RYZ014 Modules

Use Cases with AT Commands

Introduction

This document will provide RYZ014-based platform users with practical use cases of AT commands.

Target Device

RYZ014 modules

Contents

1. Introduction

The host MCU can interact with the RYZ014 modem using:

- AT commands
  This is the purpose of the current document.
- The PPP protocol.
  See the document *PPP User Guide* for more details on PPP connection setup with RYZ014 modules.

After power up, the modem sends the +SYSSTART URC when the UARTs are initialized and ready to receive AT commands.

Note: Please refer to the *System Integration Guide* for more information on AT command types and AT parser implementation.

2. Network Connection

By default, the modem starts in +CFUN=0 state with minimum functionality. It does not attach to the network until the host MCU requires full functionality by setting the +CFUN state to 1.

This section helps you to connect your RYZ014-based device to the network, following these simple steps:

1. Confirm that the SIM card in your device works properly
2. Confirm that your device is correctly configured to interact with your operator's network
3. Attach your device to the network

2.1 Check that the SIM Card is Ready

2.1.1 Feature Description

Any RYZ014 module supports two SIM slots (internal and external). If an internal SIM is soldered, the AT+CSUS command switches from one slot to the other.

This section details how to check the SIM card state, as well as how to and lock or unlock the SIM card using the PIN or PUK code.

2.1.2 Use Cases

2.1.2.1 Select the SIM Slot

Command	Response	Comment
Power up the module		
	+SYSSTART	
Check the number of supported SIM slots. If the response is +CSUS: 1, skip the following steps because only one SIM slot is available on the module.		
AT+CSUS=?	+CSUS: 2 OK	The module has 2 SIM slots, it supports an external SIM (slot 0) and an internal one (slot 1).
Check the SIM slot that is configured		
AT+CSUS?	+CSUS: 1 OK	The internal SIM slot is configured
Change the SIM slot to external. First ensure that the modem is in the +CFUN=0 state, otherwise change it with AT+CFUN=0		

Command	Response	Comment
AT+CFUN?	+CFUN: 0 OK	
AT+CSUS=0	OK	Select external SIM slot
AT+CSUS?	+CSUS: 0 OK	Verify that the change was implemented
AT+CFUN=4	OK	Set the modem to airplane mode so that the SIM is read
AT+CIMI?	208019706 849013 OK	Make sure that the IMSI corresponds to that of the SIM you want to use. If CIMI is sent before the modem finishes reading the SIM card, it returns ERROR.
AT^RESET	OK	Restart the modem
	+SHUTDOWN +SYSSTART	
AT+CSUS?	+CSUS: 0 OK	The configuration is not changed at reboot

Notes: The number of SIM slots supported can be checked with AT+CSUS=?. This command can only be used when the module is in CFUN=0 state. The SIM slot configuration survives reboots and software upgrades.

2.1.2.2 Power on the SIM Slot

Select one function mode from Airplane or Full functionality. Airplane mode disables both transmit and receive RF circuits.

Command	Response	Comment
AT+CFUN=4	OK	Enter Airplane mode
	or	
AT+CFUN=1	OK	Enter Full functionality mode

2.1.2.3 Check the SIM Card Status after Powering on the SIM Slot

Command	Response	Comment
Check the SIM status		
AT+CPIN?		
	+CPIN: READY OK	The SIM card is present and unlocked, ready to use.
Option: Check the SIM card state by enabling +SQNSIMSTURC		
AT+SQNSIMST=1	OK	Enable SIM state URC
AT+CFUN=4	OK	Set the modem to airplanemode to read the SIM card
	+SQNSIMST: 1	Start reading the SIM card
	+SQNSIMST: 5	The SIM card is now ready to use
AT+SQNSIMST?	+SQNSIMST: 1,5 OK	If the URC are not enabled, it is possible to check the SIM statewith this command as well

2.1.2.4 Enable SIM Lock with PIN Code

Command	Response	Comment
AT+CLCK="SC" ,1,"0000"	OK	"SC": SIM (lock SIM/UICC card installed in the currently selected card slot) (SIM/UICC asks for password during MT power-up and when this lock command issued) 1: lock "0000": PIN code

2.1.2.5 Disable SIM Lock with PIN Code

Command	Response	Comment
Unlock SIM with correct PIN code		
AT+CPIN="0000"	OK	"0000": PIN code
Disable SIM lock with correct PIN code.		
AT+CLCK="SC",0,"0000"	OK	"SC": SIM (lock SIM/UICC card installed in the currently selected card slot) (SIM/UICC asks for password during MT power-up and when this lock command issued) 0: unlock "0000": PIN code

2.1.2.6 Enter PIN Code to Unlock SIM

Command	Response	Comment
Check current SIM card state		
AT+CPIN?		
	CPIN: SIM PIN OK	SIM PIN is required to unlock SIM card
Attempt to unlock the SIM with the "1234" PIN code		
AT+CPIN="1234"		
	ERROR	PIN code is not correct, SIM card is still locked
Attempt to unlock the SIM the with "0000" PIN code		
AT+CPIN="0000"		
	OK	PIN code is correct, SIM card unlocked
Check SIM card state		
AT+CPIN?		
	+CPIN: READY	SIM card is present and unlocked, ready to use

2.1.2.7 Enter PUK Code to Unlock SIM

Command	Response	Comment
Check current SIM card state		
AT+CPIN?		
	+CPIN: SIM PUK OK	Require SIM PUK to unlock SIM card
Type PUK code to unlock with "12345678" PUK code		
AT+CPIN="12345678"		
	ERROR	The PUK code is not correct, the SIM card is still locked
Type PUK code to unlock with "00000000" PUK code		
AT+CPIN="00000000"		
	OK	The PUK code is correct, the SIM card is unlocked
Check SIM card state		
AT+CPIN?		
	+CPIN: READY OK	The SIM card is present and unlocked, ready to use

2.1.3 Error Handling

- The SIM card is read only when the modem is in CFUN=1 (fully functional) or CFUN=4 (airplane mode) states. Trying to access the SIM card with AT commands in CFUN=0 state will result in ERROR.
- If the SIM card is not present or not detected, check that the SIM card is inserted properly to the SIM slot, and check again.

Command	Response	Comment
Enable return final result code		
AT+CMEE=2	OK	Enable +CME ERROR: <err> result code and use verbose <err> values
Check SIM card state		
AT+CPIN?		
	+CME ERROR: SIM not inserted	SIM card is not present or not detected

The AT+CSUS command requires that the UE is in CFUN=0 state. If you get an error while using the AT+CSUS command, first check how many SIM slots are supported by the module, and second confirm the CFUN=0 state.

Command	Response	Comment
Check the number of supported SIM slots (case only 1 slot)		
AT+CSUS=?	+CSUS: 1 OK	Only one SIM slot is supported (external)
Trying to switch to the internal SIM slot results in error		
AT+CSUS=1	+CME ERROR: ERROR	
If the CFUN state is 1 or 4, the SIM slot cannot be switched		
AT+CFUN?	+CFUN: 4 OK	
AT+CSUS=1	+CME ERROR: ERROR	
Change CFUN state to 0		
AT+CFUN=0	OK	
Check the number of supported SIM slots (case 2 slots)		
AT+CSUS=?	+CSUS: 2 OK	External is #0, internal is #1.
Trying to switch to the internal SIM slot succeeds		
AT+CSUS=1	OK	

2.2 Configure the Operator Mode

2.2.1 Feature Description

RYZ014 modules support up to 17 LTE bands. Scanning all the bands takes several minutes. Specifically, cell detection duration per candidate EARFCN is 30 ms/18 mJ (1.3 µAh). Scanning the full 17 bands will take 186 seconds and consume 115J (8.4 mAh).

To reduce the overall scan time, it is possible to configure the list of the bands that need to be scanned with the AT+SQNBANDSEL command.

Several operator modes are preloaded by default in the module. The operator mode can be selected with the AT+SQNCTM command.

The operator mode enables the support of specific requirements requested by the various carriers, such as:

- Supported RF bands to scan
- Predefined scanning profile

- Roaming availability
  Note: When roaming is disabled, `CEREG: 5` does not work. Only `CEREG: 1` is supported.
- Feature group in UE capability
- PDN configuration
- LwM2M support

`AT+SQNBANDSEL? command` returns the list of the predefined operator modes and their respective scan configuration. By default, the software is configured with standard operator mode.

A UE scan begins with the EARFCN to which it was attached previously. It proceeds with all the configured bands, without any precedence.

Note: See the System Integration Guide for more information on the operator modes and the scanning algorithm

2.2.2 Use Cases

2.2.2.1 Check the Currently Configured Operator Mode

Command	Response	Comment
By default the UE will be configured in the “standard” operator mode.		
`AT+SQNCTM?`	`+SQNCTM: standard` `OK`	

2.2.2.2 Limit the Number of Bands

Command	Response	Comment
Limit the number of bands to be scanned while in "standard" mode.		
Check that you are using the standard mode		
`AT+SQNCTM?`	`+SQNCTM: standard` `OK`	
If not in standard mode, change it with:		
`AT+SQNCTM="standard"`	`OK`	
	`+SHUTDOWN` `+SYSSTART`	The modem restarts
`AT+SQNCTM?`	`+SQNCTM: standard` `OK`	After reset, the CTM mode is correctly set
Check the bands that are configured for each operator modes.		

`AT+SQNBANDSEL?`	`+SQNBANDSEL: 0,3gpp-conformance,""`
	`+SQNBANDSEL: 0,att,"2,4,12"`
	`+SQNBANDSEL: 0,docomo,"1,19"`
	`+SQNBANDSEL: 0,dtag,"3,8,20"`
	`+SQNBANDSEL: 0,kddi,"18,26"`
	`+SQNBANDSEL: 0,orange,"20,3"`
	`+SQNBANDSEL: 0,softbank,"1,8"`
	`+SQNBANDSEL: 0,soracom,"2,4,12"`
	`+SQNBANDSEL: 0,sprint,"2,4,5,12,25"`
	`+SQNBANDSEL: 0,standard,"1,2,3,4,5,8,12,13,17,18,19,20,25,26,28,66"`
		17 bands are configured for the standard operator mode.

Command	Response	Comment
	+SQNBANDSEL: 0,telstra,"3,28" +SQNBANDSEL: 0,telus,"12,4,5" +SQNBANDSEL: 0,truphone,"1,2,4,8,12,20" +SQNBANDSEL: 0,verizon-no-roaming,"4,13" +SQNBANDSEL: 0,verizon,"13,4,5,12,17,20" +SQNBANDSEL: 0,vodafone,"20,8" (...) OK	
Reduce the number of bands to be scanned		
AT+SQNBANDSEL=0,"standard","3,8,20"	+SQNBANDSEL: 0,standard,"3,8,20" OK	Scan is limited to bands 3, 8 and 20.
No band has precedence over another, so enter the band in any order. More bands to scan means a longer time to attach to the network. Please keep in mind that it takes around 30 ms to scan one EARFCN.		

2.2.2.3 Select a Specific Operator Mode

Command	Response	Comment
Select a specific operator mode. If you are using an MNO SIM card, you need operator specific features to be enabled.		
AT+SQNCTM=?	+SQNCTM: ("3gpp-conformance", "ais", "aptg", "att", "bell", "cht", "cta", "dialog", "dish", "docomo", "dtag", "etisalat", "kddi", "kpn", "kt", "lgu", "orange", "ptcrb", "singtel", "skt", "softbank", "soracom", "spark", "sprint", "standard", "swisscom", "telenor", "telstra", "telus", "tim", "truphone", "turkcell", "verizon", "vodafone") OK	Check the list of supported operator modes
In this example, select “verizon” operator mode.		
AT+SQNCTM="verizon"	OK	
	+SHUTDOWN +SYSSTART	The modem restarts.
AT+SQNCTM=?	+SQNCTM: verizon OK	Read the operator mode.
For Advanced user only: You can also use +SQNBANDSEL command to reduce the number of bands scanned in a specific operator mode. It is only possible to **decrease the number of bands to be scanned and not increase it**. If you add a new band, the AT command accepts it but it is ignored during scanning. It is highly recommended to use the +SQNBANDSEL command with the standard operator mode only.		
AT+SQNBANDSEL=0,"verizon","20"	+SQNBANDSEL: 0, verizon,"20" OK	Scanning is now limited to LTE Band 20. It was previously LTE Band 13, 4, 5, 12, 17 and 20.

2.2.3 Error Handling

The AT+SQNBANDSEL command only **limits the number** of bands to be scanned compared to the default configuration. You cannot add a new band to scan with this command. If you enter the AT+SQNBANDSEL command with a band that was not set for a specific operator mode, is ignored: the command will not return any error, but the band will not be scanned.

2.3 Connect to the Network and Check that Attach is Done

2.3.1 Feature Description

This section describes how to attach to or detach from the network.

The related AT commands are:

- AT+CEREG
- AT+CFUN
- AT+CGACT
- AT+CGATT
- AT+CGCDCONT
- AT+COPS
- URC +CEREG

2.3.2 Use Cases

2.3.2.1 Attach to the Network

Command	Response	Comment
Insert a SIM card and power-on the UE		
AT+CFUN=1	OK	UE should attach to network automatically. Note that CFUN = 1 is an asynchronous command. It will return OK immediately. The OK response does not mean that the modem is attached to the network.
	+CEREG:2	By default, <n> parameter if +CEREG URC is set to 2 to enable network registration and URC.
	+CEREG:1,”0002”,”01A2 2002”,7	

2.3.2.2 Check the Network’s Registration Status

Command	Response	Comment
Query network registration status		
AT+CEREG?		
	+CEREG: 2,1 OK	2: Network registration and location information URC enabled 1: Registered, home network

2.3.2.3 Check the PDP Context Configuration

Command	Response	Comment
Get current PDP context configuration		
AT+CGDCONT?		
	+CGDCONT: 1,"IPV4V6","broadband",,,,0,0,0,0,0,0,0,,0 +CGDCONT: 2,"IPV4V6","lwaactivate",,,,0,0,0,0,0,0,0,,0 +CGDCONT: 3,"IPV4V6","custom",,,,0,0,0,0,0,0,0,,0 +CGDCONT: 4,"IPV4V6","attm2mglobal",,,,0,0,0,0,0,0,0,,0 OK	
Get current PDP context activation state		
AT+CGACT?		

Command	Response	Comment
	+CGACT: 1,1 +CGACT: 2,0 +CGACT: 3,0 +CGACT: 4,0 OK	PDP context with cid 1 is activated

2.3.2.4 Activate the PDP Context

Command	Response	Comment
AT+CGACT=1,3	OK	1: activate PDP context 3: cid 3
Query PDP context activation state		
AT+CGACT?		
	+CGACT: 1,1 +CGACT: 2,0 +CGACT: 3,1 +CGACT: 4,0 OK	PDP context with cid 3 is activated in addition of PDP context with cid 1.

