

Premium FOTA Management Application Note

80000NT10013a Rev.14, 2014-12-04



APPLICABILITY TABLE

	SW Versions
GC Family (Compact)	
GC864-QUAD	10.00.xx7
GC864-QUAD V2	
GC864-DUAL V2	
GE/GL Family (Embedded)	
GE864-QUAD	10.00.xx7
GE864-QUAD V2	
GE864-QUAD Automotive V2	
GE864-QUAD ATEX	
GE864-DUAL V2	
GE864-GPS	
GE865-QUAD	
GL865-DUAL	
GL865-QUAD	
GL868-DUAL	
GE910-QUAD	13.00.xx3
GE910-QUAD AUTO	
GE910-GNSS	
GE910-QUAD V3	16.00.xx2
GE866-QUAD	
GL865-QUAD V3	
GL865-DUAL V3	
GL868-DUAL V3	12.00.xx4
GT Family (Terminal)	
GT863-PY	
GT864-QUAD	
GT864-PY	
HE910 Family	
HE910 (1)	
HE910-GA	
HE910-D	
HE910-EUR / HE910-EUD	
HE910-EUG / HE910-NAG	
HE910-NAR / HE910-NAD	
UE/UL Family (Embedded)	
UE910-EUR / UE910-EUD	
UE910-NAR / UE910-NAD	
UL865-EUR / UL865-EUD	
UL865-NAR / UL865-NAD	
UL865-N3G	

NOTICE: the features and AT commands covered by the present document are concerning the software version shown in the Applicability Table. To get more information about the AT commands and their syntax see the AT Commands Reference Guide referring to the software version indicated in the table. Where it is needed, a note is indicated if a specific feature is not supported by the previous software versions

(1): HE910 is the “type name” of the products marketed as HE910-G & HE910-DG

Tab. 1: Products and Software Versions



SPECIFICATIONS SUBJECT TO CHANGE WITHOUT NOTICE

Notice

While reasonable efforts have been made to assure the accuracy of this document, Telit assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. The information in this document has been carefully checked and is believed to be entirely reliable. However, no responsibility is assumed for inaccuracies or omissions. Telit reserves the right to make changes to any products described herein and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Telit does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others.

It is possible that this publication may contain references to, or information about Telit products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Telit intends to announce such Telit products, programming, or services in your country.

Copyrights

This instruction manual and the Telit products described in this instruction manual may be, include or describe copyrighted Telit material, such as computer programs stored in semiconductor memories or other media. Laws in the Italy and other countries preserve for Telit and its licensors certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Telit and its licensors contained herein or in the Telit products described in this instruction manual may not be copied, reproduced, distributed, merged or modified in any manner without the express written permission of Telit. Furthermore, the purchase of Telit products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Telit, as arises by operation of law in the sale of a product.

Computer Software Copyrights

The Telit and 3rd Party supplied Software (SW) products described in this instruction manual may include copyrighted Telit and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the Italy and other countries preserve for Telit and other 3rd Party supplied SW certain exclusive rights for copyrighted computer programs, including the exclusive right to copy or reproduce in any form the copyrighted computer program. Accordingly, any copyrighted Telit or other 3rd Party supplied SW computer programs contained in the Telit products described in this instruction manual may not be copied (reverse engineered) or reproduced in any manner without the express written permission of Telit or the 3rd Party SW supplier. Furthermore, the purchase of Telit products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Telit or other 3rd Party supplied SW, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.



Usage and Disclosure Restrictions

License Agreements

The software described in this document is the property of Telit and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

Copyrighted Materials

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Telit

High Risk Materials

Components, units, or third-party products used in the product described herein are NOT fault-tolerant and are NOT designed, manufactured, or intended for use as on-line control equipment in the following hazardous environments requiring fail-safe controls: the operation of Nuclear Facilities, Aircraft Navigation or Aircraft Communication Systems, Air Traffic Control, Life Support, or Weapons Systems (High Risk Activities”). Telit and its supplier(s) specifically disclaim any expressed or implied warranty of fitness for such High Risk Activities.

Trademarks

TELIT and the Stylized T Logo are registered in Trademark Office. All other product or service names are the property of their respective owners.

Copyright © Telit Communications S.p.A.



Contents

1.	Introduction	7
1.1.	Scope.....	7
1.2.	Audience.....	8
1.3.	Contact Information, Support.....	8
1.4.	Document Organization	9
1.5.	Text Conventions	9
1.6.	Related Document.....	9
2.	Document History.....	10
3.	SMS Protocol.....	12
3.1.	Requirements.....	12
3.1.1.	Preliminary Requirements.....	12
3.1.2.	Alerts.....	13
3.1.2.1.	RTS/CTS/DCD handshaking	14
3.2.	Upgrade Process.....	15
3.2.1.	Remote Registration.....	16
3.2.2.	Provisioning.....	17
3.2.3.	Update.....	18
3.2.3.1.	Firmware update failure handling.....	20
3.3.	Test.....	20
3.4.	Query	20
4.	Combined SMS-TCP/IP Protocol	22
4.1.	Requirements.....	22
4.1.1.	Preliminary Requirements.....	22
4.1.2.	Alerts.....	23
4.1.2.1.	RTS/CTS/DCD handshaking	23
4.2.	Upgrade Process.....	24
4.2.1.	Remote Registration.....	25
4.2.2.	Update.....	26
4.2.2.1.	Firmware update failure handling.....	29
4.3.	Test.....	29
4.4.	Query.....	29



5. TCP/IP Protocol	31
5.1. Requirements.....	31
5.1.1. Preliminary Requirements.....	31
5.1.2. Alerts.....	32
5.1.2.1. RTS/CTS/DCD handshaking	33
5.2. Upgrade Process.....	33
5.2.1. Remote Registration.....	34
5.2.2. Update.....	35
5.2.2.1. Firmware update failure handling.....	36
6. URC Disabling	37
7. Critical Scenario.....	38
8. Firmware Certification Program	40
9. Appendix	41
9.1. Commands parameters stored during update process	41
10. Abbreviations and acronyms	42



1. Introduction

Premium FOTA Managements provides a cost-effective, fast, secure and reliable way for wirelessly re-flashing the firmware on mobile devices, ensuring that embedded software is up-to-date with the latest enhancements and features.

