LwM2M server. The following servers are prerequisites of general LwM2M FOTA update:

An LwM2M server where the LwM2M service is supplied, via the LwM2M protocol.

A packet server where the update files are downloaded from, via the CoAP(S) or HTTP(S) transfer protocol.

The LeShan Server is not provided by Telit.

The Cinterion® IoT Suite Server is provided by Telit, please contact Telit for more information.

The Lifetime resource configuration affects the module's power consumption. Pay attention when configuring the Lifetime resource on the LwM2M server.

The module periodically updates the registration information to the LwM2M server. The time interval for updates is defined by the Lifetime resource of the LwM2M server object instance. By default, the Lifetime resource of the registration is 180 seconds (i.e. 3 mins), while it is configurable by writing new value to the Lifetime Resource (i.e. "/1/0/1") on the LwM2M server side.

6.1 General LwM2M FOTA Application Example

This chapter gives an LwM2M FOTA application example, thereby explaining the basic steps with detail.

Internet connection setup

`AT+CGDCONT=1,"IP","internet"` `OK`	// Define Internet context.

`AT+CGDCONT?`
`+CGDCONT: 1,"IP","inter-net","0.0.0.0",0,0,0,0,0,0`
`OK`
	// Query current PDP contexts.

`AT^SGAUTH=1,2,<password>,<user-name>`	//In case of using private APN with PDN authentication, which need to set type of Authentication for PDP-IP Connection and the corresponding <password> and <username> both need to be specified.

`AT+COPS?`
`+COPS: 0,0,"CHINA MOBILE",7`
`OK`
	// Module is started and attached to the network.

Configure the LwM2M client associate with PDN settings

`AT^SNLWM2M=cfg/ext,LeShan,CID,1`
`OK`
 	
`Or below AT.`
`AT^SNLWM2M=cfg/ext,LeShan,/,conid,1`
`OK`
	// Configure Lwm2m client to use conid as 1 which associate the PDP-IP Connection setting from AT+CGDCONT

`AT^SNLWM2M=cfg/ext,MODS,/0/0/10,USER_NAME,<Username>`
 	
`AT^SNLWM2M=cfg/ext,MODS,/0/0/10,PASSWORD,<Password>`
	//In case of using private APN with PDN authentication, the corresponding <Username> and <Password> both need to be specified

Configure the LwM2M objects

To prepare for firmware download from the web server, the Internet connection with the LwM2M server is necessary.

Configure the LwM2M security, server, access control objects via AT^SNNLWM2M.

`AT^SNLWM2M=cfg,LeShan,/0/0/0,coap:// 182.92.198.110:5863`	///Configure the LwM2M server url
`AT^SNLWM2M=cfg,LeShan,/0/0/1,false`	//Configure a standard LwM2M server, instead of LwM2M bootstrap server.
`AT^SNLWM2M=cfg,LeShan,/0/0/2,3`	//Used under non-DTLS condition //0:PSK secure mode,2:certificate secure mode,3:non-secure mode
`AT^SNLWM2M= cfg,LeShan,/0/0/10,112`	//Configure short server ID
`AT^SNLWM2M=cfg/object,LeShan,/0/0,new`	//Create the new or update the existing security object 0 to make effect according to above configurations
`AT^SNLWM2M=cfg,LeShan,/1/0/0,112`	//Configure the LwM2M server to be also belonging to the short server ID
`AT ^SNLWM2M=cfg,LeShan,/1/0/1,180`	//Configure the lifetime of the registration in seconds.
`AT ^SNLWM2M=cfg,LeShan,/1/0/2,1`	//Configure the default value the LwM2M Client should use for the Minimum Period of an Observation in second.
`AT ^SNLWM2M=cfg,LeShan,/1/0/3,60`	//Configure the default value the LwM2M Client should use for the Maximum Period of an Observation in second.
`AT ^SNLWM2M=cfg,LeShan,/1/0/5,86400`	//Configure the period to disable the Server. After this period, the LwM2M Client MUST perform registration process to the Server. If this Resource is not set, a default timeout value is 86400 (1 day/24hours).