2.3.2.5 Check IP Address

Command	Response	Comment
List IP address of all cids		
AT+CGPADDR	+CGPADDR: 1,"192.168.6.3","32.1.4.104.48.6.0.3.3 2.1.4.104.48.6.0.3" +CGPADDR: 2 +CGPADDR: 3,"192.168.11.2" +CGPADDR: 4 OK	cid 1, IPv4 and IPv6 address cid 2, not activated, no IP address cid 3, IPv4 address only
Query IP address of cid=1		
AT+CGPADDR=1	+CGPADDR: 1,"192.168.6.3","32.1.4.104.48.6.0.3.3 2.1.4.104.48.6.0.3" OK	cid 1, IPv4 and IPv6 address

2.3.2.6 Detach from the Network

Command	Response	Comment
AT+CFUN=0	OK	Power-off UE Note that AT+CFUN=0 is a synchronous command. The OK response is sent when the modem is detached from the network.
	+CEREG:0	If enabled, the CEREG:0 URC will immediately follow the OK response from AT+CFUN=0 command

2.3.2.7 Force an Attachment to a Specific Operator (AT+COPS)

Command	Response	Comment
AT+COPS is available only when the modem is set to full functionality (CFUN: 1 state)		
AT+CFUN=1	OK +CEREG: 2	
Deregister from the network		
AT+CGATT=0	OK +CEREG: 0	
AT+COPS=1,2,"310410",7	OK	Force the modem to attach onAT&T network
	+CEREG: 2	
	+CEREG: 5,"0936","0C702F0F",7	

2.3.3 Error Handling

2.3.3.1 If AT+CEREG? returns status 0

If AT+CEREG? returns status 0, the UE is not registered, and is not currently searching an operator to register to.

Command	Response	Comment
AT+CEREG?		Query network registration status
	+CEREG: 2,0 OK	
Possible causes: SIM card error: SIM card not detected, PIN code not entered, SIM card read error. The registration is not started (+COPS=2): execute the actions below.		
AT+CFUN?		Check if current CFUN state is 1
	+CFUN: 1 OK	
AT+CGATT=1	OK	Force EPS attach

2.3.3.2 If CEREG? returns status 2

If CEREG? returns status 2, the modem not registered, but it is currently trying to attach or is searching an operator to register to.

Command	Response	Comment
AT+CEREG?		Query network registration status
	+CEREG: 2,2 OK	
Possible causes: No network available Available networks have insufficient Rx level HPLMN or allowed PLMN are available but the registration is rejected, for example, roaming is not allowed in this Location Area		
Wait for the module to retrieve a coverage (no action required)		
	+CEREG:1	
Verify reception signal strength. In the response below <rssi> is the signal strength of the antenna, and <ber> is the bit error rate in percent. Please refer to *AT Commands User's Manual* for details on values and levels.		
AT+CSQ	+CSQ: <rssi>,<ber>	If the signal strength is low, change to a different position and try again.

2.3.3.3 If AT+CEREG? returns status 3

If AT+CEREG? returns status 3, the registration is denied.

Command	Response	Comment
AT+CEREG?		Query network registration status
	+CEREG: 2,3 OK	
Possible causes: • Illegal mobile equipment • IMSI unknown at HLR (Home Location Register) • PLMN not allowed		
Actions: 1. Check if right SIM card and right device is used 2. Check if right PLMN is selected with the command below		
AT+COPS?		Check the operator mode
	+COPS: 0,0,"Amarisoft Network",7 OK	0: automatic operator select mode 0: long format alphanumeric <oper> "Amarisoft Network": <oper> name 7: E-UTRAN

2.3.3.4 If AT+CEREG? returns status 4

If AT+CEREG? returns status 4, an unknown error occurred (for example: out of E-UTRAN coverage).

Command	Response	Comment
AT+CEREG?		Query network registration status
	+CEREG: 2,4 OK	
Check current signal strength		
AT+CSQ		
	+CSQ: 18,99 or not detectable OK	18: RSSI -77dBm 99: channel ber, not known If the signal strength is low, change to a different position and try again.

If AT+CEREG? returns status 80, a PLMN loss indication is received from RRC. Most frequently, this means that the modem got rejected from the network.

Command	Response	Comment
AT+CEREG?		Query network registration status
	+CEREG: 2,80 OK	
Check your SIM card validity		

2.3.3.5 APN Configuration

In LTE-M, APN auto configuration is sufficient in most cases. There is no need for the user to set a specific APN. In case a specific APN needs to be set, the following command can be applied. These APN settings are persistent at reboot.

On AT&T specifically, if the APN is different from the one mentioned in the above examples, the SMS services will not be functional.

Command	Response	Comment
`AT+CGDCONT=1,"IPV4V6","m2m.com.attz",,,,0,0,0,0,0,0,,0`	`OK`	Apply m2m.com.attz APN
`AT+CGDCONT?`	`+CGDCONT: 1,"IPV4V6","m2m.com.attz",,,,0,0,0,0,0,0,,0` `OK`	Check the new APN settings

3. How to Manage TLS Certificates

3.1 Feature Description

For the best security, we strongly advise that you configure mutual authentication TLS connections. For secured socket connection, it is necessary to write the certificate or the private key beforehand in the non-volatile memory. `AT+SQNSNVW` is used to write or delete data in the non-volatile memory using "`certificate`" or "`privatekey`" parameters with the specific index in the file system. The file size corresponds to the exact number of bytes to be uploaded.

After an `AT+SQNSNVW` write command is issued, the user sends certificate bytes in PEM (Privacy- enhanced Electronic Mail) format. To delete a certificate or a private key, the user simply writes a '0'-byte certificate or private key using file ID as `<index>`. A RYZ014 module holds 20 slots to store certificates and 20 slots for private keys. These files are stored on the file system of the module.

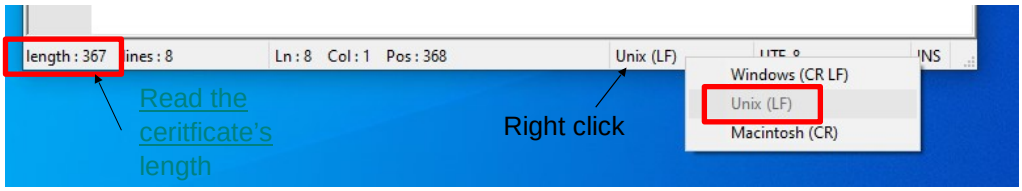
The size of a certificate cannot exceed 8 kB and the size of a private key must be less than 2 kB. Additionally, the total allocatable user non-volatile memory is 200 kB, and the `AT+SQNSNVW` returns `ERROR` when no memory space is left.

CA certificates chain is supported: it is possible to combine several root CA certificates into one. The module is preloaded with default certificates needed to connect to some operator specific LwM2M servers. To avoid erasing preloaded certificates, it is highly recommended to use slots 8 to 19 only.

3.2 Use Cases with Certificates

To get the file size, use Linux command `ls -l filename`, or DOS command `dir`, or open the file with Notepad++ to check its length.

With Notepad++, make sure to select the Unix (LF) encoding to get the right size of the certificate:



3.2.1 Identify a Free Certificate Index Entry

Command	Response	Comment
RYZ014 modules come with some pre-provisioned certificates.		
AT+SQNSNVR="certificate"		
+SQNSNVR: "certificate",1,"/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc. - For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G5","000000000000000000000000000000000000000000000000","/C=US/O=VeriSign, Inc./OU=VeriSign Trust Network/OU=(c) 2006 VeriSign, Inc. - For authorized use only/CN=VeriSign Class 3 Public Primary Certification Authority - G5","06/11/08 00:00:00","36/07/16 23:59:59","sha1RSA","00000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000000000","sha1","52b1d7e64e2e1a453322ced6aa1c993bcb11f187" +SQNSNVR: "certificate",2,"/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA","0000000000000000","/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA","06/11/10 00:00:00","31/11/10 00:00:00","sha1RSA","00000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000000000000000000000 0000000000000000000","sha1","9aacd9b54b2f972ef2e1bd488eb550afcc462d46" +SQNSNVR: "certificate",3,"/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA","0000000000000000","/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA","06/11/10 00:00:00","31/11/10 00:00:00","sha1RSA","00000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000000000000000000000 0000000000000000000","sha1","4418290c0af661843b28c70f4eb728f4cc462960" +SQNSNVR: "certificate",4,"/CN=root/OU=Service Platform Development department/O=SoftBank Corp./L=Minato-ku/C=JP","00000000000000000000000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000","/CN=root/OU=Service Platform Development department/O=SoftBank Corp./L=Minato-ku/C=JP","18/02/26 01:33:37","19/02/26 01:33:37","sha256ECDSA","000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000","sha1","38db2b4bde4278b9f460cd175ec4c04f88fbc9b8"		
	OK	
Indexes 1 to 4 are already used. If you wish to keep them and add a new certificate, choose any other index between 10 and 19.		

3.2.2 Add Certificate at Index 19

Command	Response	Comment
Upload a certificate type file with size 1078 bytes into the file system.		
AT+SQNSNVW="certificate",0,1078		
	>	
After prompt '>', enter the data from certificate file and type enter in the end.		
-----BEGIN CERTIFICATE----- MIIC8DCCAlmgAwIBAgIJAOD63PlXjJi8MA0GCSqGSIb3DQEBBQUAMIGQMQswCQYD VA+GIbdYKO3JprPxSBoRponZJvDGEZuM3N7p3S/lRoi7G5wG5mvUmaE5RAgMBAAGj ( )REyPOFdGdhBY2P1FNRy0MDr6xr+D2ZOwxs63dG1nnAnWZg7qwoLgpZ4fE SPD3PkA 1ZgKJc2zbSQ9fCPxt2W3mdVav66c6fsb7els2W2Iz7gERJSX END CERTIFICATE-----		
	OK	

3.2.3 Read Certificate at Index 19

Command	Response	Comment
AT+SQNSNVR="certificate", 19		Read certificate at index 19
	+SQNSNVR: "certificate",0,"/C=GB/ST=United Kingdom/L=Derby/O=Mosquitto/OU=CA/CN=mosquitto.org/emai lAddr ess=roger@atchoo.org","00000000000000000000000000000000000 00 000000 00000000000000000000000000000000000000(...)00000000 00000 00000000000000000000000000000000000000","/C=GB/ST=U nited Kingdom/L=Derby/O=Mosquitto/OU=CA/CN=mosquitto.org/emailAd dress=roger@atchoo.org","12/06/29 22:11:59","22/06/27 22:11:59","sha1RSA","00000000000000000000","sha1","1d21 4e931ab1 da59c 1e08f025f268d2783a51f0a" OK	

3.2.4 Remove Certificate at Index 19

Command	Response	Comment
AT+SQNSNVW="certificate",19, 0	OK	Remove certificate at index 19

3.3 Use Cases with Private Keys

3.3.1 Upload a Private Key at Index 1

Command	Response	Comment
Upload a private key type file with size 1679 bytes into file system at index 1.		
AT+SQNSNVW="privatekey",1,167 9		
	>	
After prompt '>', enter the data from certificate file and press Enter at the end.		
-----BEGIN RSA PRIVATE KEY----- MIIEpQIBAAKCAQEA0DeexyAY2TP1LeRL/MR7nVXzq+eQysfvZCzZVy39KXPtSaGL5gHjlGS2ufB9ZB3KgOxS MlF+W7oqB6xa5FLMD4YQfgQiUux6kmuQZ4r3yvCUlOxD(…)		

Command	Response	Comment
h46R1gIvDPGBeS0r7Ex4ILu WCYDIWrQ740KaxODp8+z10GfqFzKMq7eVFBl6gBtzU1JMs7L12qnx7U+rJqf0zL7 /yoN9g25RqCbUczK1h9gkwky1TVKnZDK2+gE JJjNhnbp8T4zgPiS8X/V0YypVeTnu2Yl7oXFDeHeci77DKXcGz5eWMo = -----END RSA PRIVATE KEY-----		
	OK	

3.3.2 Read the Private Key at Index 1

Command	Response	Comment
AT+SQNSNVR="privatekey",1		Read the private key at index 1
	+SQNSNVR: 1,"-----BEGIN RSA PRIVATE KEY----- MIIEpQIB (...) Gz5eWMo= "-----END RSA PRIVATE KEY----“" OK	

3.3.3 Remove the Private Key at Index 1

Command	Response	Comment
AT+SQNSNVW="privatekey",1,0	OK	Remove the private key at index 1

3.4 Use Cases to Setup a Security Profile

3.4.1 With a Private Key Stored in the Non-Volatile Memory (NVM)

Command	Response	Comment
Upload a certificate type file with size 1078 bytes into the file system.		
AT+SQNSNVW="certificate",19,1078		
	>	
After prompt '>', enter the data from certificate file and type enter in the end.		
-----BEGIN CERTIFICATE----- MIIC8DCCAlmgAwIBAgIJAOD63PlXjJi8MA0GCSqGSIb3DQEBBQUAMIGQMQswCQYD VA+GIbdYKO3JprPxSBoRponZJvDGEZuM3N7p3S/lRoi7G5wG5mvUmaE5RAgMBAAGj (…) REyPOFdGdhBY2P1FNRy0MDr6xr+D2ZOwxs63dG1nnAnWZg7qwoLgpZ4fESPD3PkA 1ZgKJc2zbSQ9fCPxt2W3mdVav66c6fsb7els2W2Iz7gERJSX -----END CERTIFICATE-----		
	OK	
Upload Server Certificate Authority on the modem		
AT+SQNSNVW="certificate",18,683		
	>	
After prompt '>', enter the data from certificate file and press Enter at the end.		
-----BEGIN CERTIFICATE----- MIIBzDCCAXECFGw5Gx1S52QxSP44Sx4pQ0ptMOKDMAoGCCqGSM49BAMCMIGLMQsw (…) xJ3LStv06Yd0EiB2cu8csxr4Z6TtApSJdCQpN+gusUQ= -----END CERTIFICATE-----		
	OK	
Upload a 1679 byte private key type file to the file system.		
AT+SQNSNVW="privatekey",0,1679		
	>	
After prompt '>', enter the data from certificate file and press Enter at the end.		

Command	Response	Comment
-----BEGIN RSA PRIVATE KEY----- MIIEpQIBAAKCAQEA0DeexyAY2TP1LeRL/MR7nVXzq+eQysfvZCzZVy39KXPtSaGL 5gHjlGS2ufB9ZB3KgOxSMlF+W7oqB6xa5FLMD4YQfgQiUux6kmuQZ4r3yvCUlOxD (…) h46R1gIvDPGBeS0r7Ex4Ilu WCYDIWrQ740KaxODp8+z10GfqFzKMq7eVFBl6gBtzU1JMs7L12qnx7U+rJqf0zL7/ yoN9g25RqCbUczK1h9gkwky1TVKnZDK2+gE JJjNhnbp8T4zgPiS8X/ V0YypVeTnu2Yl7oXFDeHeci77DKXcGz5eWMo= ---END RSA PRIVATE KEY-----		
	OK	
Setup the security profile with both certificate and private key Note that there is no requirement for the certificate sequence; the module will send everything at the certificate/privatekey index mentioned in the secure profile to the server as is.		
AT+SQNSPCFG=1,3,"",1,0,0,""	+SQNSPCFG: 1,3,"",1,0,0,"","" OK	By default, the last parameter <storageId> is set to 0 to indicate that the private key is stored in the NVM.

3.5 Error Handling

AT+SQNSNVW can return +CME ERROR: operation not supported when the certificate is not correctly formatted and that the length specified in the command does not match the content of the certificate including <CR>, <LF>, 'space' and so on.