The ability to manage software over-the-air is a necessary requirement for all users who design m2m products because of long lifecycles of m2m enabled products. The lifecycle of m2m enabled applications in the market ranges from 5-10 years. Downloading firmware version updates with new features represents an important new capability for m2m applications. It does away with the need to have the device updated in the field by technicians, cutting costs and timing of maintenance of the fielded applications. Such issues typically arise from a network configuration, a network software update to „fixing bugs“ or the introduction of new additional features into the Telit module required by the market.

Telit, which has signed a partnership agreement with the worldwide leader of Mobile Software Management Red Bend, has integrated in its own proprietary protocol the unique vCurrent® Mobile Update Installer and Update Generator software for use in its m2m product portfolio. Telit is therefore able to update its products, using Firmware Over The Air (FOTA) technology, by transmitting only a delta file, which represents the difference between one firmware version and another.

VCurrent® is a registered trademark of Red Bend Software Inc.

1.1. Scope

Scope of this document is to provide all necessary information about Premium FOTA Managements, and how to design an application that benefits from these services.



1.2. Audience

This document is intended for those users that need to develop applications dealing with FOTA service.



WARNING-

Note that this service will be enabled only after signing specific agreement with Telit. Users, who want to benefit from this service, must pass through the Telit certification program, where Telit will assist the customer in validating the correct implementation of firmware update service.

1.3. Contact Information, Support

For general contact, technical support, to report documentation errors and to order manuals, contact Telit's Technical Support Center (TTSC) at:

TS-EMEA@telit.com
TS-NORTHAMERICA@telit.com
TS-LATINAMERICA@telit.com
TS-APAC@telit.com

Alternatively, use:

<http://www.telit.com/en/products/technical-support-center/contact.php>

For detailed information about where you can buy the Telit modules or for recommendations on accessories and components visit:

<http://www.telit.com>

To register for product news and announcements or for product questions contact Telit's Technical Support Center (TTSC).

Our aim is to make this guide as helpful as possible. Keep us informed of your comments and suggestions for improvements.

Telit appreciates feedback from the users of our information.



1.4. Document Organization

This document contains the following chapters:

Chapter 1:	contains helping sub-channels.
Chapter 2:	Document History.
Chapter 3:	describes FOTA based on SMS protocol.
Chapter 4:	describes FOTA based on SMS-TCP/IP protocols.
Chapter 5:	describes FOTA based on TCP/IP protocol.
Chapter 6:	describes how to operate to disable URCs.
Chapter 7:	describes a critical scenario.
Chapter 8:	how to benefit from FOTA Service.
Chapter 9:	Appendix.
Chapter 10:	Abbreviation and acronyms.

1.5. Text Conventions



Danger – This information MUST be followed or catastrophic equipment failure or bodily injury may occur.



Caution or Warning – Alerts the user to important points about integrating the module, if these points are not followed, the module and end user equipment may fail or malfunction.



Tip or Information – Provides advice and suggestion that may be useful when integrating the module.

All dates are in ISO 8601 format, i.e. YYYY-MM-DD.

1.6. Related Document

- [1] AT Commands Reference Guide, 80000ST10025a
- [2] HE910/UE910/UL865 AT Commands Reference Guide, 80378ST10091A
- [3] /
- [4] PFM Certification Program Application Note, 80000nt10022a
- [5] PFM Product Description, 80287ST10048a



2. Document History

Revision	Date	Changes
ISSUE #0	2008-03-18	First Issue
ISSUE #1	2008-07-17	Updated applicability table
ISSUE #2	2008-07-18	Updated applicable products table Title changed into the proper name of the service. Introduction changed Premium FOTA Managements Certification Program chapter added.
ISSUE #3	2008-07-17	Updated applicable products table Updated preliminary requirements Updated alert list Added § 3.3.1 "Expected times" Added § 3.3.2 Firmware update failure handling Added § 6 Critical scenario Added new § 8 "Appendix" Review of document layout
ISSUE #4	2008-11-06	Highlighted that the PFM support for the GE863-PRO3 products, is available for the GSM/GPRS engine only, and will be available for the ARM application in a later phase.
ISSUE #5	2009-02-06	Updated applicability list Title changed into proper name Highlighted the importance of registration sms.
ISSUE #6	2010-02-23	Added "Related Document" paragraph Deleted AT#OTASUAN description and added note referring to AT Commands reference Guide Added command +IPR to table in "Commands parameters stored during update process" paragraph Added note on DTE speed in "Alerts" paragraph Added AT+CGCLASS in "Alerts" paragraph to the list of AT commands inhibited during delta firmware download Added explanation about automatic update in 3.3 paragraph Adapted URC text to module: #OTAEV: Server notified about successful FW Upgrade Added information about no class 7 bit SMS Added to applicability table the GE863 Pro ³ 128/64, GE864-QUAD V2, UC864-E, UC864-G, UC864-WD/WDU, UC864-E-AUTO and GE865. Removed GC864-QUAD-C2 form applicability table.



PFM Application Note
80000NT10013a Rev.14, 2014-12-04

		Applied new format
ISSUE #7	2010-06-29	Changed string " #OTAEV: Server notified about successful FW Upgrade ": did not correspond to the real one
ISSUE #8	2010-09-24	Added "Combined SMS-TCP/IP protocol" chapter Changed string " #OTAEV: Server notified about successful FW Upgrade ": did not correspond to the real one Changed note on NVM in 3.1.2 Added GL865 to the applicability table
ISSUE #9	2011-01-13	Added "TCP/IP protocol" chapter Aligned, in all chapters, paragraphs "Test" and "Query" Updated figures Minor edits
ISSUE #10	2011-02-10	Update applicability table Added note on chapter 3 and 4
ISSUE #11	2012-08-08	Added a better explanation on chapter 2.2.1
ISSUE #12	2012-11-29	Updated Applicability Table: added GE864-GPS, GL865-QUAD, GE910-QUAD, HE910 Family; removed: GM862-GPS, GC864-DUAL, GC864-QUAD-SIM-HOLDER, GE863-GPS, GE863-SIM, GE863-PRO3, and UC Family. Updated the format of the document. Removed two chapters called each one: Expected times.
ISSUE #13	2013-05-07	Updated Applicability Table.
ISSUE #14	2014-12-04	Updated Applicability Table.



3. SMS Protocol

In general, firmware update operations are based on a protocol for communication between module and server. Specifically, this protocol can entirely rely on SMSs or can use the TCP/IP. This section deals with SMS protocol, the next with TCP/IP protocol.

3.1. Requirements



WARNING: the **Requirements** listed in paragraph 3.1.1 and **Alerts** in paragraph 3.1.2 must be fully respected otherwise the firmware update service is not guaranteed.