`AT ^SNLWM2M=cfg,LeShan,/1/0/6,true`	//Configure the whether the Lwm2m Client reports stored "Notify" operations to the Server or not, after the Lwm2m client back to enable/online from previous disable/offline.
`AT ^SNLWM2M=cfg,LeShan,/1/0/7,UQS`	//Configure the transport binding Mode.
`AT ^SNLWM2M=cfg/object,LeShan,/1/0,new`	//Create the new or update the existing server object 1 to make effect according to above configurations

`AT^SNLWM2M=cfg,LeShan,/2/2/0,5`
`AT^SNLWM2M=cfg,LeShan,/2/2/1,0`
`AT^SNLWM2M=cfg,LeShan,/2/2/2/112,31`
`AT^SNLWM2M=cfg,LeShan,/2/2/3,112`
`AT^SNLWM2M=cfg/object,LeShan,/2/2,new`
	//Create the new or update the existing access control object instance which point to instance 0 of Firmware update object 5 and configure the access rights associate with short server id of a certain Lwm2m server

- For DTLS condition with certificate secure mode for both registration and FOTA

`AT^SNLWM2M=cfg,LeShan,/0/0/0,coaps://182.92.198.110:5864`	//Config to LwM2M Secure Server address via COAPS protocol and ports
`AT^SNLWM2M=cfg,LeShan, /0/0/2,2`	//Used under DTLS condition with certificate secure mode //0:PSK secure mode,2:certificate secure mode,3:non-secure mode
`AT^SNLWM2M=cfg/object,LeShan,/0/0,new`	//Create the new or update the existing security object 0 to make effect according to above configurations

`AT^SNLWM2M=cfg/ext, LeShan,/0/0/10,SECURITY_SUITES,"C0AE,C023`	//Configure the Certificate cipher suite for secure registration for LwM2M client
	//TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8(C0AE)
	//TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256(C023)

`AT^SNLWM2M=cfg/ext,MODS,/ ,DEFAULT_LWM2M_ROOT_CA_THUMB-PRINT,{certificate's thrumb-print}`	//Configure the certificate thrumbprint to specified which server certificate will be used for connecting the secure LwM2M server, the certificate thrumb-print can be queried via AT^SBNR=pre-config_cert,1
`AT^SNLWM2M=cfg/ext,MODS,/ ,FOTA_SECURITY_MODE,2`	//Configure the FOTA secure mode /Either 2:certificate secure mode, or 3:non-secure mode
`AT^SNLWM2M=cfg/ext,MODS,/ ,FOTA_SECURITY_VERSION,12`	//Configure to use TLS1.2(if transport protocol via HTTPS) or DTLS1.2(if trans-port protocol via COAPS)
`AT^SNLWM2M=cfg/ext,MODS,/ ,FOTA_SECURITY_- SUITES,"C0AE,C023"`	//Configure the certificate cipher-suite for FOTA secure connection //TLS_ECDHE_ECD-SA_WITH_AES_128_CCM_8(C0AE) //TLS_ECDHE_ECD-SA_WITH_AES_128_CBC_SHA256(C023)

Notes:

- The PSK key is generate as a random AES 128-bit hex encoded PSK Secret Key. There is a reference example, which "Application Notes 62 - Transport Layer Security for Client TCP/IP Services" described SecurityCertMgr script tool's below option can be used to generate and inject PSK key to specified LwM2M profile.

```
# 25. "[LwM2M PSK]Write PSK to Specified LwM2M Profile Security Ob-
jectInstance 0" #
```

- The certificate secure mode which need additional steps for certificate installing on both module side and LeShan server side separately;
  - For module side certificate installation which including the reusing preconfig client certificate or reinstall specified preconfig client certificate and install the Lwm2m server specified server certificate which need to refer to additional manual for detail information and please contact Telit for more information.
  - For LeShan server side's server certificate deployment, please refer to Leshan website for technical information.

Start the LwM2M Client

Start the LwM2M client via AT^SNLWM2M

```
AT^SNLWM2M=act,LeShan,start                    //Start the LwM2M client
OK
```

The LwM2M web server lists all the modules and object resources which can be used for FOTA. Connect the packet server to Internet and upload the corresponding incremental firmware package file to pack server before further incremental firmware package starts to be downloaded.

Notes:

The LeShan Server's bundled packet server support CoAP(s) transport protocol only. As the pack server could be separate file server which support HTTP(s) transport protocol, so any HTTP(s) host can be used as package server as well.

The Cinterion® IoT Suite Server's packet server support both CoAP(s) and HTTP(s) transport protocols.