You can use AT+SQNSNVR="certificate" and AT+SQNSNVR="privatekey" to dump all the available certificates and private keys stored in the system. If you use CA certificate chains and try to read back the slot index with AT+SQNSNVR, it only outputs the first certificate in the chain.

When using AT+SQNSNVW, if you get ERROR (CME_ERROR 4), please make sure first that the certificate is valid. If the certificate is confirmed valid, please check if you used the proper terminator for AT command. Only one char is allowed. The AT command syntax is described in the *3GPP 27.007* (§4.1 and §4.2) and *ITU V250* (§5.2.1). The termination character is <CR> by default. For example,using <CR><LF> ("\r\n") as terminator would have no impact for most of AT commands since the "\n" would be treated as invalid AT command. But for AT commands which need input data, the second char <LF> ("\n") would remain in the buffer and be treated as input data. When sending data in text mode, the module will not return ERROR, but the server would receive data starting with "\n", and this may trigger problems. When sending data in HEX mode, ERROR is sent immediately as "\n" is an invalid HEX char. The terminator char can be changed by an ATS3 command. Please refer to *AT Commands Reference Manual* for more details. When developing an application on the host MCU based on AT commands, if no specific requirements are set, please use <CR> ("\r") as the terminator character.

4. Proprietary FOTA

This section describes FOTA as a proprietary feature using the AT+SQNSUPGRADE command. It does not apply to FOTA through LwM2M.

4.1 Feature Description

The AT+SQNSUPGRADE command is used to trigger a device upgrade. The firmware is located either on an external FTP or HTTP/HTTPS server or on the file system of the device, if it was previously downloaded from any external server. The customer is responsible for hosting the firmware files on its own server. The FOTA process is a device-initiated firmware update triggered by the host system. The modem downloads the firmware file from the specified server if needed and automatically applies the update.

The firmware type must be a full DUP (a .dup file with the full software upgrade) or diff DUP (a .dup file including a differential upgrade). The differential FOTA allows the customer to upgrade the firmware or downgrade the firmware over-the-air to a new/old version. Before upgrading the firmware, the customer

needs to prepare the firmware package containing only the differences between the old and new firmware version. This reduces the amount of data transmission and accelerates the firmware upgrade.

Note: A device reboot is required to finalize the system upgrade. This can be triggered through the <reboot>parameter of AT+SQNSUPGRADE command, or any other kind of reboot (AT^RESET, AT+SQNSSHDN or a hardware reset).

The FW upgrade can be launched in foreground (synchronous upgrade) or background (asynchronous upgrade) as specified by a <command> parameter. The user can cancel upgrade by sending cancel <command> value '2' any time before the device's reboot when using the background upgrade.

Customers need to operate the following steps to upgrade the firmware:

- Get the firmware packages or differential firmware packages from the release
- Upload the differential firmware packages on an external FTP or HTTP/HTTP server.
- Execute the AT+SQNSUPGRADE command to upgrade. The module will upgrade automatically.

When the image is not already on the device file system, the FOTA process requires the modem to be registered on the network and needs to have a correctly configured PDP context. The network must allow internet access to the server hosting the files.

Once the modem's network connection has been verified, the modem can start downloading the firmware file as shown in the use cases below.

4.2 Use Cases

The test is to be run with an external server.

Note: <firmware_url> protocol can be HTTP, HTTPS or FTP (compliant with RFC1738).

4.2.1 Synchronous Upgrade using HTTPS Protocol

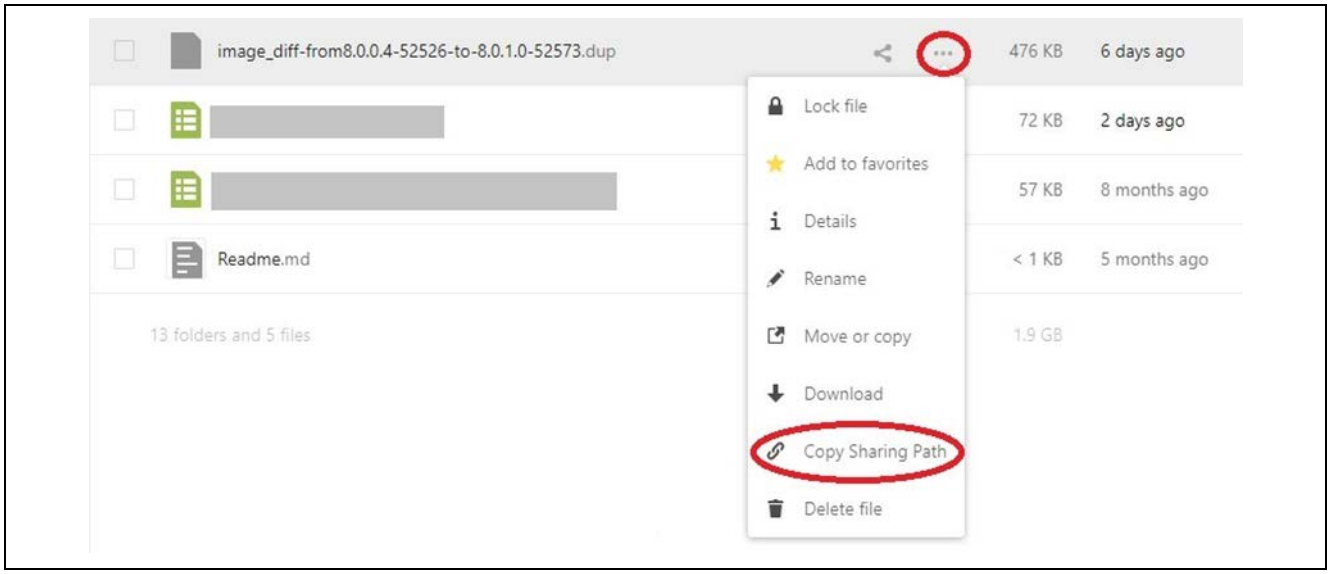
Command	Response	Comment
Launch the device upgrade.		
AT+SQNSUPGRADE="https://s3-us-west-2.amazonaws.com/FileShare/ 41613-ue.dup",1,10,0		The device will reboot automatically after the firmware is installed, and report progress every 10%, in synchronous upgrade.
	OK	
	+SQNSUPGRADE: “available”	UE can access URL
	+SQNSUPGRADE: “downloading”,0	Start download
	+SQNSUPGRADE: “downloading”,10 +SQNSUPGRADE: “downloading”,20 +SQNSUPGRADE: “downloading”,30 +SQNSUPGRADE: “downloading”,40 +SQNSUPGRADE: “downloading”,50 +SQNSUPGRADE: “downloading”,60 +SQNSUPGRADE: “downloading”,70 +SQNSUPGRADE: “downloading”,80 +SQNSUPGRADE: “downloading”,90	Progress notifications
	+SQNSUPGRADE: “downloading”,100 OK	FW is downloaded to the UE file system
	+SQNSUPGRADE: “rebooting”	Device is rebooting and going in updater mode to finish the upgrade
Upgrade duration depends on the DUP type. After upgrade is finished, the device reboots in FFF mode.		
	+SQNSUPGRADE: “installed”	Device is upgraded to the new FW
	+SYSSTART	Device is ready for operation

4.2.2 Synchronous Upgrade using HTTPS Protocol with Certificates

Command	Response	Comment
AT+SQNSPCFG=1,0,"0x002F;0x003C;0x0035;0x003D",1,5,,,"", "",0	+SQNSPCFG: 1,0,"0x002F;0x003C;0x0035;0x003D",1,5,,,"","",0 OK	Set the security profile to be used, pointing to the right certificate
AT+SQNSUPGRADE="https://ec23-134-42-3.us-east-2.compute.amaz onaws.com/naa/bl_51630.dup",1,1, 0,1		The device will reboot automatically after the firmware is installed, and report progress every 1%, in synchronous upgrade.
	+SQNSUPGRADE: "available"	UE can access the URL specified in the command
	+SQNSUPGRADE: "downloading",1	Download started
	+SQNSUPGRADE: "downloading",2 (…)	Progress notification
	+SQNSUPGRADE: "downloading",100 OK	The new SW image is downloaded and stored in the UE's file system
	+SQNSUPGRADE: "rebooting"	The UE will reboot to install the new SW image
	+SQNSUPGRADE: "installed"	Device is upgraded to the new SW image
	+SYSSTART	Device is ready for operation

4.2.3 Synchronous Upgrade using HTTPS Protocol and Credentials

It is possible to test the AT+SQNSUPGRADE command with a software image stored on the Cloud. To get the URL of the file, first connect to Sequan's Cloud (http://cloud.sequans.com) with your credentials. Then right click on the three dots next to the filename to see a menu and click on "Copy Sharing Path," as shown on the following picture. This copies/ pastes the URL of the file in your clipboard.



Command	Response	Comment
AT+SQNSUPGRADE="https:// login:pwd@cloud.sequans.com/ apps/ sharingpath/team-iot-bb- support/Internal/image_diff-from8.0.0. 4-52526- to-8.0.1.0-52573.dup",1,1,0		The credentials are hidden here, you should use your own. If there is a "@" character in your login or pwd, please replace it by its HTML encoding "%40". The device will reboot automatically after the firmware is installed, and report progress every 1%, in synchronous upgrade.
	+SQNSUPGRADE: "available"	UE can access the URL specified in the command
	+SQNSUPGRADE: "downloading",1	Download started
	+SQNSUPGRADE: "downloading",2 (…)	Progress notification
	+SQNSUPGRADE: "downloading",100 OK	The new SW image is downloaded and stored in the UE's file system
	+SQNSUPGRADE: "rebooting"	The UE will reboot to install the new SW image
	+SQNSUPGRADE: "installed"	Device is upgraded to the new SW image
	+SYSSTART	Device is ready for operation

4.2.4 Asynchronous Upgrade using HTTPS Protocol

Set the URL of the firmware, reboot automatically after the firmware is installed, report progress every 10% in asynchronous upgrade.

Command	Response	Comment
AT+SQNSUPGRADE="https://s3-us-west- 2.amazonaws.com/FileShare/ 41613-ue.dup",1,10,1		Reboot automatically after the firmware is installed, report progress every 10%, in asynchronous upgrade.
	OK	
	+SQNSUPGRADE: “available”	
	+SQNSUPGRADE: “downloading”,0	
Background upgrade, AT interface is still allowed to issue AT command, read command to check the current state of upgrade process		

Command	Response	Comment
AT+SQNSUPGRADE?	+SQNSUPGRADE: “downloading”,5 OK	
	+SQNSUPGRADE: “downloading”,10 +SQNSUPGRADE: “downloading”,20 +SQNSUPGRADE: “downloading”,30 +SQNSUPGRADE: “downloading”,40 +SQNSUPGRADE: “downloading”,50 +SQNSUPGRADE: “downloading”,60 +SQNSUPGRADE: “downloading”,70 +SQNSUPGRADE: “downloading”,80 +SQNSUPGRADE: “downloading”,90 +SQNSUPGRADE: “downloading”,100	Progress notifications
	+SQNSUPGRADE: “rebooting”	Device is rebooting and will enter updater mode to finish the upgrade
	+SYSSTART	

4.2.5 Cancel Asynchronous Upgrade with HTTPS Protocol

Command	Response	Comment
Cancelling an upgrade is possible only in asynchronous mode. (Asynchronous upgrade going on)		
	+SQNSUPGRADE: “downloading”,10 +SQNSUPGRADE: “downloading”,20 +SQNSUPGRADE: “downloading”,30 +SQNSUPGRADE: “downloading”,40	Progress notifications
Cancel upgrade if any, then returns OK		
AT+SQNSUPGRADE=“https://s3-us-west-2.amazonaws.com/FileShare/41613-ue.dup”,1,10,2		
	OK	
	+SQNSUPGRADE: “cancelled”	

4.2.6 Asynchronous Upgrade using FTP Protocol

Command	Response	Comment
Launch the asynchronous update with FTP protocol. Login is `ftpuser` and password is `ftppwd`.		
`AT+SQNSUPGRADE="ftp://ftpuse r: ftppwd@192.168.0.225/5410-4715148548-ue.dup",1,10,1`		

	`OK`
	`+SQNSUPGRADE: "available"`
	`+SQNSUPGRADE: "downloading",0`
	`+SQNSUPGRADE: "downloading",10`
	`+SQNSUPGRADE: "downloading",20`
	`+SQNSUPGRADE: "downloading",30`
	`+SQNSUPGRADE: "downloading",40`
	`+SQNSUPGRADE: "downloading",50`
	`+SQNSUPGRADE: "downloading",60`
	`+SQNSUPGRADE: "downloading",70`
	`+SQNSUPGRADE: "downloading",80`
	`+SQNSUPGRADE: "downloading",90`
	`+SQNSUPGRADE: "downloading",100`
	`+SQNSUPGRADE: "rebooting"`
	`+SQNSUPGRADE: "installed"`
	`+SYSSTART`	

4.2.7 Cancel Asynchronous Upgrade

Command	Response	Comment
Launch the asynchronous update with FTP protocol. Login is ftpuser and password is ftppwd.		
`AT+SQNSUPGRADE="ftp://ftpuse r: ftppwd@192.168.0.225/5410-4715148548-ue.dup",1,10,1`	`OK`	
	`+SQNSUPGRADE: "available"`	
`AT+SQNSUPGRADE="ftp://ftpuse r: ftppwd@192.168.0.225/5410-4715148548-ue.dup",1,10,2`	`OK`	

	`+SQNSUPGRADE: "downloading",0`
	`+SQNSUPGRADE: "downloading",10`
	`+SQNSUPGRADE: "cancelled"`	

`AT+SQNSUPGRADE?`	`+SQNSUPGRADE: "idle"` `OK`	

4.2.8 Asynchronous Upgrade though FTP using a Specific Port

Command	Response	Comment
Launch the asynchronous update with FTP protocol. Login is `ftpuser` and password is `ftppwd`, port is 8080.		
`AT+SQNSUPGRADE="ftp://ftpuse r: ftppwd@192.168.0.225:8080/5410- 47151-48548- ue.dup",1,10,1`		
	`OK`	

	`+SQNSUPGRADE: "available"`
	`+SQNSUPGRADE: "downloading",0`
	`+SQNSUPGRADE: "downloading",10`
	`+SQNSUPGRADE: "downloading",20`
	`+SQNSUPGRADE: "downloading",30`
	`+SQNSUPGRADE: "downloading",40`
	`+SQNSUPGRADE: "downloading",50`
	`+SQNSUPGRADE: "downloading",60`
	`+SQNSUPGRADE: "downloading",70`
	`+SQNSUPGRADE: "downloading",80`
	`+SQNSUPGRADE: "downloading",90`
	`+SQNSUPGRADE: "downloading",100`
	`+SQNSUPGRADE: "rebooting"`
	`+SQNSUPGRADE: "installed"`
	`+SYSSTART`	

4.3 Error Handling

If an error code (code:529) is received while the modem is trying to download the firmware files or to verify downloaded firmware reports a corrupted image, first check that the correct firmware file is used. The firmware file needed has an extension `*.dup`. The raster file (image file used for manufacturing) is not supported with this feature.