3.1.1. Preliminary Requirements

In order to benefit from Telit's firmware update service the following requirements must be fulfilled:

- The SIM needs to have enabled internet connection
- The SIM needs to have enabled SMS service also in roaming
- After the update, the PIN insertion must be managed by the external application or the Python script
- To perform the update procedure, the external application or the Python script has to confirm the update request
- For every firmware update service enabled module, the client has to provide to Telit the IMEI and the phone number (MSISDN) of the on board SIM
- If the GPRS bearer is used to download the delta firmware file:
 - The SIM needs to have GPRS traffic enabled
 - The GPRS Auto attach flag has to be set to 1
 - The GPRS class must not be set to "CC"
- If the CSD bearer is used to download the delta firmware file:
 - The GPRS class must not be set to "CG"



3.1.2. Alerts

Please, pay attention on the following module behavior when you are performing firmware update:

- During the delta firmware file download the module must not be powered off
- During the delta firmware file download the following AT commands are inhibited:
 - AT#GPRS
 - AT#SGACT
 - AT+CGATT
 - AT+CGACT
 - ATD
 - AT+COPS=2
 - AT+CFUN=4
 - AT+CGCLASS
- The file system will remain unchanged after a firmware update. The NVM stored configuration will be lost after a firmware update; only the setting regarding the parameters listed in 9.1 will be kept.



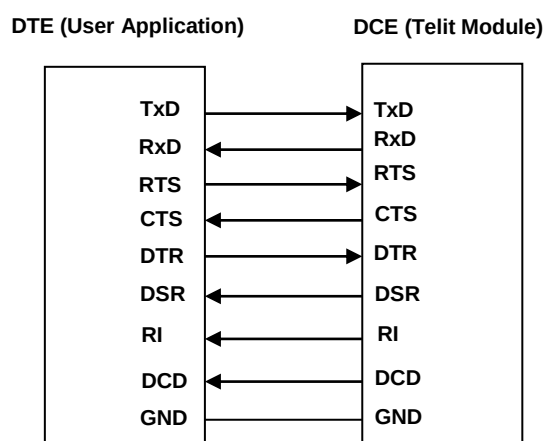
WARNING: the external application or the Python scripts are responsible of restoring the settings made before the firmware update.

- Every active context, socket, FTP or call will be closed before starting the delta firmware file download.
- The server will send class 0, 8 bit or no class, 7 bit SMS to the module. After these are recognized as firmware update SMS, they will be handled and then silently discarded from the module.
- During the flash updating the Python interpreter is halted (no script execution).
- During the delta firmware validation and the flash updating the AT interface is frozen.
- If the DTE speed is set to autobauding, then, after the reboot performed during the firmware update, the unsolicited result codes prompted on the AT interface could be lost. To avoid this, it is necessary to set the DTE speed to the DCE speed using the AT+IPR command (For more detailed AT commands and parameters definitions please consult the AT Commands Reference Guide).



3.1.2.1. RTS/CTS/DCD handshaking

For reader convenience, here is shown the V.24 serial interface provided by the Telit Modules. During the update phase the DCD line is alternatively high and low to indicate to the user that the process is in progress, while the DSR and RTS lines are low.



3.2. Upgrade Process

The preliminary SMS based phase is called Remote Registration and that permits the server to know the association between device IMEI and phone number of the on board SIM. This operation is necessary only if the client does not provide to Telit the IMEI, the phone number, Firmware version, model and APN of the on board SIM for each module. The following figure shows the screenshot of the AT interface while a module is performing the operations listed below:

1. performs a **Remote Registration**; the current version is 10.00.005
2. performs the **Provisioning**
3. receives the request to update the firmware
4. accepts the request
5. performs the **Delta Firmware File Download**
6. performs the **Firmware Update**
7. **Reboots** after the update with the new firmware 10.00.006

The steps 1 and 2 are performed only once.

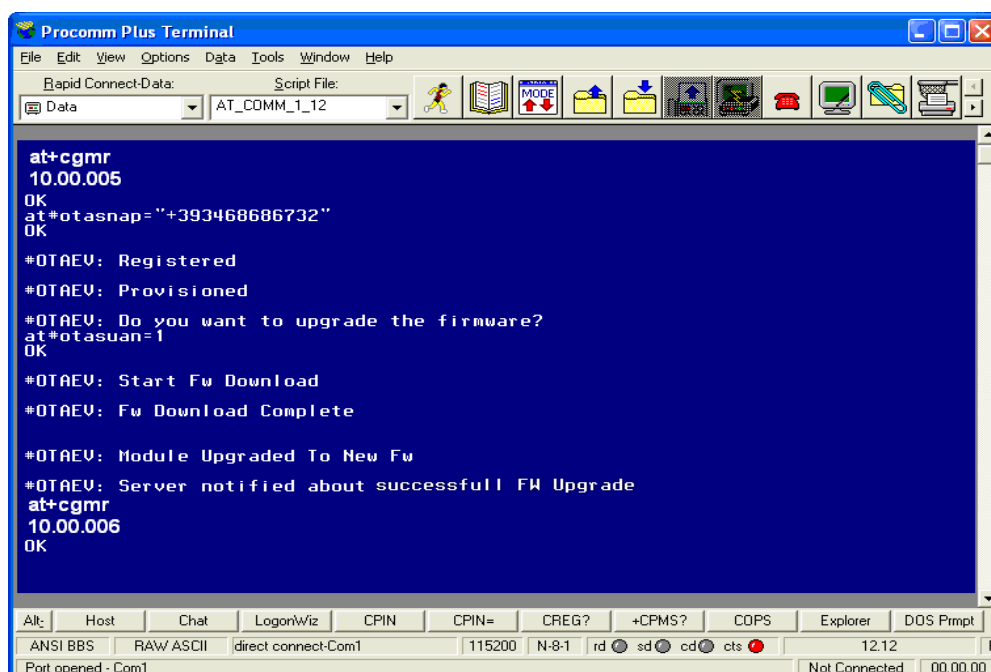


fig. 1: AT interface Screenshot of the Upgrade Process-SMS Protocol

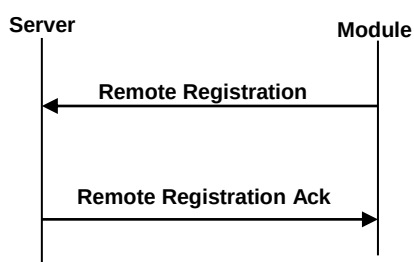


3.2.1. Remote Registration

In order to send a SMS containing all the needed information (IMEI, phone number, model, IMSI, current PLMN) from the module to the server, it is necessary to issue the following AT command:

- AT#OTASNAP="number"

where number represents the phone number in international format of the server. The server will respond with a SMS that ends the registration procedure. The SMS scenario is the following:



When the “Remote Registration Ack” SMS is received, the following unsolicited result code (URC) will be prompted on the AT command interface:

- #OTAEV: Registered

If, for some reason, the “Remote Registration Ack” SMS is not received, then the module will not be registered and, on every power on, the module will resend automatically the “Remote Registration” SMS.