Start FOTA download and update procedure

Open the LwM2M server and the object of the module will be shown. Follow the steps to start FOTA:

1.Write the FOTA URL to the Package URI field(/5/0/1). for example

http:// 182.92.198.110:8081/fota.usf)

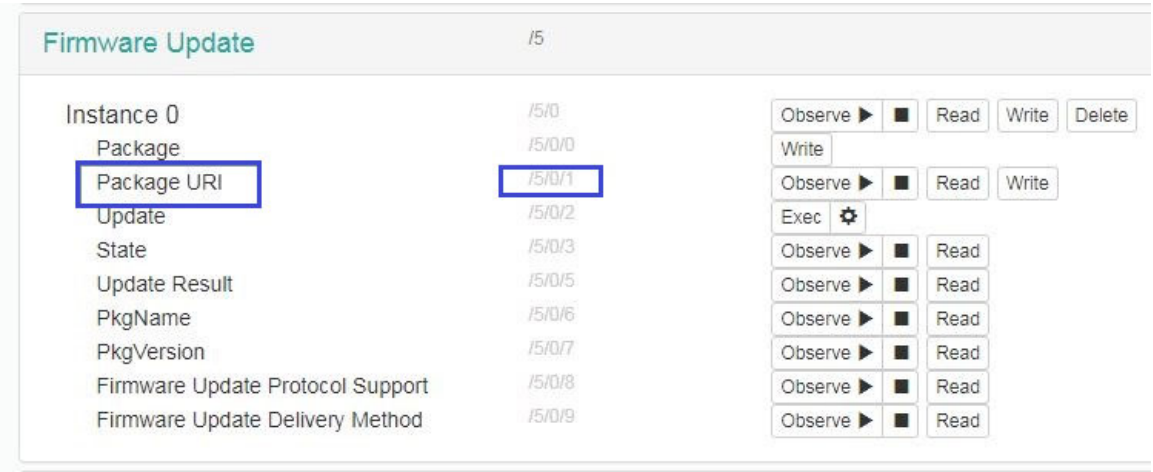
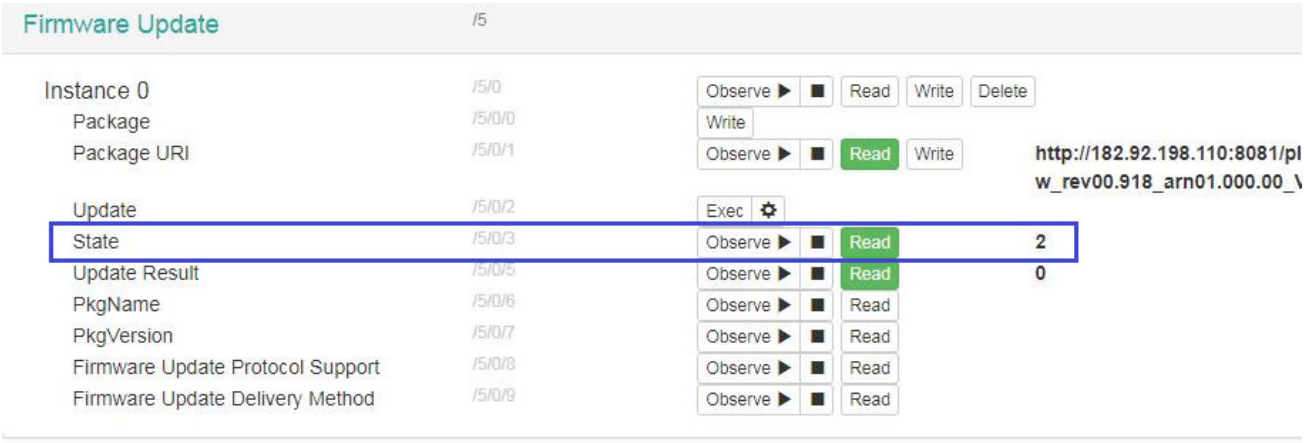
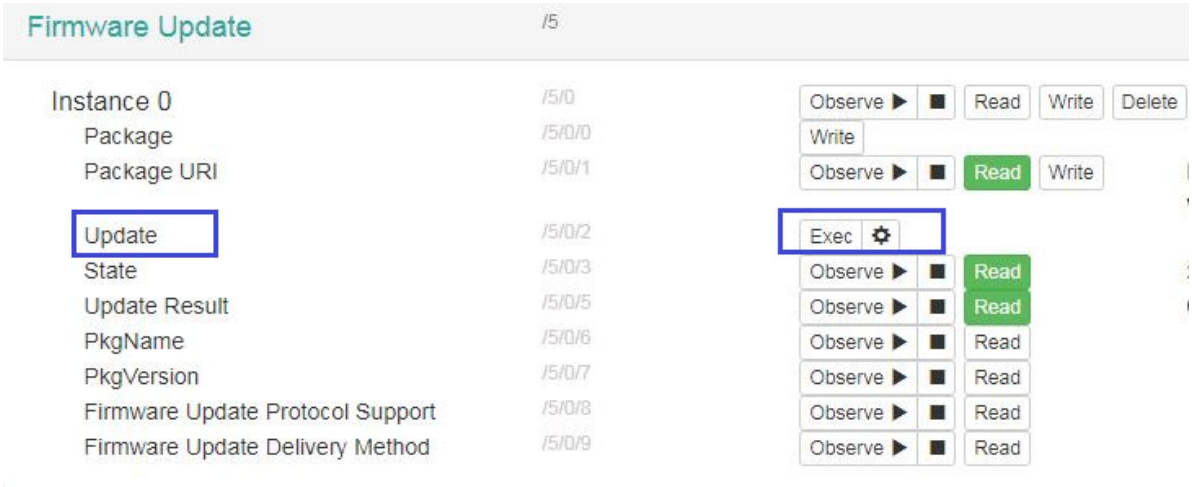