If an error (code:529) is received when the modem is trying to apply differential update, check that the diff `.dup` file is properly generated. The `.dup` package contains the changes between the current firmware version (the old version) in the device and the future firmware version.

If an error (code:531) is received while the host system is trying to initiate FOTA upgrade, check that the modem attaches on the network before starting FOTA upgrade. If the modem loses the network connection, it attempts to reattach only ten times before giving up and sending `ERROR`.

The modem cannot be powered down during the firmware download. Doing so aborts the upgrade, which has to be started again later with a new FOTA upgrade command.

If the modem lost the network connection during firmware download and receives error (code:531), the download must be restarted with a new command.

Once the file is successfully downloaded, applying the firmware update takes a few minutes to complete. If the modem is powered down during this process, the update process resumes once power is restored, but this is not recommended as URC notifications about the update may be missed.

5. Factory Reset

5.1 Feature Description

This causes the device to reset to its factory state. Both file system and the PSI (Platform Specific information) will reset to factory state. It impacts:

- All the parameters modified using the AT+SQNHWCFG command after the restauration point was created
- The entire filesystem including:
  - low power settings
  - The operator mode and the bands to be scanned.

Note: Device reboot is required to complete the operation. This can be triggered through AT^RESET, AT+SQNSSHDN, or a hardware reset.

Important: To perform a factory reset of the modem, please note that a restoration point MUST have been initially created during the module's manufacturing using the command AT+PSISAVECURRENT = "OEM". Please refer to the *Manufacturing Guide*.

The AT command AT&F executes a factory reset of the filesystem, including LPM and band configuration settings. It makes a partial reset of the HW configuration, specifically the UART settings that were changed using the following commands:

ATE ATV ATQ AT&C AT&D AT&S ATS3 ATS4 AT+IFC AT+ICF AT+IPR

This command does not know about restoration point and must not be used.

5.2 Use Cases

Command	Response	Comment
AT+SQNSFACTORYRESET		
	OK	You will get result after a while
AT^RESET	OK	Perform a device reboot to make it take effect
	+SHUTDOWN +SYSSTART	
At this point, the HW configuration settings are reset to the OEM restoration point.		

5.3 Error Handling

If AT+SQNSFACTORYRESET returns ERROR, the most likely reason is that there is no OEM restoration point.

Command	Response	Comment
AT+SQNSFACTORYRESET	ERROR	
AT+CFUN=5	OK	
AT+SQNHWCFGSAVE="OEM"	OK	Create a restoration point
AT^RESET	OK	
	+SHUTDOWN +SYSSTART	
AT+SQNSFACTORYRESET	OK	

6. Data over UART

Data socket can be opened to exchange data on various protocols (UDP, TCP, HTTP, TFTP, FTP, MQTT and COAP). A TLS is available to secure data sockets if needed.

A maximum of six sessions can be opened in parallel, with one session per socket. A socket is created by the RYZ014 module and not by the host MCU. UDP and TCP sockets can be opened with either in command or online modes:

In command mode, the UART transmits AT commands and responses. In that mode, the user can send data using either with:

- AT+SQNSSEND: the user enters the data to be sent after the prompt and committed with <CTRL+Z> or cancelled with <ESC>.
- AT+SQNSSENDEXT: in that case, the host MCU defines the size of the payload to be sent and the modem automatically sends the data once the given number of bytes is reached.

In online mode, all data is transferred verbatim. No AT command interpretation takes place. The host MCU must use the escape sequence +++ to switch back to command mode. The socket remains open. The +++ sequence must respect the timings given below. Different timings lead to the sequence being sent as raw data.

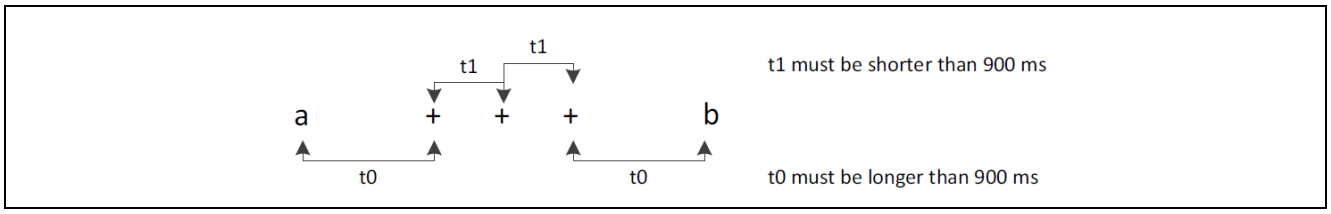


Figure 1. Escape Sequence Timing

AT+SQNSO <connId> command resumes the online mode for connection <connId>, provided the socket timer has not expired. Sockets support both text data and HEX data formats. TCP/UDP listening port is supported in specific way that is different from a typical server. Once the module accepts an incoming socket connection, it stops listening to the port and assigns the session to the connection. Socket configuration is stored into non-volatile memory and is restored automatically after each low power cycle in Deep Sleep mode.

Important Note: Sockets can be closed without warning when server keepalive timers expire. Therefore, it is recommended to check the socket status with AT+SQNSS command before sending data.

Certificates and private keys used by the TLS stack for secure socket connection can be stored in the non-volatile memory using appropriate AT commands.

Specific AT commands are implemented for HTTP, HTTPS, FTP and TFTP transfers. Two modes are supported with these commands. In asynchronous mode, the command is executed in background by the system. For instance, a file transfer is initiated, but the user can initiate another action. Progress and results are displayed with URCs. In synchronous mode, the command is executed and the UART is locked until the command completes. For instance, a file transfer is initiated, and the user must wait for its completion before initiating another action.

As the receive buffer size is only 2524 bytes long, it is mandatory to dump it regularly with AT+SQNSRECV, AT+SQNHTTPRCV, AT+SQNFGETDATA, AT+SQNSMQTTRCVMESSAGE or AT+SQNCOAPRCV commands, otherwise data risks being lost.

6.1 How to Send Data with UDP

6.1.1 Feature Description

The user can open a UDP socket and send data in either online mode or command mode.

After a UDP socket session is established, both local IP address/port and remote IP address/port are fixed. By default, only a message coming from the remote IP address/port to this specific local IP address/port will be accepted and a `+SQNSRING` URC will be generated for the host MCU. Any other packet will be dropped. It is possible to disable the filtering done by the modem and accept incoming response messages with different remote IP address/port (source IP address/port) with the `<acceptAnyRemote>` parameter in `AT+SQNSD` command.

Important Note: With UDP protocol, there is no URC to inform the host MCU that a UDP packet was transmitted by the modem.

The related AT commands are:

- `AT+SQNSD`
  Use parameter `<TxProt>` of `AT+SQNSD` to configure the transmission protocol (TCP or UDP).
- `AT+SQNSSEND`
- `AT+SQNSSENDEXT`
- `AT+SQNSRECV`
- `AT+SQNSH`
- URC `+SQNSRING`

Important: If `+SQNSRING` URC mode is set to 2 (data view mode), it is required to use `AT+SQNSRECV` to receive the data. Otherwise, the data buffer would remain full and the additional data are lost.

6.1.2 Use Cases in Online Mode

Command	Response	Comment
Ensure that UE is attached to LTE network. You can then configure the socket.		
`AT+SQNSCFG=1,1,0,0,600,50`	`OK`	Configure socket with default configuration.
`AT+SQNSCFGEXT=1,0,0,0`	`OK`	Configure extra socket parameters with default configuration:
`AT+SQNSD=1,1,4000,"192.168.13.1",0,4004,0`		Configure socket connection id 1 and open socket connect to `192.168.13.1`
	`CONNECT`	Connected to server
Got again		Type string, and press <enter> when complete.
		`OK`
`AT+SQNSS?`		Check socket configuration status

	`+SQNSS: 1,2,"192.168.13.3",49165,"192.168.13.1",8008`
	`+SQNSS: 2,0`
	`+SQNSS: 3,0`
	`+SQNSS: 4,0`
	`+SQNSS: 5,0`
	`+SQNSS: 6,0 OK`	

`AT+SQNSO=1`		Resumes socket connection, The CONNECT indication is given and the modem goes into online data mode again.
	`CONNECT` `OK`	
	`+SQNSRING: 1`	The SQNSRING URC indicates that there is an incoming connection on 1st socket.
`AT+SQNSRECV=1,100`		Receive up to 100 bytes from 1st socket.

Command	Response	Comment
	+SQNSRECV: 1,10 Got again OK	10 bytes are received. The content is displayed.
AT+SQNSH=1	OK	

6.1.3 Use Cases in Command Mode

Command	Response	Comment
Ensure that UE is attached to LTE network. You can then configure the socket.		
AT+SQNSCFG=1,1,0,0,600,50	OK	Configure socket with defaultconfiguration
AT+SQNSCFGEXT=1,0,0,0	OK	Configure extra socket parameters with default configuration
AT+SQNSD=1,1,4000,”192.168 .13.1”,0,4004,1	OK	Configure socket connection id1 and open socket connect to 192.168.13.1
AT+SQNSSEND=1		Send data in command mode through socket connection id 1.
> Hello extend from client	OK	Type <Ctrl+Z> to confirm and <ESC > to cancel.
AT+SQNSSENDEXT=1,24		Configure how many bytes are to be sent. **Note**: Maximum number of bytes to send is 1500.
> Hello extend from client	OK	
	+SQNSRING: 1	There is incoming connection on 1st socket.
AT+SQNSRECV=1,100		Receive up to 100 bytes from 1st socket.
	+SQNSRECV: 1,24 Hello extend from client OK	24 bytes are actually received.
AT+SQNSH=1	OK	Shutdown connection

6.1.4 Accept Any Remote Option

The following examples show how to receive packets coming from another IP address/port and how to send packets to another IP address/port.

6.1.4.1 Receive Data from a Different Server

Command	Response	Comment
Ensure that UE is attached to LTE network. You can then configure the socket.		
AT+SQNSCFG=1,1,300,0,0,50	OK	Basic socket configuration
AT+SQNSCFGEXT=1,2,0,0	OK	
AT+SQNSD=1,1,5000,"172.16.72.2",0,3000,1,1	OK	Enable receive data from any other remotethan <IPaddr>:<rPort>
Run below command from the server#1 (IP 172.16.72.2) and send data. nc -u 192.168.55.2 3000 11111		
	+SQNSRING: 1,6,11111	A URC is generated bythe modem when receiving the packet
AT+SQNSRECV=1,6	+SQNSRECV: 1,6,11111 OK	Read the buffered data

Command	Response	Comment
Send data from the server#2 (IP 172.16.72.8) and send data. nc -u 192.168.55.2 3000 222222		
	+SQNSRING: 1,6,22222	The packet was not dropped by the modem even though the IP address does not matchthe one configured with SQNSD
AT+SQNSRECV=1,6	+SQNSRECV: 1,6,22222 OK	Read the message to empty the buffer

6.1.4.2 Send Data to Different Server within the Same Socket

Command	Response	Comment
Ensure that UE is attached to LTE network. You can then configure the socket.		
AT+SQNSCFG=1,1,300,0,0,50	OK	Basic socket configuration
AT+SQNSCFGEXT=1,2,0,0	OK	
AT+SQNSD=1,1,5000,"172.16.72.2",0,3000,1,2	OK	Enables receive data from any other remote than <IPaddr>:<rPort> and enables send data toany other remote than <IPaddr>:<rPort> within the same socket family using +SQNSSEND command.
Run the following command on server#1 (IP 172.16.72.2) to listen to packets on port 5001 nc -lu 5001		
AT+SQNSSEND=1,"172.16.72.2",5001		Send data to the server#1 (172.16.72.2/5001)
	> hello1 <ctrl+z> OK	
Check that you get “hello1” on the server#1 (port 5001) even though the remote port configured for the socket is 5000		
Run below command on the server#2 to listen to packets on port 5002 : nc -lu 5002		
AT+SQNSSEND=1,"172.16.72.8",5002		
	> hello2 <ctrl+z> OK	
Check that you get “hello2” on the server#2 even though both the IP address and port are different from the ones configured for the socket		

6.1.5 Error Handling

When sending HEX data with AT+SQNSSEND or AT+SQNSSENDEXT, if you get ERROR (CME_ERROR4), please make sure first that the data to send is valid. If the data is confirmed valid, please check if you use the proper terminator for AT command. Only one character is allowed. The AT command syntax is described in the *3GPP 27.007* (§4.1 and §4.2) and *ITU V250* (§5.2.1).

The termination character is <CR> by default. For example, when using <CR><LF> (“\r\n”) as the terminator for AT commands which need input data, the second char <LF> (“\n”) remains in the buffer and is treated as input data for the next command. It will trigger an ERROR immediately as “\n” is an invalid HEX char.

When sending data in text mode, the module does not return ERROR, but the server receives data starting with "\n", and this may cause other problems. The terminator character can be changed with the ATS3 command. Please refer to *AT Commands Reference Manual* for details. When developing an application on the host MCU based on AT commands, if no specific requirements are set, please use <CR> ("\r") as the terminator character.

The format of +SQNSRING can be configured by AT+SQNSCFGEXT. When AT+SQNSCFGEXT parameter <srMode> is set to 2, the Unsolicited Response is +SQNSRING: <connId>,<recData>,<data>. The received data is output with the URC, but this does not flush the bytes from the buffer.

An ERROR is reported when the receive buffer fills up and all the additional data are lost. The received bytes are not flushed until explicitly read through AT+SQNSRECV command.

Internal buffering is limited and +SQNSRING notification is suspended until host starts reading data with the AT+SQNSRECV command. URC will be sent again if enough data has been read and if there are still new incoming data.

6.2 How to Send Data with TCP

6.2.1 Feature Description

The user can open TCP socket and send data either in online mode or command mode.

Note: If +SQNSRING URC mode is set to 2 (data view mode), it is required to use AT+SQNSRECV to retrieve the data. Otherwise, the data Rx buffer will eventually overflow, causing data loss.

Related AT commands are:

- AT+SQNSD
  Use parameter <TxProt> of AT+SQNSD to configure the transmission protocol (TCP or UDP).
- AT+SQNSSEND
- AT+SQNSSENDEXT
- AT+SQNSRECV
- AT+SQNSH
- URC +SQNSRING

A typical TCP setup is illustrated in Figure 2.