Another way to force the “Remote Registration” SMS sending when the module is not registered, is to give again the #OTASNAP command.

If a module is still registered and after that the SIM is changed, the module will send automatically the Remote Registration SMS, because the server needs to be updated with the new information regarding the SIM (number, IMSI, etc). If you want to avoid this behavior, please simply run

- AT#OTASNAP=""



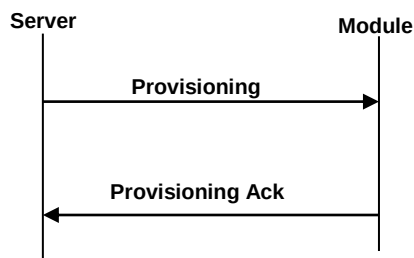


NOTE: the issue of #OTASNAP command, i.e. the issue of registration SMS, must be performed at least once. In this way PFM server knows the parameters of that specific module. Moreover, the issue of OTASNAP command informs Telit module that it is going to use PFM service; this means that after the first issue of OTASNAP, Telit module will send a registration SMS each time the SIM card is changed

3.2.2. Provisioning

Before the first update, a preliminary operation called provisioning will be performed. This has the goal to provide the module with the data relating the GPRS network access point or the CSD number, which the module needs to set up the delta firmware file download.

The server sends the *Provisioning* SMS to the module and this responds with the *Provisioning Ack* SMS. The scenario is the following:



3.2.3. Update

The update operation begins with the Command SMS, see figure below, (containing the FTP server address and credentials) sent from the server to the module. In this message the server requires the module to start the procedure either automatically (without client – user - interaction) or manually (with client – user - interaction): this is an option decided by the server side.

- In the automatic case the following unsolicited result code will be prompted on the AT interface:
 - **#OTAEV: Automatic Fw Upgrade Requested**
- In the manual case the following unsolicited result code will be prompted on the AT interface, see fig. 1:
 - **#OTAEV: Do you want to upgrade the firmware?**

If the user wants to accept this request, it has to provide a response in 60 seconds, giving the following AT command:

- AT#OTASUAN=1

In both cases a Command Ack SMS is sent to acknowledge the server and, in the same time, the module starts the procedure of downloading the delta firmware file by opening a FTP connection with the FTP server. When the module starts to download the delta firmware file the following unsolicited result code will be prompted on the AT interface:

- #OTAEV: Start Fw Download

When the delta firmware file download is terminated, a Command Progress SMS will be sent to the server and the following unsolicited result code will be prompted on the AT interface:

- #OTAEV: Fw Download Complete

At this point, the module checks the delta firmware file validity and in case, it starts the updating phase.



At the end of this phase, the module restarts with the new firmware and the following unsolicited result code will be prompted on the AT interface:

- **#OTAEV: Module Upgraded To New FW**

A Command Final SMS is sent to the Server and, if this operation is successful, the following unsolicited result code will be prompted on the AT interface:

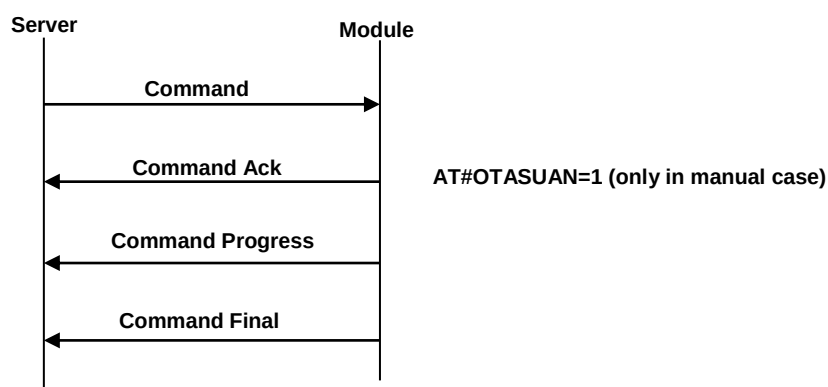
- **#OTAEV: Server notified about successful FW Upgrade**

Now, the procedure is completed.

In case, at any of above described steps, something goes wrong (the delta firmware file is bad, the ftp connection opening fails, etc.) a SMS containing the error code will be sent to the server and the following unsolicited result code will be prompted on the AT interface:

- **#OTAEV: OTA FW Upgrade Failed**

Usually, the update scenario is the following:



3.2.3.1. Firmware update failure handling

Possible causes for firmware update failure can be:

- Delta firmware file corruption: the version of the downloaded delta file is wrong or the file is corrupted due for example to a partial download;
- FTP error during the download;
- GPRS context activation error or CSD call setup error.

In these cases the firmware update process is interrupted, a URC is sent through the serial port while the module goes on working properly and the external application continues to control it as before the firmware update process.

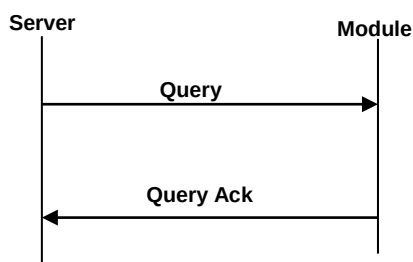
A power supply failure (voltage drop, battery fail...) during firmware update phase is fail proof. In case of power fail during updating phase, the module, at the next restart, will recognize the interruption of the former updating process. It will perform the updating process restarting from the point of interruption. The update process will be completed without any external action.

3.3. Test

On initiative of the server, the test operation can be started to simulate the delta firmware file download operation. In this case the update is not performed, but only the SMS protocol involved in firmware download is exercised between the server and the module.

3.4. Query

The query operation forces the module to send a SMS to the server containing all the information concerning the module: IMEI, phone number, model, IMSI, current PLMN. The scenario is the following:



When the module receives the Query SMS, the following unsolicited result code will be prompted on the AT command interface:

- **#OTAEV: Notified**



4. Combined SMS-TCP/IP Protocol

The idea is to use the TCP/IP protocol to exchange messages between module and server. An SMS is sent by the server to trigger the TCP/IP connection from the module as described in paragraph 4.2.