Figure 2: General LwM2M FOTA Application Example

2. In the State field, when the state changes to "1", the downloading starts. When the state changes to "2", the download is completed. The firmware package is downloaded to the module.



3. In the Update field, click Execute to start to update the firmware in the module.



Validate the update

To verify if the firmware version is updated, use ATI1 command, because there is a possibility that the upgrade failed and the module starts with the old firmware version.

```
ATI1                                    // Query current firmware version
                                        // and check for firmware update.
Cinterion
EXS82-W
REVISION 01.200
A -REVISION 01.000.00                   // Check if the firmware is upgraded to
OK                                      the latest.
```

7 NV Setting Restore Notices

The device manufacturer's MCU (micro-controller unit) application which in charge of Telit module behavior which also has responsibility to maintain module desired configu-ration and settings (Such as PDN, RAT and other settings) after firmware update (FOTA and SWUP) procedure finished should be same as firmware update triggered before to ensure the preferred PDN, RAT and other settings should be restored via re-configuration settings (issue ATs via MCU) to ensure module could work as expected and register to the network correctly as executed firmware update before.

For example:

The module was configured with customized or expected radio band settings which are different with default settings as following:

```
AT^SCFG="Radio/Band/CatM"
^SCFG: "Radio/Band/CatM","00080004"
OK

AT^SCFG="Radio/Band/CatNB"
^SCFG: "Radio/Band/CatNB","00080080"
OK
```

Afterwards the module firmware update via SWUP or FOTA between two firmware which might consist module NV update, then above both radio bands (CatM and CatNB) will be overwritten and restore to factory default settings as following:

```
AT^SCFG="Radio/Band/CatM"
^SCFG: "Radio/Band/CatM","0f0e189f","0010000200000000"
OK

AT^SCFG="Radio/Band/CatNB"
^SCFG: "Radio/Band/CatNB","0b0e189f","0010004200000000"
OK
```

So the device manufacturer's MCU (micro-controller unit) application should have logic in to reconfigure the radio band settings via resend ATs to maintain the desired configuration and settings.

```
AT^SCFG="Radio/Band/CatM","00080004"
^SCFG: "Radio/Band/CatM","00080004"
OK

AT^SCFG="Radio/Band/CatNB","00080080"
^SCFG: "Radio/Band/CatNB","00080080"
OK
```

Below is the list of AT commands together with parameters' Non-Volatile settings that should be reconfigured via MCU after a firmware update (FOTA or SWUP). This should take place if the manufacturer's configurations are different from the default ones.