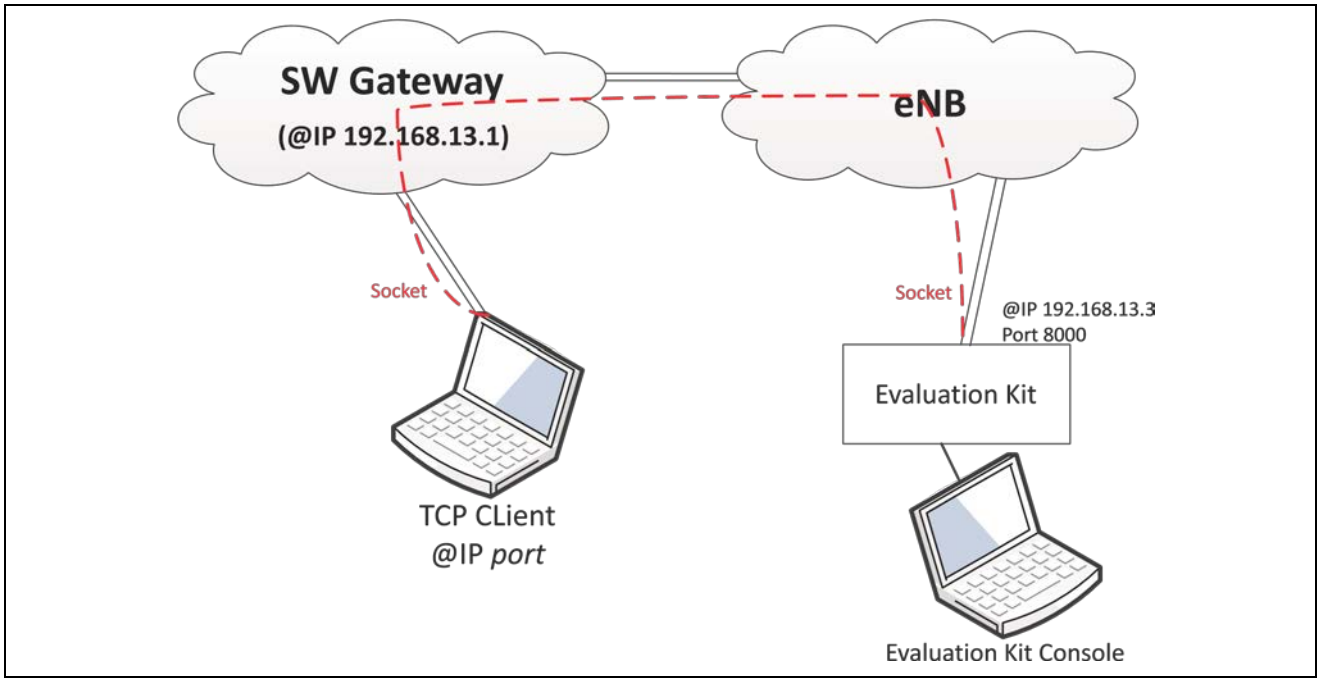


Figure 2. TCP Typical Setup

Note: The connection to the server is opened from another machine by running netcat (shorten as nc) program as follows:

"nc -l 8008". Data from the server are also typed manually.

6.2.2 Use Cases in Online Mode

Command	Response	Comment
Ensure that UE is attached to LTE network. You can then configure the socket.		
AT+SQNSCFG=1,1,0,0,600,50	OK	The second parameter is <cid> for PDP context identifier. Use Internet Cid for the test.
AT+SQNSCFGEXT=1,0,0,0	OK	Apply extended configuration: URC format, send/receive data mode, ...
AT+SQNSD=1,0,8008,"192.168.13.1",0,8000,0		Type socket dial command. Parameter <commode> is 0 for online mode. <TxProt>=0 for TCP.
	CONNECT	Intermediate result code ifthe socket is opened successfully.
	Hello this is from client	Type string, and press <enter> when complete.
You should see this string on server side. If remote host sends any data back to UE, this data shall be received over serial link.		
+++		Suspend online mode.
	OK	The UART is back to AT command mode. The socket is suspended.
AT+SQNSS		Check socket status.
	+SQNSS:1,2,"192.168.13.3",49165, "192.168.13.1",8008 +SQNSS:2,0 +SQNSS:3,0 +SQNSS:4,0 +SQNSS:5,0 +SQNSS:6,0	
AT+SQNSO=1		Restore the socket in online mode.
	CONNECT	Success indication
+++	OK	Suspend the socket.
	Got again	Send data again from the server.
	+SQNSRING: 1	URC to indicate data from remote host.
AT+SQNSRECV=1,1500		Receive data. The max bytes received once is 1500.
	+SQNSRECV: 1,10 Got again OK	10 bytes to receive, string received.
AT+SQNSH=1	OK	Shutdown the socket

6.2.3 Use Cases in Command Mode with Text Data

Command	Response	Comment
Ensure that UE is attached to LTE network. You can then configure the socket.		
AT+SQNSCFG=1,1,0,0,600,50	OK	The second parameter is <cid> for PDP context identifier. Use Internet Cid for the test.
AT+SQNSCFGEXT=1,0,0,0	OK	Configure extra socket parameters with default configuration
AT+SQNSD=1,0,8008,"192.168.13.1",0, 8000,1	OK	Type TCP socket dial command. Configure socket connection id 1 and open socket connect to 192.168.13.1

Command	Response	Comment
AT+SQNSSEND=1		
	> Hello extend from client	Send data in command mode through socket connection id 1,
Type <Ctrl+Z> to confirm and ESC to cancel.		
	OK	
AT+SQNSSENDEXT=1,24		Configure the number of bytes to be sent. The maximum is 1500.
	> Hello extend from client	
	+SQNSRING: 1	There is incoming connection on 1st socket.
AT+SQNSRECV=1,100		Receive up to 100 bytes from 1st socket.
	+SQNSRECV: 1,24	24 bytes are received.
	Hello extend from client OK	
AT+SQNSH=1	OK	Shutdown connection

6.2.4 Use Cases in Command Mode with Hex Data

In hex mode, data is represented as a sequence of hexadecimal numbers from 00 to FF. This is usually used to send a binary file. In this case, AT+SQNSSENDEXT usage is suggested since all data can be sent without any limitation. AT+SQNSSEND would process 0x1A(CTRL+Z) and 0x1B(ESC) as control chars.

Command	Response	Comment
Ensure that UE is attached to LTE network. You can then configure the socket.		
AT+SQNSCFG=1,1,0,0,600,50	OK	The second parameter is <cid> for PDP context identifier. Use Internet Cid forthe test.
AT+SQNSCFGEXT=1,0,0,0,0,1	OK	Set <sendDataMode> to HEX mode
This is to set URC format, send/receive data mode and so on.		
AT+SQNSD=1,0,8008,"192.168.13.1",0, 8000,1	OK	Type TCP socket dial command. The parameter <commMode> to indicate which mode to use, 1 is command mode. The UART is in command mode, it responds to AT commands.
AT+SQNSSENDEXT=1,10		Begin sending data.
	>	Wait for the prompt:
7D000015116000050010	OK	Send data in HEX mode.
The message should appear on the remote side.		
AT+SQNSH=1	OK	Shutdown the socket.

6.2.5 Error Handling

When sending HEX data with AT+SQNSSEND or AT+SQNSSENDEXT, if you get ERROR (CME_ERROR 4), please make sure first that the data to send is valid. If the data is confirmed valid, please check if you use the proper terminator for AT command. Only one character is allowed. The AT command syntax is described in the 3GPP 27.007 (§4.1 and §4.2) and ITU V250 (§5.2.1). The termination character is <CR> by default. For example, when using <CR><LF> (“\r\n”) as terminator, for AT commands which need input data, the second char <LF> ("\n") remains in the buffer and is treated as input data for the next command. It will trigger immediately as "\n" is an invalid HEX char. When sending data in text mode, the module will not return ERROR, but the server would receive data start with "\n”, and this may trigger other problems.

The terminator char can be changed by ATS3 command, please refer to *AT Commands Reference Manual* for more details. When developing an application on the host MCU based on AT commands, if no specific requirements are set, please use <CR> ("\r") as the terminator character.

The format of +SQNSRING can be configured by AT+SQNSCFGEXT. When AT+SQNSCFGEXT parameter <srMode> is set to 2, the Unsolicited Response is +SQNSRING: <connId>,<recData>,<data>. The received data is output with the URC, but this does not flush the bytes from the buffer. An ERROR is reported when the receive buffer fills up, and all additional data are lost. Received bytes are not flushed until explicit read through AT+SQNSRECV command.

Internal buffering is limited and +SQNSRING notification will stop until host starts reading data through AT+SQNSRECV command. URC will be sent again if enough data has been read and if there are still new incoming data.

6.3 How to Setup a Secure Socket Connection

6.3.1 Feature Description

It is possible to combine the use of SSL/TLS with a TCP or SSL/DTLS with a UDP socket for a secure connection. Two additional commands are needed:

- AT+SQNSCFG: To configure a specific security profile
- AT+SQNSSCFG: To enable a security profile to be used over TCP or UDP sockets.

6.3.2 Use Cases

Following is an example of a secure TCP connection to an AWS server using TLS 1.1.

Command	Response	Comment
Set the two required certificates and the private key. These certificates and private key are specific to the server you plan to use.		
AT+SQNSNVW="certificate",19,1342	>	
-----BEGIN CERTIFICATE----- MIIDszCCApugAwIBAgIUOt+d+ka42+WlzA6Yy85B6S1180kwDQYJKoZIhvcNAQELBQAw (…) V5fFnl/Q2AXyhmGlyTXNrnYZV9r3Q3blUSIivk3J5f/LRYYTMf/ oaIXQjWRId7QlQl9TIqrLBJ/oyieBdRNYg/-----END CERTIFICATE-----		
	OK	
AT+SQNSNVW="certificate",18,1188	>	
-----BEGIN CERTIFICATE----- MIIDQDCCAigCFEnODZGecw9dKrakkAR5E1FUdklqMA0GCSqGSIb3DQEBCwUAMGkx (…) 3ybHoJ3FPNVjxb3qw/022yy/cbhkk149fSG/+fNXpRqBkzYJVgIPENgBGrWD3GcxsA6q/ VuZZMfsRnreeJmCjOO suKc=-----END CERTIFICATE-----		
	OK	
AT+SQNSNVW="privatekey",4,167 5	>	
-----BEGIN RSA PRIVATE KEY----- MIIEowIBAAKCAQEA5Y9oi8GwKg3FOx8ZnqLtWaUN3IAKRVgWO7/ bmzkNN6HYJTxvp3v+4jGPkkLKiA+b (…) mT4lEcd4I5X00w82tdpIxobIH9UUBJlrZ2YLQ+nBAEy0zLYY532ZQwJXAI0rzejOanzMvwd+p XzwwPt ----- END RSA PRIVATE KEY-----		
	OK	
Configure SSL/TLS security profile 1, TLS 1.1, cipher suites TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA and TLS_RSA_WITH_AES_256_CBC_SHA256 (certificate validation level: 0 (no validated), certificate id: 3, 4 and 4):		
AT+SQNSPCFG=1,1,"0x2F;0x3C;0x 35;0x3D",0,19,18,4	OK	
Configure the socket. The internet cid is set to 3, as needed on Verizon networks. For most of the other network operators, the internet cid is 1.		

Command	Response	Comment
AT+SQNSCFG=1,3,300,90,600,50	OK	
AT+SQNSSCFG=1,1,1	OK	Enable security profile 1 (set above) on socket connection id 1
AT+SQNSD=1,0,32806,"ec2-3-134-42-3.useast-2.compute.amazonaws.co m",0,0,1		
	OK	
AT+SQNSSEND=1		
	> Hello with TLS	
	OK	
	+SQNSRING: 1	
AT+SQNSRECV=1,100	+SQNSRECV: 1,15 Hello with TLS OK	

6.4 How to Send Data on HTTP(S) Connection

6.4.1 Feature Description

The module can send data on HTTP connection either in asynchronous mode or synchronous mode. HTTP connection can be managed with the following specific +SQNHTTP AT commands:

- AT+SQNHTTPCFG
- AT+SQNHTTPQRY (as GET, HEAD, DELETE)
- AT+SQNHTTPRCV (as RECEIVE)
- AT+SQNHTTPSND (as POST, PUT)
- AT+SQNHTTPCONNECT and AT+SQNHTTPDISCONNECT were introduced to support asynchronous connection establishment

GET, POST and PUT can also be managed with the following AT commands:

- AT+SQNFGET (as GET)
- AT+SQNFPUT (as POST, PUT)

Note: That HW flow control must be used to send and receive large packets with SQNHTTPSND and SQNHTTPRCV commands.

The user can set up a HTTPS connection with or without certificate validation. When you access a website using HTTPS, a certificate chain should be provided. The RYZ014 module does not store it in flash memory by default. Therefore, the user needs to retrieve and load the correct certificate to use the HTTPS feature.

In synchronous mode, it can be useful to define timeouts, to avoid the modem hanging and drawing power endlessly if there is a connection issue.

<cnx_to_sec> (num) [1-120]: Connection timeout in seconds.

This timeout covers the DNS lookup plus TCP connection to the server.

<max_to_sec> (num)[0-65535]: Maximum data transfer timeout in seconds.

This timeout includes the whole connection: DNS lookup, TCP establishment, TLS handshake and HTTP data transfer.

The timeout value shall be greater than <cnx_to_sec> value. In case this rule is not respected, the AT command returns ERROR immediately.

6.4.2 Use Cases in Synchronous Mode with +SQNHTTP Commands

6.4.2.1 Send a GET Request

Command	Response	Comment
Type this command to configure the HTTP connection without SSL enabled.		
AT+SQNHTTPCFG=1,"httpbin.org",80,0,"","",0,120,1		
	OK	
AT+SQNHTTPCFG?		Read command of HTTP configuration
	+SQNHTTPCFG: 0,"",80,0,"","",0,120,3 +SQNHTTPCFG: 1,"httpbin.org",80,0,"","",0,120,1 +SQNHTTPCFG: 2,"",80,0,"","",0,120,3	
AT+SQNHTTPQRY=1,0,"/"	OK	QRY command to query a test file. See below the note on <extra-header-line> parameter.
If succeed before timeout, you would get an URC. This means the file is found and length is 13011.		
	+SQNHTTPRING: 0,200,"text/html; charset=utf-8",13011	
AT+SQNHTTPRCV=1,0		RCV command to get it:
Then would get the file shown on the screen. This is ended by an "OK" in the last line.		
	(...) OK	Note that SQNHTTPRCV returns error when there is no body (only a header) in the data received.

6.4.2.2 Send POST Request with AT+SQNHTTPSND

This test is to be run after the GET request sequence.

Command	Response	Comment
AT+SQNHTTPSND=1,0,"/post",7		Type the command. See below the notes on <post-param> and <extra-header-line> parameters.
	>	Get a prompt
Enter the string with the additional parameter and press CTRL+Z		
foo=bar		
	OK	In case of success ,you will get the URC
	+SQNHTTPRING: 1,200,"application/json",258	
AT+SQNHTTPRCV=1,0		Read the data received:
You would get the data, followed by an "OK" in a separated line.		
	(...) OK	Note that SQNHTTPRCV returns error when there is no body (only a header) in the data received.

6.4.2.3 Note on <post_param> and <extra-header-line> Parameter

In AT+SQNHTTPSND, the parameter <post_param> is optional. It is to be used only for POST request type and is related to <Content-Type> in the HTTP header. In the example above, "0" default value is used. HTTP packets include, in the header:

```
Content-Type: application/x-www-form-urlencoded
```

You might want to define charset for text/plain, or boundary for multipart/form-data. In these cases, you need an extension as detailed below:

- Set charset to us-ascii:
  Set <post_param> to "1:charset=us-ascii", then the request will contain "Content-type: text/plain; charset=us-ascii" header line.
  AT+SQNHTTPSND=1,0,"/post",7,"1:charset=us-ascii"
- Set boundary "—-WebKitFormBoundaryv9K2Q6NJOnI5kAZX"

Set <post_param> to “3:boundary=—-WebKitFormBoundaryv9K2Q6NJOnI5kAZX”, then the request will contain “Content-Type: multipart/form-data; boundary=—-WebKitFormBoundaryv9K2Q6NJOnI5kAZX” header line.

```
AT+SQNHTTPSND=0,0,"/upload.php",336,"3:boundary=----WebKitFo
rmBoundaryv9K2Q6NJOnI5kAZX"
```

In the example above, data length is 336. And after you get a ">" prompt, enter 336 bytes as content with boundary string as a separator.