4.1. Requirements



WARNING: the **Requirements** listed in paragraph 4.1.1 and **Alerts** in paragraph 4.1.2 must be fully respected otherwise the firmware update service is not guaranteed.

4.1.1. Preliminary Requirements

In order to benefit from Telit firmware update service the following requirements must be fulfilled:

refer to Tab. 1	
Software Version equal/greater than:	Combined SMS-TCP/IP Protocol
10.00.xx3	available
13.00.xx2	available
12.00.xx.2	available

- The SIM needs to have enabled internet connection
- The SIM needs to have enabled SMS service also in roaming
- After the update, the PIN insertion must be managed by the external application or the Python script
- To perform the update procedure, the external application or the Python script has to confirm the update request
- For every firmware update service enabled module, the client has to provide to Telit the IMEI and the phone number (MSISDN) of the on board SIM
- If the GPRS bearer is used for the firmware update protocol and to download the delta firmware file:
 - The SIM needs to have GPRS traffic enabled
 - The GPRS Auto attach flag has to be set to 1
 - The GPRS class must not be set to "CC"
- If the CSD bearer is used for the firmware update protocol and to download the delta firmware file:



- The GPRS class must not be set to “CG”

4.1.2. Alerts

Please pay attention on the following module behavior when you are performing firmware update through TCP/IP protocol:

- During the entire upgrade process the module must not be powered off
- During the entire upgrade process the following AT commands are inhibited:
 - AT#GPRS
 - AT#SGACT
 - AT+CGATT
 - AT+CGACT
 - ATD
 - AT+COPS=2
 - AT+CFUN=4
 - AT+CGCLASS
- The file system will remain unchanged after a firmware update. The NVM stored configuration will be lost after a firmware update; only the setting regarding the parameters listed in 9.1 will be kept.



WARNING: the external application or the Python scripts are responsible of restoring the settings made before the firmware update.

- Every active context, socket, FTP or call will be closed before starting the upgrade process.
- The server will send class 0, 8 bit or no class, 7 bit SMS to the module. After these are recognized as firmware update SMS, they will be handled and then silently discarded from the module.
- During the upgrade process the Python interpreter is halted (no script execution).
- During the upgrade process the AT interface is frozen.
- If the DTE speed is set to autobauding, then, after the reboot performed during the firmware update, the unsolicited result codes prompted on the AT interface could be lost. To avoid this, it is necessary to set the DTE speed to the DCE speed using the AT+IPR command (For more detailed AT commands and parameters definitions please consult the AT Commands Reference Guide).

4.1.2.1. RTS/CTS/DCD handshaking

Refer to § 3.1.2.1.



4.2. Upgrade Process

The preliminary TCP/IP based phase is called Remote Registration and it permits the server to know the association between device IMEI and phone number of the on board SIM, just as in the SMS case. This operation is necessary only if the client does not provide to Telit the IMEI, the phone number, Firmware version, model and APN of the on board SIM for each module. The following figure shows the screenshot of the AT interface while a module is performing the operations listed below:

1. performs a **Remote Registration**
2. receives a message containing the data relating to the GPRS network access point or to the CSD number
3. opens a TCP/IP connection to the server and sends an acknowledge
4. receives the request to update the firmware
5. accepts the request
6. performs the **Delta Firmware File Download**
7. performs the **Firmware Update**
8. **Reboots** after the update with the new firmware

The step 1 is performed only once.

```
at+cgmr
10.00.005
OK
at#otasnapipcfg=2,"ibox.tim.it"
OK
at#otasnapip= port,hostname,"+39335475718"
OK
#OTA EV: Registered
#OTA EV: Do you want to upgrade the firmware?
at#otasuan=1
OK
#OTA EV: Start Fw Download
#OTA EV: Fw Download Complete
#OTA EV: Module Upgraded To New Fw
at+cpin=6755
OK
#OTA EV: Server notified about successfull FW Upgrade
at+cgmr
10.00.006
ok
```

fig. 2: AT interface Screenshot of the Upgrade Process-Combined Protocol

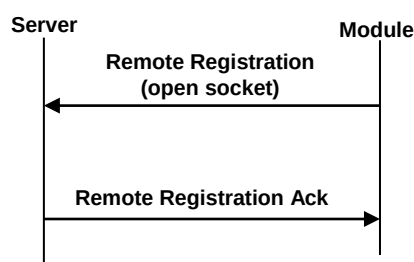


4.2.1. Remote Registration

In order to open a TCP/IP connection from the module to the server and send a message containing all the needed information (IMEI, phone number, model, IMSI, current PLMN), it is necessary to issue the following two AT commands:

- AT#OTASNAIPCFG=<bearer>,<APN>[,<username>,<password>]
- AT#OTASNAIP=<IPort>,<IPaddr>[,<mynumber>]

where <IPort> and <IPAddr> represent the IP Port and Address of the server. The module closes all the calls and all the PDP contexts and opens a TCP/IP socket connection toward the server; through this socket it sends the message. The server replies with a message that ends the registration procedure. The scenario is the following:



When the Remote Registration Ack is received, the following unsolicited result code will be prompted on the AT command interface:

- #OTAEV: Registered

A way to force the Remote Registration sending when the module is not registered is to give again the #OTASNAPIP command.

If a module is still registered and after that the SIM is changed, the module will do automatically the Remote Registration via SMS, because the server needs to be updated with the new information regarding the SIM (number, IMSI, etc).





NOTE: the issue of #OTASNAIP command, i.e. the issue of registration TCP/IP message, must be performed at least once. In this way PFM server knows the parameters of that specific module. Moreover, the issue of OTASNAIP command informs Telit's module that it is going to use PFM service; this means that after the first issue of OTASNAIP, Telit module will send a registration SMS message each time the SIM card is changed.

4.2.2. Update

The update operation begins with a Command SMS from the server, refer to figure below, containing the data relating to the GPRS network access point or to the CSD number.

In this message the server requires the module to start the procedure either automatically (without client `-user-` interaction) or manually (with client `-user-` user interaction): this is an option decided by the server side.

- In the automatic case the following unsolicited result code will be prompted on the AT interface:
 - **#OTAEV: Automatic Fw Upgrade Requested**
- In the manual case the following unsolicited result code will be prompted on the AT interface, refer to fig. 2:
 - **#OTAEV: Do you want to upgrade the firmware?**

If the client wants to accept this request, it has to provide a response in 60 seconds, giving the following AT command:

- AT#OTASUAN=1

In both cases the module then closes all the calls and all the PDP contexts and opens a TCP/IP socket connection to the server.