Table 3: **ATC list**

Category	Command	Non-volatile parameter
Configuration	AT^SCFG= "GPRS/AutoAttach"[,<gaa>]	<gaa>(NV)
	AT^SCFG= "GPRS/MTU/Mode",<nwmode>	<nwmode>(NV)
	AT^SCFG= "GPRS/MTU/Size",<mtusize>	<mtusize>(NV)
	AT^SCFG= "Ident/Manufacturer"[,<manufacturer>]	<manufacturer>(NV)
	AT^SCFG= "Ident/Product"[,<product>]	<product>(NV)
	AT^SCFG= "MEopMode/RscMgmt/Rrc"[,<order>]	<order>(NV)
	AT^SCFG= "MEopMode/SRPOM"[,<srpom>]	<srpom>(NV)
	AT^SCFG= "Radio/Band/2G"[,<rba2g>]	<rba2g>(NV)
	AT^SCFG= "Radio/Band/CatM"[,<rbacatm-1>][,<rbacatm-2>]	<rbacatm-1>(NV) <rbacatm-2>(NV)
	AT^SCFG= "Radio/Band/CatNB"[,<rbacatnb-1>][,<rbacatnb-2>]	<rbacatnb-1>(NV) <rbacatnb-2>(NV)
	AT^SCFG= "Radio/Suspend"[,<SuspendMode>]	<SuspendMode>(NV)
	AT^SCFG= "Security/GEA"[,<gea>]	<gea>(NV)
Network Service	AT+CEDRXS= [<mode>[,<AcT-type>[,<Requested_eDRX_value>]]]	<mode>(NV) <Requested_eDRX_value>(NV)
	AT^SEDRXS= [<mode>[,<AcT-type>[,<Requested_eDRX-_value>][,<Requested_Paging_time_window>]]]	<mode>(NV) <Requested_eDRX_value>(NV) <Requested_Paging_time_window>(NV)
	AT^SXRAT= <AcT>[,<AcT_pref1>[,<AcT_pref2>]]	<AcT>(NV) <AcT_pref1>(NV) <AcT_pref2>(NV)
	AT+CCIOTOPT= [<n>[,<supported_UE_opt>[,<preferred_UE_opt>]]]	<supported_UE_opt>(NV) <preferred_UE_opt>(NV)

Table 3: ATC list

Category	Command	Non-volatile parameter
SMS	AT^SSDA= <da>	<da>(NV)
Packet Domain	AT+CEMODE= <mode>	<mode>(NV)
	AT+CGDCONT= <cid>[,<PDP_-type>[,<APN>[,<PDP_addr>[,<d_comp>[,<h_comp>[,<IPv4AddrAl-loc>[,<emergency_indication>[,<P-CSCF_discovery>[,<IM_CN_Signalling_-Flag_Ind>[,<NSLPI>[,<securePCO>[,<IPv4_MTU_discov-ery>[,<Local_Addr_Ind>]]]]]]]]]]]]]	<cid>(NV) <PDP_type>(NV) <APN>(NV) <PDP_addr>(NV) <d_comp>(NV) <h_comp>(NV) <IPv4AddrAlloc>(NV) <emergency_indication>(NV) <P-CSCF_discovery>(NV) <IM_CN_Signalling_Flag_Ind>(NV)
	AT+CGSMS= <service>	<service>(NV) (&V)
	AT^SGAPN= <cid>,<apnClass>[,<apnType>[,<APN>[,<bearer>[,<enabled-Flag>[,<inactivityTimeout>[,<max_pdn_conn>[,<max_pdn_conn_time>[,<max_pdn_req_wait_time>]]]]]]]]	<cid>(NV) <apnClass>(NV) <APN>(NV) <apnType>(NV) <bearer>(NV) <enabledFlag>(NV) <inactivityTimeout>(NV) <max_pdn_conn>(NV) <max_pdn_conn_time>(NV) <max_pdn_req_wait_time>(NV)
	AT^SGAUTH= <cid>[,<auth_type>[,<passwd>,<user>]]	<cid>(NV) <auth_type>(NV) <passwd>(NV) <user>(NV)
	AT^SGCONF= [<llc_pdu_length_U>][,[<llc_pdu_length_I>][,[<GPRS msclass>][,[<EGPRS msclass>][,<msClassChangeMode>]]]]	<GPRS msclass>(NV) <EGPRS msclass>(NV)

8 Document History

Preceding document: AN17: "Over-the-Air Firmware Update", Version 05

New document: AN17: "Over-the-Air Firmware Update", Version 06

Chapter	What is new
3	FOTA URC Error explanation section added.

Preceding document: AN17: "Over-the-Air Firmware Update", Version 04

New document: AN17: "Over-the-Air Firmware Update", Version 05

Chapter	What is new
3	Note for Install firmware from FFS has been updated.

Preceding document: AN17: "Over-the-Air Firmware Update", Version 03

New document: AN17: "Over-the-Air Firmware Update", Version 04

Chapter	What is new
3	Logs updated

Preceding document: AN17: "Over-the-Air Firmware Update", Version 02

New document: AN17: "Over-the-Air Firmware Update", Version 03

Chapter	What is new
3	New section added: FOTA secure connection setup

Preceding document: AN17: "Over-the-Air Firmware Update", Version 01

New document: AN17: "Over-the-Air Firmware Update", Version 02

Chapter	What is new
6	Chapter's description edited. Table 2 added.

Chapter	What is new
--	Initial document setup.