Both AT+SQNHTTPSND and AT+SQNHTTPQRY commands support the optional parameter <extra_header_line>.

It allows inclusion of an additional HTTP header line. '@' character is used to identify the header line ending. If you want to type ‘@’ char in header, just echo it with another ‘@’ char.

For instance, “gizmopal-device-access-token: UNDEFINED@@ FORMAT@@@battery-level: 100@” is parsed to two header lines:

- “gizmopal-device-access-token: UNDEFINED@ FORMAT@”
- “battery-level: 100”

```
AT+SQNHTTPQRY=1,0,"/","gizmopal-device-access-token: UNDEFINED@@
FORMAT@@@battery-level: 100@"
```

6.4.3 Use Case with +SQNFGET Command

Command	Response	Comment
AT+SQNFGET="http:/192.168.13.1/index.html"		By default, it is synchronous downloading. In case the <local_filename> parameter is not specified; this AT command switches AT channel to data mode and outputs downloadedbinary octet stream to the host.In this scenario, host is responsible for error handling.
	<!doctype html> <html> <head> <title>Example Domain</title> [... output omitted partly ...] </head> <body> Example Domain This domain is established to be used for illustrative examples in documents. You may use this domain in examples without prior coordination or asking for permission. More information... </body> </html>	
	OK	After all data is received, the AT returns OK

6.4.4 Use Case with +SQNFPUT Command

The AT+SQNFPUT command performs a HTTP POST or PUT request with file content to server. When an answer from HTTP server is received, you will see +SQNHTTPRING URC with information.

The fifth parameter <post_param> is different from the one in +SQNHTTPSND command. It can take two different values:

- json-log-txt
- json-log-zip

It will convert the uploading content to json {"format": "zip|txt", "logs": "BASE_64_FILE"}. If one of the two above types is specified, the command will ignore the fourth parameter <filename>. and sends event logs to the server instead. The use of this parameter is limited to specific debug cases. In general, please specify the <filename> value and avoid using <post_param>.

Please refer to the *AT Commands Reference Manual* for further information.

Command	Response	Comment
AT+SQNHTTPCFG=0,"192.168.13.1",80,,,,0,60,1		Config server address, cid and ssl and so on
AT+SQNFPUT=0,0,"/process/uploading","mylocalfile","2"		Upload the file to /process/uploading. This AT command can only be used to upload files located from the device's filesystem to the server. Use HTTP commands set to upload files from the host MCU's filesystem.
	+SQNHTTPRING: 0,200,"application/json",77 OK	response ok with 200

6.4.5 Error Handling

AT+SQNHTTPSND is a synchronous command. The modem will not accept any other AT commands and send any URC while the command is being executed. This command depends on the network conditions. Under bad RF condition, the command will take some time to execute. The user can define a timeout for this AT command with SQNHTTPCFG: AT+SQNHTTPCFG=0,"192.168.10.3",443,,,,1,60,3,2. In this example, the timeout is set to 60 seconds.

When sending HEX data with AT+SQNHTTPSND, if you get ERROR (CME_ERROR 4), please make sure first that the data to send is valid. If the data is confirmed valid, please check if you use the proper terminator for AT command. Only one character is allowed. The AT command syntax is described in the *3GPP 27.007* (§4.1 and §4.2) and *ITU V250* (§5.2.1). The termination character is <CR> by default.

For example, when using <CR><LF> (“\r\n”) for AT commands which need input data, the second char <LF> ("\n") remains in the buffer and is treated as input data for the next command. It will trigger ERROR immediately as “\n” is an invalid HEX char.

When sending data in text mode, the module does not return ERROR but the server receives data that starts with “\n” and this may cause other problems. The terminator char can be changed by ATS3 command, please refer to *AT Commands Reference* Manual for more details. When developing an application on the host MCU based on AT commands, if no specific requirements are set, please use <CR> ("\r") as the terminator character.

The timeout values should be correctly set. <cnx_to_sec> must be smaller than <max_to_sec> value, otherwise the command returns ERROR.

6.5 How to Use TFTP AT Commands

6.5.1 Feature Description

The user can send data on TFTP connection in two different modes, asynchronous mode and synchronous mode. The AT commands for TFTP support are:

- AT+SQNFGET: File download command
- AT+SQNFGETDATA: Read asynchronously received data (asynchronous)
- +SQNFGETREPORT: Download status URC (asynchronous)
- +SQNFGETRING: Download size URC (asynchronous)

6.5.2 Use Case

The example below shows how to download a file to the Host (MCU/PC/…) in asynchronous mode.

Command	Response	Comment
AT+SQNFG”T="tftp://192.168.13.1/test.”xt",0		Start downloading by TFTP
	OK	
	+SQNFGETREPOR“: "started" +SQNFGETRING: 114 +SQNFGETREPORT: "downloading"	Receive “download status” URC and “download size” URC:
AT+SQNFGETDATA		Read received data
You would see the content displayed then, followed by a result status.		
	[Data] OK	
If all data are received, you will get the download status URC to indicate that the download is complete.		
	+SQNFGETREPORT: "complete"	

6.6 How to Use FTP(S) AT Commands

6.6.1 Feature Description

The user can send data on FTP connection in two different modes, asynchronous mode and synchronous mode.

The AT commands for TFTP support are:

- AT+SQNFGET: File download command
- AT+SQNFGETDATA: Read asynchronously received data (asynchronous)
- +SQNFGETREPORT: Download status URC (asynchronous)
- +SQNFGETRING: Download size URC (asynchronous)

Note: In asynchronous mode, the <local_filename> parameter of AT+SQNFGET command is used for local save of the file to the file system, in /fs/local_filename. If <local_filename> parameter is not provided, then the received data is stored in an internal FIFO, and you need to use AT+SQNFGETDATA command to read it.

6.6.2 Use Cases

6.6.2.1 Synchronous Mode

Command	Response	Comment
Download the test file from the remote FTP server 192.168.10.1 and save the file as mylocalfile on the device’s file system.		
AT+SQNFGET="ftp://192.168.10.1/testfile",1,"mylocalfile"		
	OK	
The possible status values are: started, downloading, error, complete, not running		
AT+SQNFGET?	+SQNFGET: "complete" OK	Read the status.

6.6.2.2 Asynchronous Mode

Command	Response	Comment
Download the test file from the remote ftp server 192.168.10.1 and save the file as `mylocalfile` on the device's file system.		
`AT+SQNFGET="ftp://192.168.10.1/testfile",0,"mylocalfile"`		
	`OK`	

	`+SQNFGETREPORT: "started"`
	`+SQNFGETRING: 200`
	`+SQNFGETREPORT: "downloading"`
	`+SQNFGETREPORT: "complete"`	

`AT+SQNFGET="ftp://192.168.10.1/testfile",0`		If <local_filename> is omitted, the received data is accumulated in internal buffer
	`OK`	
	`+SQNFGETREPORT: "started" +SQNFGETRING: 200 +SQNFGETREPORT: "downloading"` `+SQNFGETREPORT: "complete"`	Data can only be read with `AT+SQNFGETDATA` once `+SQNFGETRING` is received, sending `AT+SQNFGETDATA` before getting the latter URC will end up in `ERROR`
`AT+SQNFGETDATA`		Read internal buffer, the default parameter is 0 which means infinite reading
	`[Data]` `OK`	

6.7 How to Use MQTT(S) Commands

6.7.1 Feature Description

6.7.1.1 AT Commands

Renesas provides the following set of dedicated AT commands to implement MQTT protocol:

- Configure MQTT client: `+SQNSMQTTCFG`
- Initiate a MQTT client connection to a broker: `+SQNSMQTTCONNECT`
- Subscribe client to MQTT topic on a broker: `+SQNSMQTTSUBSCRIBE`
- Publish payload text message into MQTT topic: `+SQNSMQTTPUBLISH`
- Disconnect MQTT client by id: `+SQNSMQTTDISCONNECT`
- Receive MQTT message: `+SQNSMQTTRCVMESSAGE`

Important: There is no AT command to unsubscribe from a topic.

6.7.1.2 MQTT and TLS

MQTT relies on TCP as transport protocol, which means that by default the connection does not use an encrypted communication. To encrypt the whole MQTT communication, most MQTT brokers allow to use TLS in addition to the standard username/password authentication.

While it is enough for the server to use a private/public key pair to establish a secure connection, some clients can handle a unique public/private key pair which can be used in the TLS handshake. The client sends its certificate (which includes the public key of the client) as part of the TLS handshake after the server certificate is validated. The server is then able to verify the identity of the client and can abort the handshake if the verification of the client certificate fails. This allows authenticating the client before a secure connection is established.

Most of the IoT platforms such as AWS IoT, Google IoT Core, Azure, and Orange Live Objects are using this approach.

The AT command AT+SQNSNVW should be used to upload the certificates on the device. The AT command AT+SQNSPCFG sets the security profile parameters required to configure the following SSL/TLS connections properties.

6.7.2 MQTT Server

AWS IoT platform, Cloud IoT Core, Azure, or any other MQTT server can be used tests and usage. Another test server is Mosquitto https://test.mosquitto.org/.

6.7.2.1 Mosquitto

Mosquitto is a MQTT open-source test server: https://test.mosquitto.org/. This server can run on a local setup. To test MQTTS connection, use `openssl` to generate certificate and keys.

6.7.2.2 AWS IoT

AWS IoT provides secure, bi-directional communication between Internet-connected devices such as sensors, actuators, embedded micro-controllers, or smart appliances and the AWS Cloud. This enables to collect telemetry data from multiple devices, store and analyze the data.

To use AWS IoT you need to get an AWS account (note that Amazon offers the possibility to open free accounts: https://aws.amazon.com/free/?all-free-tier.sort-by=item.additionalFields.Sort Rank&all- free-tier.sort-order=asc). You first need to register under https://aws.amazon.com/iot/. For detail information about AWS IoT, please refer to http://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html.

Then, you need to create an AWS IoT Thing for your device as follows. When you login to your AWS IoT console, register your device in the AWS IoT registry. AWS IoT provides the detailed developer guides on how to register a device, create, and activate certificates here:

https://docs.aws.amazon.com/en_us/iot/latest/developerguide/register-device .html

Once the certificates are created, you will get the device's public and private keys, the device certificate, and the root certificate authority (CA).

Please download:

- The device certificate (created once a certificate has been added for your thing)
- The private key (created once a certificate has been added for your thing)
- The root CA file

Depending on which type of data endpoint you are using and which cipher suite you have negotiated, AWS IoT Core server authentication certificates are signed by different root CA certificates, Please refer to: https://docs.aws.amazon.com/iot/latest/developerguide/server-authentication.html#server-authentication-certs. If no specific needs, you can choose the RSA 2048 bit key: Amazon Root CA 1.

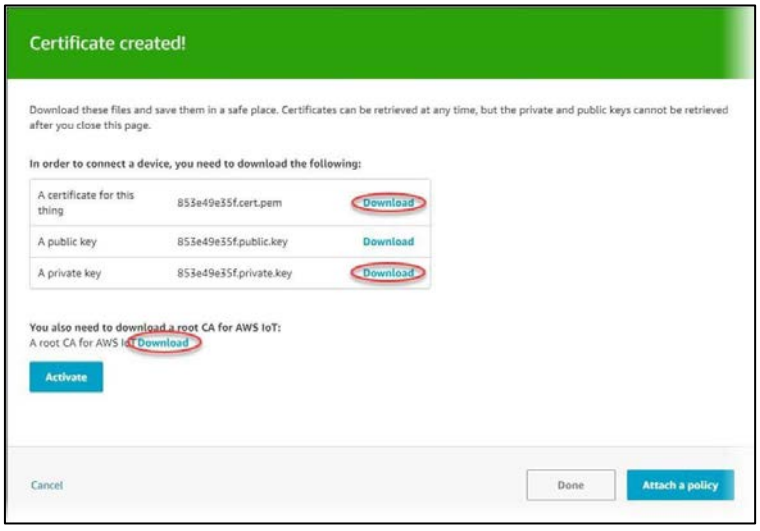


Figure 3. AWS Certificate Creation

You need then to upload the two certificates and the private key on your device using the AT+SQNSNVW commands. Then, set a security profile (with AT+SQNSPCFG) using the two certificates and the private key you just uploaded. Please refer to section 5.8.3.3 for more details on +SQNSNVW and +SQNSPCFG usage.

Please refer to Section 6.7.3.3 to connect to AWS IoT server, subscribe and publish to a topic. Pay attention to the following:

- The <client id> parameter to be set in the AT+SQNSMQTTCFG command is the Thing name that you chose when you created it (for example *myIotThing*)
- The domain name to be used in the +SQNSMQTTCONNECT command is called endpoint on AWS.
- The URL to be used should come from "AWS IoT -> manage -> Things -> "Select the thing you created" -> Interact". Then select the URL under "Update your Thing Shadow using this Rest API Endpoint".
- The format of the end point parameter is "*identifier*.iot.*region*.amazonaws.com".

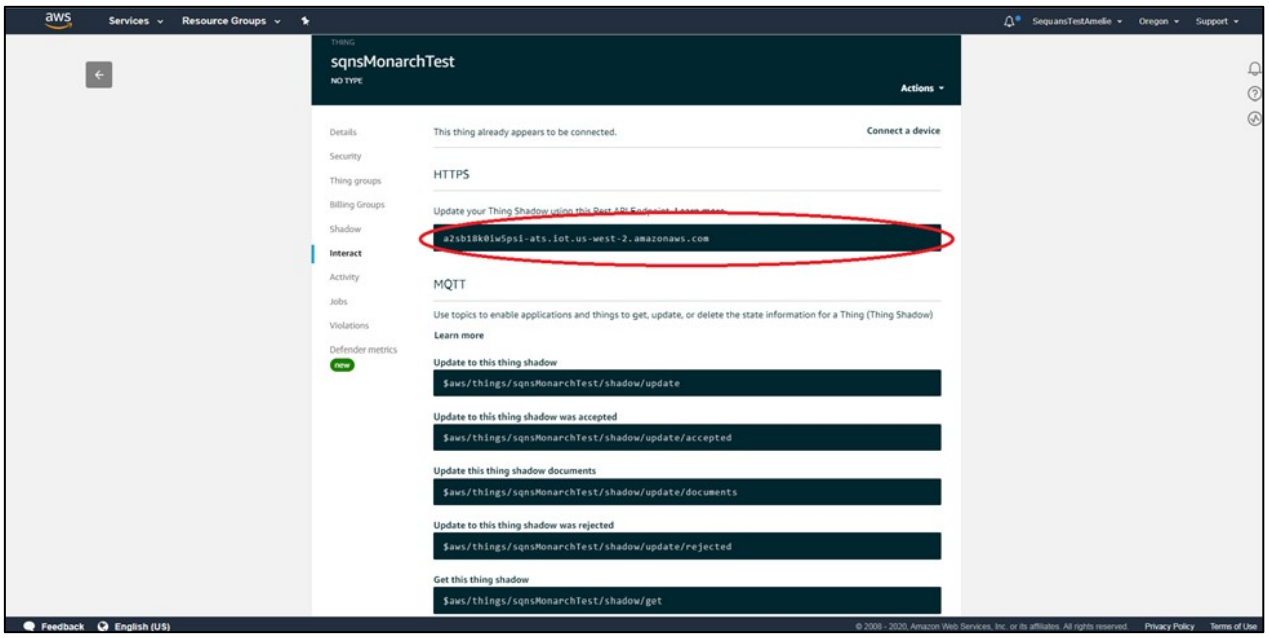


Figure 4. AWS End Point Parameters

More details on how to retrieve the end point can be found here: https://docs.aws.amazon.com/iot/latest/developerguide/device-shadow-rest-api.html.