Through this socket it sends a Command Ack message and receives from the server a Command Progress message (containing the FTP server address and credentials).

The module starts the procedure of downloading the delta firmware file by opening a FTP connection with the FTP server. When the module starts to download the delta firmware file the following unsolicited result code will be prompted on the AT interface:



- **#OTAEV: Start Fw Download**

When the delta firmware file download is terminated, a Command Progress Ack message will be sent to the server via TCP/IP and the following unsolicited result code will be prompted on the AT interface:

- **#OTAEV: Fw Download Complete**

At this point, the module checks the delta firmware file validity and in case, it starts the updating phase.

At the end of this phase, the module restarts with the new firmware and the following unsolicited result code will be prompted on the AT interface:

- **#OTAEV: Module Upgraded To New FW**

At this point the module has to open a new TCP/IP socket connection to the server in order to send a Command Final message. If this operation is successful, the following unsolicited result code will be prompted on the AT interface:

- **#OTAEV: Server notified about successful FW Upgrade**

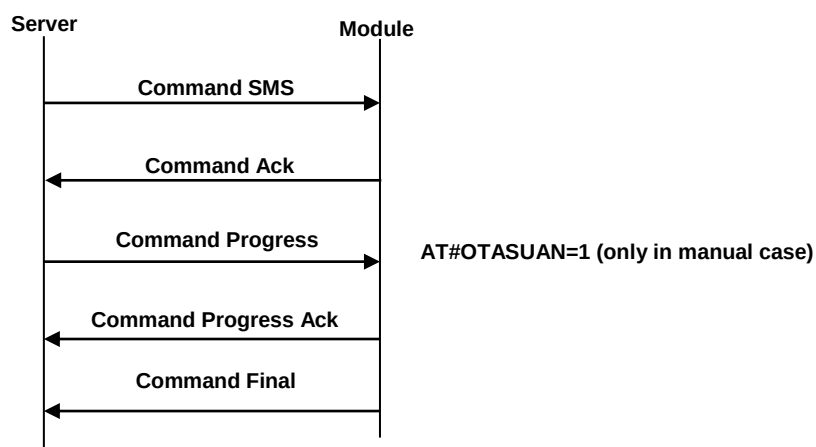
Now, the procedure is completed.

In case, at any of above described steps, something goes wrong (the delta firmware file is bad, the ftp connection opening fails, etc.) a TCP/IP message containing the error code will be sent to the server and the following unsolicited result code will be prompted on the AT interface:

- **#OTAEV: OTA FW Upgrade Failed**



Usually, the update scenario is the following:



4.2.2.1. Firmware update failure handling

Possible causes for firmware update failure can be:

- Delta firmware file corruption: the version of the downloaded delta file is wrong or the file is corrupted due for example to a partial download;
- FTP error during the download;
- GPRS context activation error or CSD call setup error.

In these cases the firmware update process is interrupted, a URC is sent through the serial port while the module goes on working properly and the external application continues to control it as before the firmware update process.

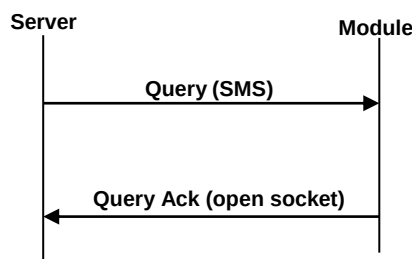
A power supply failure (voltage drop, battery fail...) during firmware update phase is fail proof. In case of power fail during updating phase, the module, at the next restart, will recognize the interruption of the former updating process. It will perform the updating process restarting from the point of interruption. The update process will be completed without any external action.

4.3. Test

On initiative of the server, the test operation can be started to simulate the delta firmware file download operation. In this case the update is not performed, but only the TCP/IP protocol involved in firmware download is exercised between the server and the module.

4.4. Query

The query operation forces the module to open a TCP/IP connection toward the server and send a message containing all the information concerning the module: IMEI, phone number, model, IMSI, current PLMN. The scenario is the following:



When the module receives the Query SMS, the following unsolicited result code will be prompted on the AT command interface:

- **#OTAEV: Notified**



5. TCP/IP Protocol

It is possible to use only the TCP/IP protocol and avoid using the SMS protocol, starting the Update process from the module and not from the server.

5.1. Requirements



WARNING: the Requirements listed in paragraph 5.1.1 and Alerts in paragraph 5.1.2 must be fully respected otherwise the firmware update service is not guaranteed.

5.1.1. Preliminary Requirements

In order to benefit from Telit's firmware update service the following requirements must be fulfilled:

refer to Tab. 1	
Software Version equal/greater than:	TCP/IP Protocol
10.00.xx4	available
13.00.xx2	available
12.00.xx.2	available

- The SIM needs to have enabled internet connection
- After the update, the PIN insertion must be managed by the external application or the Python script
- To perform the update procedure, the external application or the Python script has to request the update
- For every firmware update service enabled module, the client has to provide to Telit the IMEI and the phone number (MSISDN) of the on board SIM
- If the GPRS bearer is used for the firmware update protocol and to download the delta firmware file:
 - The SIM needs to have GPRS traffic enabled
 - The GPRS Auto attach flag has to be set to 1
 - The GPRS class must not be set to “CC”
- If the CSD bearer is used for the firmware update protocol and to download the delta firmware file:
 - The GPRS class must not be set to “CG”



5.1.2. Alerts

Please pay attention on the following module behaviors when you are performing firmware update through TCP/IP protocol:

- During the entire upgrade process the module must not be powered off
- During the entire upgrade process the following AT commands are inhibited:
 - AT#GPRS
 - AT#SGACT
 - AT+CGATT
 - AT+CGACT
 - ATD
 - AT+COPS=2
 - AT+CFUN=4
 - AT+CGCLASS
- The file system will remain unchanged after a firmware update. The NVM stored configuration will be lost after a firmware update; only the setting regarding the commands listed in 9.



WARNING: the external application or the Python scripts are responsible of restoring the settings made before the firmware update.

- Every active context, socket, FTP or call will be closed before starting the upgrade process.
- During the upgrade process the Python interpreter is halted (no script execution).
- During the upgrade process the AT interface is frozen.
- If the DTE speed is set to autobauding, then, after the reboot performed during the firmware update, the unsolicited result codes prompted on the AT interface could be lost. To avoid this, it is necessary to set the DTE speed to the DCE speed using the AT+IPR command (For more detailed AT commands and parameters definitions please consult the AT Commands Reference Guide).