- The topic to be used to publish with AT+SQNSMQTTPUBLISH is the one you want (for example *myTopic*)

6.7.2.3 Cloud IoT Core

Cloud IoT Core is a fully managed service that allows you to connect, manage, and ingest data from millions of globally dispersed devices easily and securely. You can get an overview of this cloud in https://services.google.com/fh/files/misc/iot_device_partner_integration_guid e1.0.pdf or follow the quick start guide https://cloud.google.com/iot/docs/quickstart.

First, register to google cloud as described in https://cloud.google.com/iot/docs/how-tos/getting-started.

Follow carefully the steps described in https://cloud.google.com/iot/docs/how-tos/credentials/keys to generate the public/private key pair (with a Linux OS) that will be used to authenticate your device on the cloud. On Windows™, you can use PUTTYgen to do that. The private key (rsa_private.pem) is required to generate a JWT (Jason Web Token) as explained below. The public key (rsa_public.pem) should be used when creating the device on the cloud as explained in https://cloud.google.com/iot/docs/how-tos/devices.

You will get the root CA certificate to upload to the device in https://cloud.google.com/iot/docs/how-tos/mqtt-bridge#downloading_mqtt_server_certificates. For a quick start, you should choose the complete Google root CA certification package (https://pki.goog/roots.pem) and upload it in the module with AT+SQNSNVW command.

Then, set a security profile (with AT+SQNSPCFG) using the certificate and the private key you just uploaded.

Please refer to Section 6.7.3.3 to connect to Cloud IoT core server, subscribe and publish to a topic. Pay attention to the following:

- The client id parameter to be set in the AT+SQNSMQTTCFG command is formatted in this way: `projects/project_id/locations/region/registries/registry_id/devices/device_id`
  - Where the `project_id` is the name that you chose for your project (*MyFirstProject* for example)
  - The `region` is the region that you selected when you created your registry (*europe-west1* for example)
- The `registry_id` is the name you chose when creating the registry (*myRegistry* for example)
- The `device_id` is the name you chose when creating your device (*myDevice* for example)

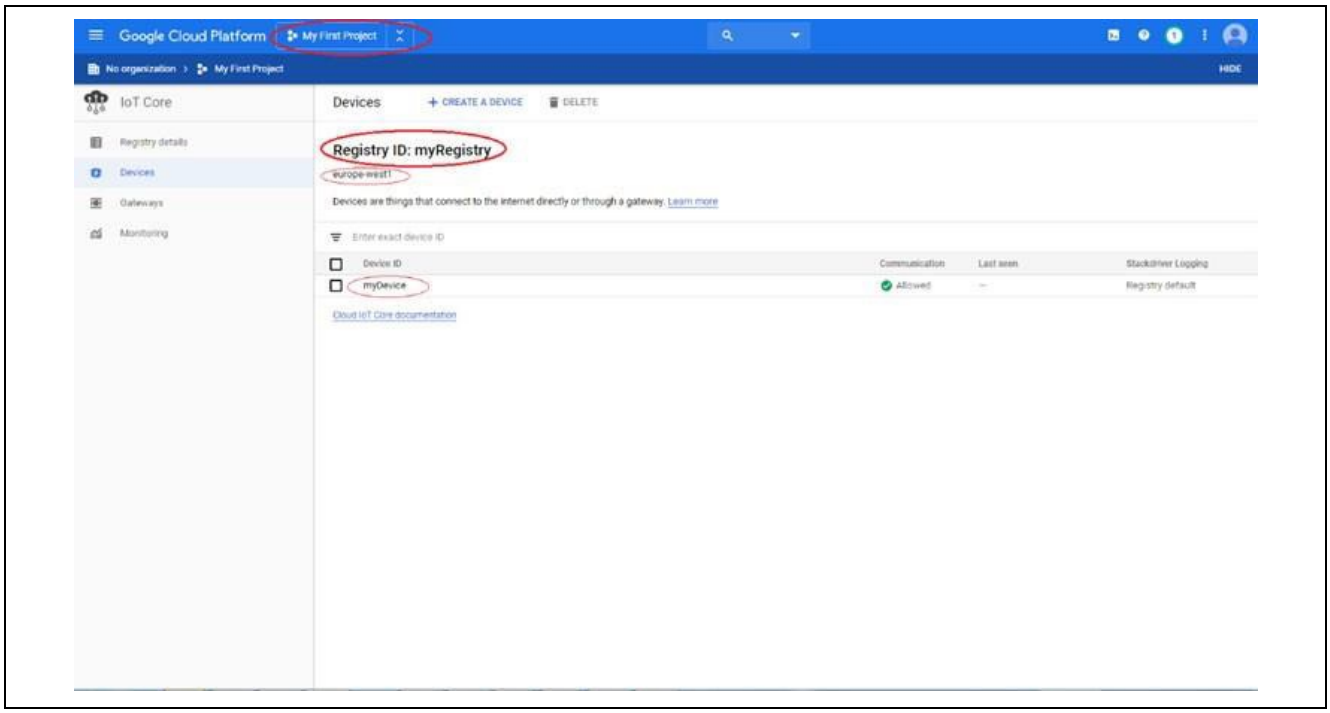


Figure 5. Cloud IoT Core Client Id Parameters

You will need also to set a password using a JWT (Jason Web Token). Please refer to https://cloud.google.com/iot/docs/how-tos/credentials/jwts to generate the JWT signature that will be set in the pwd parameter of +SQNMQTTCFG (4th parameter)

The host/domain name to be used in the AT+SQNSMQTTCONNECT command is mqtt.googleapis.com.

6.7.3 Use Cases

6.7.3.1 Non-Encrypted

Command	Response	Comment
Configure client id and client id string. Note that the client id must be 0.		
`AT+SQNSMQTTCFG=0,"sqn/gm01q"`	`OK`	
Initiate client id 0 new connection to test Mosquitto broker with non-encrypted port 1883.		
`AT+SQNSMQTTCONNECT=0,"192.168.13.1",1883`	`OK`	In real usage, <host> is a domain name. In this test with local setup, we use IP address. <port> 1883 is for test with MQTT unencrypted.
	`+SQNSMQTTONCONNECT: 0,0`	Notification that the connection operation is finished.
Subscribe to a topic “sqn/test” on test Mosquitto broker previously connected.		

Command	Response	Comment
AT+SQNSMQTTSUBSCRIBE=0,"sqn/ test",1	OK	
	+SQNSMQTTONSUBSCRIBE:0,"sqn/test",0	Notification that subscribing operation is finished.
Publish a payload into a topic on a test Mosquitto broker. The command responses the prompt '>' and waits for the data to send. The data is provided as length-defined multi-line data. Use <ESC> to cancel publishing.		
AT+SQNSMQTTPUBLISH=0,"sqn/tes t",1, 32	>	32 is the length of the payload to be entered after the '>' prompt.
>{"msg": "hello from IoT device"}		The AT ends automatically once 32 bytes of data are entered.
	+SQNSMQTTPUBLISH:2 OK	
	+SQNSMQTTPUBLISH:0,2,0	Notification that publishing operation is finished for client 0.
Receive a message by client id 0 or last received message in case of <qos>=0 when receive +SQNSMQTTONMESSAGE URC.		
	+SQNSMQTTONMESSAGE:0,"sqn/test",32,1,1	Notification about a newly received message which was stored to the internal message cache for client 0
AT+SQNSMQTTRCVMESSAGE=0," sqn/test ",1	{"msg": "hello from IoT device"} OK	Collect the message
AT+SQNSMQTTDISCONNECT=0	OK	Disconnect from a test Mosquitto broker.
	+SQNSMQTTONDISCONNECT: 0,0	Notification about drop of MQTT connection for client 0.

6.7.3.2 Encrypted

Command	Response	Comment
Upload test Mosquitto broker certificate into file system, certificate index 0. Note: If there is a certificate with index 0 already, remove it by the same command but setting the length to 0: AT+SQNSNVW="certificate",0,0 OK		
AT+SQNSNVW="certificate",0,1326	>	
	>(copy the certificate here)	After the prompt '>', copy the certificate into UART tool. If the length matches the one you used in the command, the command ends automatically. If the last "\n" is not copied, you need to type an <Enter> to end it. This configuration allows UE to verify the server connection.

Command	Response	Comment
Configure the security profile: • If the remote server does not support one of the cipher suites configured in the <cipherSpecs> list, the handshake fails. • For security reason, it is recommended to reduce the list to the minimum to avoid “man in the middle” attack like. • The third parameter is cipher suites. Supported cipher suites (IANA number: RFC Name): — 0x2F: TLS_RSA_WITH_AES_128_CBC_SHA — 0x3C: TLS_RSA_WITH_AES_128_CBC_SHA256 — 0x35: TLS_RSA_WITH_AES_256_CBC_SHA — 0x3D: TLS_RSA_WITH_AES_256_CBC_SHA256 — 0x8C: TLS_PSK_WITH_AES_128_CBC_SHA — 0x8D: TLS_PSK_WITH_AES_256_CBC_SHA — 0xAE: TLS_PSK_WITH_AES_128_CBC_SHA256 — 0xAF: TLS_PSK_WITH_AES_256_CBC_SHA384		
AT+SQNSPCFG=1,2,"0x3D;0x2F;0x8C",1,0,,,""		
	+SQNSPCFG: 1,2,"0x3D;0x2F;0x8C",1,0,,,"","" OK	
Configure client id, client id string, and set the index of the security profile configured previously by AT+SQNSPCFG.		
AT+SQNSMQTTCFG=0,"sqn/gm01 q",,,1	OK	
Initiate client id 0 a new connection to test Mosquitto broker with encrypted port 8883.		
AT+SQNSMQTTCONNECT=0,"192.168.13.1",8883	OK	In real usage, <host> is a domain name. In this test with local setup, we use IP address. <port> 8883 is for test with MQTT encrypted.
	+SQNSMQTTONCONNECT:0,0	URC notifies that connection operation is finished.
Subscribe to a topic “sqn/test” on test Mosquitto broker previously connected with SQNSMQTTCONNECT command.		
AT+SQNSMQTTSUBSCRIBE=0,"sq n/test",1	OK	
	+SQNSMQTTONSUBSCRIBE:0,"sqn/test",0	URC notifies that subscribing operation is finished.
Publish a payload into a topic on a test Mosquitto broker. The command responses the prompt ‘>’ and waits for the data to send. The data is provided as length-defined multi-line data. Use <ESC> to cancel publishing.		
AT+SQNSMQTTPUBLISH=0,"sqn /test",1,32.....	>	32 is the length of the payload to be entered after the ‘>’ prompt.
	>{"msg": "hello from IoT device"}	
	+SQNSMQTTPUBLISH:2 OK	The AT ends automatically once 32 bytes of data are entered.
	+SQNSMQTTPUBLISH:0,2,0	URC notifies that publishing operation is finished for client 0.
Receive a message by client id 0 or last received message in case of <qos>=0 when receiving +SQNSMQTTONMESSAGE		
	+SQNSMQTTONMESSAGE:0,"sqn /test",32,1,1	URC notifies about a new received message which was stored to the internal message cache for client 0.

Command	Response	Comment
AT+SQNSMQTTRCVMESSAGE=0, "sqn/test",1	{"msg": "hello from IoT device"} OK	
Disconnect from a test Mosquitto broker.		
AT+SQNSMQTTDISCONNECT=0	OK	
	+SQNSMQTTONDISCONNECT:0, 0	URC notifies about drop of MQTT connection for client 0.

6.7.3.3 Encrypted and Client Certificate Required

MQTT servers can also require clients to provide a certificate to authenticate their connection. This requires a client certificate (including public key) and private key to be uploaded by AT+SQNSNVW. You can configure a secure profile with AT+SQNSPCFG, and then combine its index and MQTT connection using the MQTT configuration command. In the following example, we assume certificate indexes 0 and 1, private key index 0 are not defined.

Command	Response	Comment
Upload test Mosquitto broker certificate into file system, certificate index 0. Note: If there is a certificate with index 0 already, remove it as follows: AT+SQNSNVW="certificate",0,0		
AT+SQNSNVW="certificate",0,1 326	>	
	OK	After the prompt '>', copy the certificate into UART tool. If the length matches the one you used in the command, the command ends automatically. If the last "\n" is not copied, you need to type an <Enter> to end it. This configuration allows UE to verify the server connection.
AT+SQNSNVW="certificate",1,1 545	>	(Copy the certificate here)
	OK	
AT+SQNSNVW="privatekey",0,1675	>	(Copy client private key here)
	OK	
Configure the security profile: If the remote server does not support one of the cipher suites configured in the <cipherSpecs> list, the handshake fails. • If the remote server does not support one of the cipher suites configured in the <cipherSpecs> list, the handshake fails. • For security reason, it is recommended to reduce the list to the minimum to avoid "man in the middle" type attacks.		
Use AT+SQNSNVR="certificate" and AT+SQNSNVR="privatekey" to dump all the available certificates and private keys stored in the system. Note that there is no requirement for the certificate sequence; the module will send everything at the certificate/privatekey index mentioned in the secure profile to the server as is		
AT+SQNSPCFG=2,3,"0x3D;0x2F;0x8C",1,0,1,0," "		Configure secure profile to index 0 with TLS1.3. If the list of supported cipher suites does not include the one that you need to set to connect to the MQTT server, you should leave the 3rd parameter empty ("")
	+SQNSPCFG: 2,3,"0x3D;0x2F;0x8C",1,0,1,0,"","" OK	
Configure client id, client id string, and set the index of the security profile configured previously with AT+SQNSPCFG.		