5.1.2.1. RTS/CTS/DCD handshaking

Refer to § 3.1.2.1.

5.2. Upgrade Process

The preliminary TCP/IP based phase is, also in this case, the Remote Registration. It permits the server to know the association between device IMEI and phone number of the on board SIM. This operation is necessary only if the client does not provide to Telit the IMEI, the phone number, Firmware version, model and APN of the on board SIM for each module. The following figure shows the screenshot of the AT interface while a module is performing the operations listed below:

1. performs a **Remote Registration**
2. **starts an Update**, opening a TCP/IP connection to the server and receiving information about the FTP server.
3. performs the **Delta Firmware File Download**
4. performs the **Firmware Update**
5. **Reboots** after the update with the new firmware

The step 1 is performed only once.

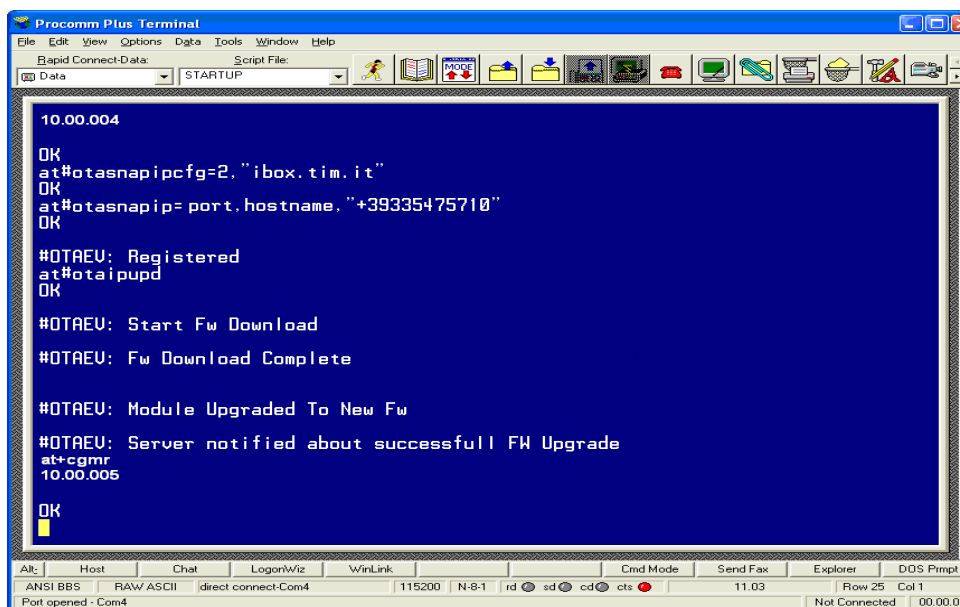


fig. 3: AT interface Screenshot of the Upgrade Process-TCP/IP Protocol

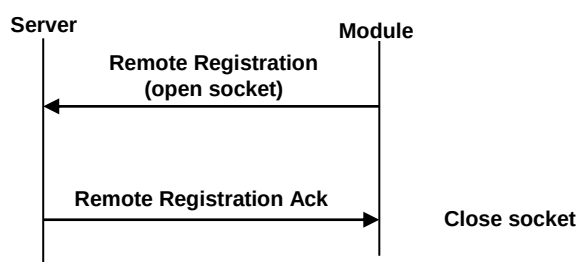


5.2.1. Remote Registration

In order to open a TCP/IP connection from the module to the server and send a message containing all the needed information (IMEI, phone number, model, IMSI, current PLMN), it is necessary to issue the following two AT commands:

- AT#OTASNAIPCFG=<bearer>,<APN>[,<username>,<password>]
- AT#OTASNAIP=<IPort>,<IPaddr>[,<mynumber>]

where <IPort> and <IPAddr> represent the IP Port and Address of the server. The module closes all the calls and all the PDP contexts and opens a TCP/IP socket connection toward the server; through this socket it sends the message. The server replies with a message that ends the registration procedure. The scenario is the following:



When the Remote Registration Ack is received, the following unsolicited result code will be prompted on the AT command interface, refer to fig. 3:

- #OTAEV: Registered

A way to force the Remote Registration sending when the module is not registered is to give again the #OTASNAPIP command.

If a module is still registered and after that the SIM is changed, the module will do automatically the Remote Registration via SMS, because the server needs to be updated with the new information regarding the SIM (number, IMSI, etc).





NOTE: the issue of #OTASNAIP command, i.e. the issue of registration TCP/IP message, must be performed at least once. In this way PFM server knows the parameters of that specific module. Moreover, the issue of OTASNAIP command informs Telit's module that it is going to use PFM service; this means that after the first issue of OTASNAIP, Telit module will send a registration SMS message each time the SIM card is changed

5.2.2. Update

The update operation begins with the AT command AT#OTAIPUPD, refer to fig. 3. The module closes all the calls and all the PDP contexts and opens a TCP/IP socket connection to the server. Note that the server IP address and IP port can be stored in non-volatile memory through the AT command AT#OTAIPCFG, or can be set in AT#OTASNAIP.

Through this socket it receives from the server a Command Progress message (containing the FTP server address and credentials), see the figure below.

The module starts the procedure of downloading the delta firmware file by opening a FTP connection with the FTP server. When the server starts to download the delta firmware file the following unsolicited result code will be prompted on the AT interface:

- **#OTAEV: Start Fw Download**

When the delta firmware file download is terminated, a Command Progress Ack message will be sent to the server via TCP/IP and the following unsolicited result code will be prompted on the AT interface:

- **#OTAEV: Fw Download Complete**

At this point, the module checks the delta firmware file validity and in case, it starts the updating phase.

At the end of this phase, the module restarts with the new firmware and the following unsolicited result code will be prompted on the AT interface:

- **#OTAEV: Module Upgraded To New FW**

At this point the module has to open a new TCP/IP socket connection to the server in order to send a Command Final message. If this operation is successful, the following unsolicited result code will be prompted on the AT interface:

- **#OTAEV: Server notified about successful FW Upgrade**

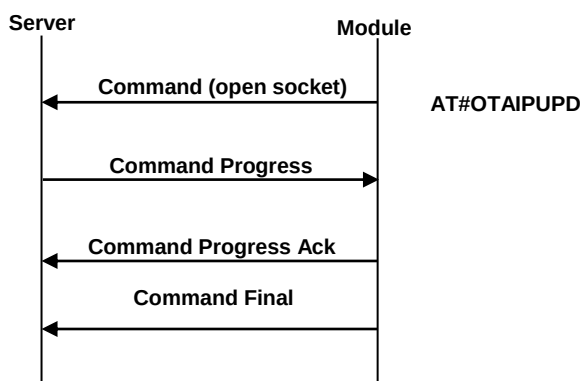


Now, the procedure is completed.

In case, at any of above described steps, something goes wrong (the delta firmware file is bad, the ftp connection opening fails, etc.) a TCP/IP message containing the error code will be sent to the server and the following unsolicited result code will be prompted on the AT interface:

- #OTA EV: OTA FW Upgrade Failed

Usually, the update scenario is the following:



5.2.2.1. Firmware update failure handling

Possible causes for firmware update failure can be:

- Delta firmware file corruption: the version of the downloaded delta file is wrong or the file is corrupted due for example to a partial download;
- FTP error during the download;
- GPRS context activation error or CSD call setup error.

In these cases the firmware update process is interrupted, a URC is sent through the serial port while the module goes on working properly and the external application continues to control it as before the firmware update process.

A power supply failure (voltage drop, battery fail...) during firmware update phase is fail proof. In case of power fail during updating phase, the module, at the next restart, will recognize the interruption of the former updating process. It will perform the updating process restarting from the point of interruption. The update process will be completed without any external action.



6. URC Disabling

To disable the unsolicited result code #OTAEV, the #OTASUAN AT command is used (the same command is used also to accept/reject a server request to update the firmware).

For more detailed AT commands and parameters definitions please consult the AT Commands Reference Guide.



7. Critical Scenario

The following critical scenario has been detected and has to be avoided:

1. there are 2 modules:
 - a. SIM A inserted in module A
 - b. [module A, SIM A] registered for the Service
 - c. SIM B inserted in module B
 - d. [module B, SIM B] registered for the Service
2. Move SIM A from module A to module B: the module A remains without SIM and the module B executes automatically a registration to communicate to the server the new SIM. After this operation, the situation is the following:
 - a. by the server side:
 - i. module A is not registered to any SIM
 - ii. [module B, SIM A] registered for Service
 - b. By the module side:
 - i. module A is without SIM but the SIM A IMSI is stored in the NVM
 - ii. SIM A inserted in module B
 - iii. [module B, SIM A] registered for Service
3. Move back SIM A from module B to module A: the module B remains without SIM. The module A doesn't execute automatically the registration because it reads from NVM the SIM A IMSI: it means that [module A, SIM A] should be already registered. After this operation the situation is the following:
 - a. by the server side:
 - i. module A is not registered to any SIM
 - ii. [module B, SIM A] registered for Service
 - b. By the module side:
 - i. SIM A inserted in module A
 - ii. [module A, SIM A] registered for Service
 - iii. module B is without SIM but the SIM A IMSI is stored in the NVM

It is now impossible to request a firmware updating of module A firmware





WARNING: SIM insertion and removing must be handled carefully.

4. Current recovery action: if the user notifies the Service Administrator its inability to update the module, the Service Administrator can overcome this impasse by asking for a forced registration. After this operation the situation is the following:
 - a. by the server side:
 - i. [module A, SIM A] registered for Service
 - ii. module B is not registered to any SIM
 - b. By the module side:
 - i. SIM A inserted in module A
 - ii. [module A, SIM A] registered for Service
 - iii. module B is without SIM but the SIM A IMSI is stored in the NVM
5. Future recovery action: the Server will maintain for every module the number of the last registration (e.g. [module A, SIM A]) and the user will have the ability to ask for a special updating of module A using this number. After this operation everything goes as in the above case (This feature is not released yet).



8. Firmware Certification Program

Customers, who want to benefit from this service, must pass through the Telit Certification Program, where Telit will assist the customer in validating the correct implementation of the Premium FOTA Management.

For information regarding how to apply for the Premium FOTA Managements Certification Program, please contact the Telit Technical Support EMEA:

TS-EMEA@telit.com
TS-NORTHAMERICA@telit.com
TS-LATINAMERICA@telit.com
TS-APAC@telit.com

Alternatively, use:

<http://www.telit.com/en/products/technical-support-center/contact.php>



9. Appendix

9.1. Commands parameters stored during update process

Command	Parameters
#ESCRPT	script name
#STARTMODESCR	Script start_mode, script_start_to
#CMUXSCR	Enable,rate
#BND	band
#AUTOBND	value
#ENS	mode
#SMSMODE	mode
#SELINT	v
#COPSMODE	Mode
#ENHSIM	Mod
+COPS	Mode, oper
#SMSATRUNCFG	muxinstance,urcmmod,timeout
#SMSATWL	index,entryType,string
#TCPATRUNCFG	connId,muxinstance,tcpPort,tcpHost tcpHostPort,tcpHost ,urcmmod,timeout,authMode,retryCnt,retryDelay
#TCPATRUNFRWL	ip_addr,net_mask
#TCPATRUNAUTH	userid,passw
+CGDCONT	cid,PDP_type,APN,PDP_addr,d_comp,h_comp
#GSMCONT	cid,P_type,CSD_num
#DNS	cid,primary,secondary
#SGACTCFG	cid,retry,delay,urcmode
#SKTSAV	-
#SKTRST	-
#SCFG	connId,cid,pktSz,maxTo,connTo,txTo
#SCFGEXT	connId,srMode,dataMode,keepalive
+IPR	rate
#STIA	Mode
#PORTCFG	Variant
+WS46	N
#ENAEVMONI	Mod
#ENAEVMONICFG	All
#EVMONI	all



NOTE: Not all the products indicated in the Applicability Table support the commands listed in the table above; refer to the AT Command Reference Guide covering the specific product to get more information.



10. Abbreviations and acronyms

APN	Access Point Name
CSD	Circuit Switched Data
CTS	Clear To Send
DCD	Data Carrier Detect
DCE	Data Communication Equipment
DTE	Data Terminal Equipment
FOTA	Firmware Over The Air
GPRS	General Packet Radio Service
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Station Identity
ISDN	International Services Digital Network
MSISDN	Mobile Station ISDN Number
NVM	Non Volatile Memory
PDP	Packet Data Protocol
PFM	Premium FOTA Management
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
RTS	Request To Send
SIM	Subscriber Identification Module
SMS	Short Message Service
URC	Unsolicited Result Code