Command	Response	Comment
AT+SQNSMQTTCFG=0,"sqn/g m01 q",,,2	OK	Please refer to sections 6.7.2.2 and 6.7.2.3 to get the client id to be used for AWS and IoT Core. Note that a password is needed to connect to Google IoT core, it should be set as 4th parameter.
Initiate client id 0 a new connection to test Mosquitto broker with encrypted port 8883.		
AT+SQNSMQTTCONNECT=0, "192.168.13.1",8883	OK	In real usage, <host> is a domain name. In this test with local setup, we use IP address. Please refer to section 6.7.2.2 and 6.7.2.3 to get the domain names to be used for AWS and IoT Core. <port> 8883 is for test with MQTT encrypted
	+SQNSMQTTONCONNECT:0,0	URC notifies that connection operation is finished.
Subscribe to a topic “sqn/test” on test Mosquitto broker previously connected with SQNSMQTTCONNECT command.		
AT+SQNSMQTTSUBSCRIBE=0,"sq n/test",1	OK	
	+SQNSMQTTONSUBSCRIBE:0,"sqn/test",0	URC notifies that subscribing operation is finished.
Publish a payload into a topic on a test Mosquitto broker. The command response with the prompt ‘>’ and waits for the data to send, the data is provided as length-defined multi-line data. Use <ESC> to cancel publishing.		
AT+SQNSMQTTPUBLISH=0,"sqn/test",1,32	>	32 is the length of the payload to be entered after the ‘>’ prompt.
>{"msg": "hello from IoT device"}	+SQNSMQTTPUBLISH:2 OK	The AT ends automatically once 32 bytes of data are entered.
	+SQNSMQTTPUBLISH:0,2,0	URC notifies that publishing operation is finished for client 0.
Receive a message by client id 0 or last received message in case of <qos>=0 when receiving +SQNSMQTTONMESSAGE URC		
	+SQNSMQTTONMESSAGE:0,"sqn/test",32,1,1	URC notifies about a new received message which was stored to the internal message cache for client 0.
AT+SQNSMQTTRCVMESSAGE=0, "sqn/test",1	{"msg": "hello from IoT device"} OK	
Disconnect from a test Mosquitto broker.		
AT+SQNSMQTTDISCONNECT=0	OK	
	+SQNSMQTTONDISCONNECT:0,0	URC notifies about drop of MQTT connection for client 0.

6.7.4 Error Handling

You should wait for +SQNSMQTTONCONNECT:0,0 URC after sending the AT+SQNSMQTTCONNECT command. It means that the connection was completed successfully. Trying to subscribe or publish to a topic before getting this URC returns an error.

If the +SQNSMQTTONCONNECT URC is received with an error code, please check again the certificates that you are using and the cloud settings.

7. SMS

The SMS service routes short messages between UEs via an SMS service center. The SMS service center serves as an interworking and relaying function between the UEs.

The RYZ014 module uses SMS over NAS, also called SMS over SG, with 3GPP format (3GPP2 format is not supported with SMS over NAS) to send or receive SMS. SMS over NAS complies with 3GPP specification 27.005. Two types of SMS are defined:

- Text mode: This is the most basic type of SMS. It is easy to use but has less options and features than PDU mode.
- PDU mode: This is an advanced type of SMS. It provides control of features like concatenated (multi-segment) SMS but it is more complex to create than a plain text mode. Usually its content is generated with a tool.

The `AT+CMGF` command selects which SMS format to use, with the PDU mode being the default choice. The `AT+CNMI` command turns on the notifications (URC) when new SMS arrive.

As a reminder, Figure 6 represents the SMS network architecture.

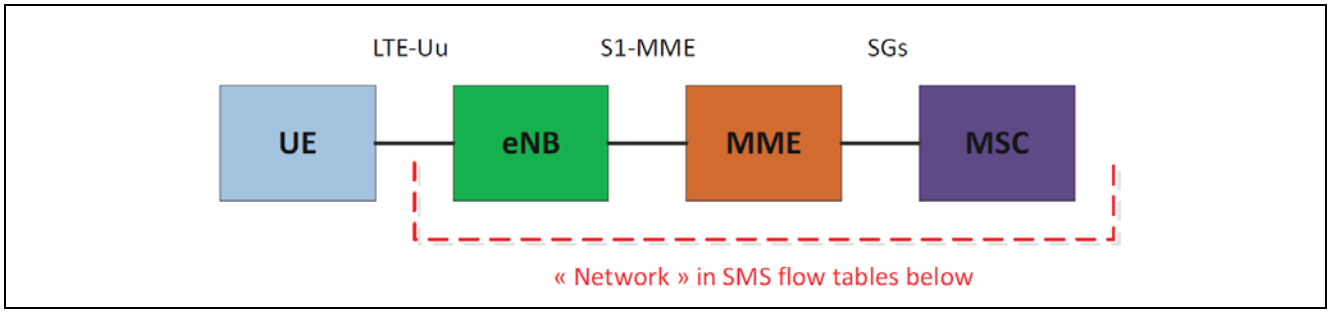


Figure 6. SMS Network Architecture

Table 1 shows the call flow for a mobile-originated SMS call, and Table 2 shows the call flow for a mobile-terminated SMS call.

Table 1. Mobile Originated SMS Flow

#	UE		Network
1	UL NAS Transport (CP-DATA / SMS-SUBMIT)	->	
2		<-	DL NAS Transport (CP-ACK)
3		<-	DL NAS Transport (CP-DATA / SMS-SUBMIT REPORT)
4	UL NAS Transport (CP-ACK)	->	

Table 2. Mobile Terminated SMS Flow

#	Network		UE
1	DL NAS Transport (CP-DATA / SMS-DELIVER)	->	
2		<-	UL NAS Transport (CP-ACK)
3 (optional if delivery report)		<-	UL NAS Transport (CP-DATA / RP-ACK)
4 (optional if delivery report)		->	DL NAS Transport (CP-ACK)

This section presents how to:

- Send and receive SMS in text mode.
- Send and receive SMS in PDU mode.
- Perform operations on memory storage (select storage area, read, delete).

7.1 How to Send and Receive SMS in Text Mode

7.1.1 Feature Description

This section details the operations required to send and receive a short message, in Latin or Asian characters.

Related AT commands are:

- AT+CMGF to set the SMS format
- AT+CSCA to configure the SMS service center
- AT+CMGS to send a SMS
- AT+CMGR to read a SMS

7.1.2 Use Cases

7.1.2.1 Read SMS

Command	Response	Comment
AT+CMGF=1	OK	Set Text mode
Read SMS at index 0		
AT+CMGR=0	+CMGL: 0,"STO UNSENT","+11484848484",,"00/00/00,00:00:00+00" How are you? OK	

7.1.2.2 Send SMS

Command	Response	Comment
EPS combined attach type is required before AT+CFUN=1.		
AT+CEMODE=2	OK	Configure UE for EPS combined attach
AT+CFUN=1	OK	
	+CEREG:2 +CEREG:1,”0002”,”01A2 2002”,7	
Configure UE to work under SMS text mode		
AT+CMGF=1	OK	
Query SMS service center address to confirm if it already well configured.		
AT+CSCA?	+CSCA: "+886932400851",145 OK	
Configure SMS service center address in case it's not well configured. Note: Contact your service provider to get SMS service center address accordingly.		
AT+CSCA=0932400851	OK	
Send SMS to subscriber phone number: "+886932123456".		
AT+CMGS="+886932123456"		Press <Enter> to get the prompt
	>This is my test message	This is prompt. Write the message here.
<CTRL-Z>		Complete the message with <CTRL-Z>
	OK	

7.1.2.3 Send an SMS in Korean Characters

The following preliminary steps are required before the test:

1. Configure your PC to allow Korean characters input
2. Configure Tera term™ terminal
3. Configure UE

Command	Response	Comment
EPS combined attach type is required before AT+CFUN=1.		

Command	Response	Comment
AT+CEMODE=2	OK	Configure UE for EPS combined attach
AT+CFUN=1	OK	
	+CEREG:2 +CEREG:1,"0002","01A2 2002",7	
Configure UTF-8 encoding		
AT+CSCS="UTF-8"	OK	
Configure SMS in text mode		
AT+CMGF=1	OK	
서울에서 따뜻합니다. 언제 우리를 방문하러 올 것입니까?		

7.2 How to Send and Receive a SMS in PDU Mode

7.2.1 Feature Description

PDU mode offers to send binary information in 7-bit or 8-bit format. That is helpful to send compressed data, binary data or to build a specific encoding of the characters in the binary bit stream. Web applications allow to send SMS in PDU mode, and others convert SMS between text and PDU modes.

The related AT commands are:

- AT+CMGF to set the SMS format
- AT+CSCA to configure the SMS service center
- AT+CMGS to send a SMS
- AT+CMGR to read a SMS

7.2.2 Use Cases

7.2.2.1 Send SMS

Command	Response	Comment
Read current SMS mode.		
AT+CMGF?	+CMGF:1 OK	Value 1 is text mode, value 0 is PDU mode.
Set PDU mode		
AT+CMGF=0	OK	
Check if SMS Service Center Address is set		
AT+CSCA?	+CSCA: "",129 OK	No SMS Service Center Address
Set SMS Service center Address		
AT+CSCA="+13123149810"	OK	
Send the SMS		
AT+CMGS=3707918405210077F70414D1ECB6FB0D8FCBE7F4BA1D0000901031809492401061361C1D76D7DB65797A0C9A36A <CTRL+Z>		
	+CMGS: 0 OK	No error

7.2.2.2 Receive SMS

Command	Response	Comment
AT+CMGR=0	+CMGR: 1,,23 04a11132f30405a11132f30000f0c020f0e2400007c8329bfd06c500 OK	

7.3 How to Manage SMS Storage

7.3.1 Feature Description

There are two storage areas for short messages on a RYZ014-based device:

- The SIM card
- The modem or device itself

Use AT+CPMS (Preferred Message Storage) command to:

- Select the message storage area that will be used when sending, receiving, reading, writing or deleting SMS messages.
- Find the number of messages that are currently stored in the message storage area.
- Find the maximum number of messages that can be stored in the message storage area.

AT+CMGL lists all the SMS in memory. AT+CMGD is used to delete a SMS.

7.3.2 Use Cases

7.3.2.1 Find the Number and the Maximum Number of Messages

Command	Response	Comment
AT+CPMS?	+CME ERROR: SIM not inserted	
AT+CFUN=1	OK	Start the modem to read the SIM card
AT+CPMS?	+CPMS: "ME",0,10,"ME",0,10,"ME",0,10	0 message stored in 10 allowed in "ME" memory

7.3.2.2 Select SIM as the Message Storage Area to be used for SMS Receiving and Reading

Command	Response	Comment
AT+CFUN=1	OK	Start the modem to read the SIM card
	+CEREG: 1,"0001","01A2D001",7	
AT+CNMI=2,1		Once UE is attached, enable SMS receiving notification
AT+CPMS?	+CPMS: "ME",0,10,"ME",0,10,"ME",0,10 OK	Check storage status
Send the message "aaaa" to number +11000000151 (yourself for the test)		
AT+CMGS="+11000000151" > aaaaa <CTRL-Z>		Press <Enter> to get the prompt after numbering, and <CTRL-Z> to proceed with the sending.
	+CMGS: 3 OK	
	+CMTI: "ME",1	One message received, stored in ME
Check storage status again.		
AT+CPMS?	+CPMS: "ME",1,10,"ME",1,10,"ME",1,10 OK	Contents of send storage area is increased, so do read area and receiving area

Command	Response	Comment
AT+CPMS="ME","ME","SM"	+CPMS: 1,10,1,10,0,20 OK	Configure storage area to SIM
AT+CMGS="+11000000151"	> bbbb <CTRL-Z>	Send two more messages to yourself again
	+CMGS: 4 OK	
	+CMTI: "SM",1	
AT+CPMS?	+CPMS: "ME",1,10,"ME",1,10,"SM",1,20 OK	
AT+CMGS="+11000000151"	> ccccc <CTRL-Z>	
	+CMGS: 5 OK	
	+CMTI: "SM",2	
AT+CPMS?	+CPMS: "ME",1,10,"ME",1,10,"SM",2,20 OK	
Read out all message, the 1st message saved in ME is read out		
AT+CMGL="ALL"	+CMGL: 1,"REC READ","11000000151",,"18/12/29,14:22:28+32" aaaaa OK	
Configure reading area to SIM. The next two messages saved in SIM are read out		
AT+CPMS="SM","ME","SM"	+CPMS: 2,20,1,10,2,20 OK	
Only working when AT+CMGF=1 (Read SMS in text mode)		
AT+CMGL="ALL"	+CMGL: 1,"REC UNREAD","11000000151",,"18/12/29,14:24:42+32" bbbb +CMGL: 2,"REC UNREAD","11000000151",,"18/12/29,14:25:29+32" cccc OK	

7.3.2.3 Delete the SMS in the Modem

Command	Response	Comment
AT+CPMS?	+CPMS: "ME",1,10,"ME",1,10,"ME",1,10 OK	
AT+CMGF=1	OK	
AT+CMGL="ALL"	+CMGL: 1,"REC READ","11000000151",,"18/12/29,14:22:28+32" aaaaa OK	
AT+CMGD=1	OK	
AT+CPMS?	+CPMS: "ME",0,10,"ME",0,10,"ME",0,10 OK	
AT+CPMS="SM","ME","ME"	+CPMS: 19,20,0,10,0,10	Delete the SMS in the SIM card
AT+CMGF=1	OK	
AT+CMGL="all"	+CMGL: 2,"REC READ","Amarisoft",,"17/10/19,05:39:38+08" hello..... +CMGL: 20,"REC READ","11000000102",,"18/03/30,03:14:45-16" sCommunicationsCommunicationsCommunications	

Command	Response	Comment
AT+CMGD=2	OK	Delete index 2
AT+CPMS?	+CPMS: "SM",18,20,"ME",0,10,"ME",0,10 OK	

7.3.3 Error Handling

Make sure that you are using a USIM which supports SMS. Some USIM are for data only and do not support SMS.

Pre-requisites to send a SMS are:

- The UE is attached to the eNB and Registered to EMM:

Command	Response	Comment
AT+CEREG?	+CEREG: 2,1,"CAE4","016F1704",7 OK	

- The SIM card is inserted and unlocked:

Command	Response	Comment
AT+CPIN?	+CPIN: READY OK	

- The SMS Center number is set : AT+CSCA? returns a phone number

Command	Response	Comment
AT+CFUN=1	OK	
	+CEREG: 2	
AT+CSCA?	+CSCA: "+33689004000",145 OK	

- Concatenated SMS are not always supported by the carrier network. The SMS application can also split the message into separate SMS instead of sending a multi-segment SMS.
- MT concatenated SMS sent as multiple segments will be stored as multiple SMS in the memory. For example, if the MT concatenated SMS contains 4 segments, then the SMS will use 4 SMS memory slots for its storage. Thus, when receiving concatenated SMS, it is recommended to regularly check SMS memory usage otherwise once it is full the UE will not be able to receive any SMS (text or PDU-mode)

8. Low Power with PSM

Please refer to the power consumption measurements application note for more details on low power mode with RYZ014 modules.

8.1 How to Use PSM Feature

8.1.1 Feature Description

A UE may use the PSM (Power Saving Mode) to reduce its power consumption.

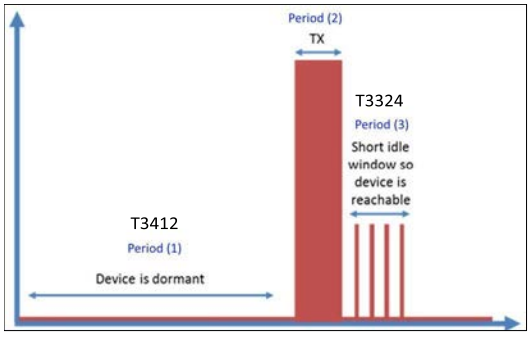


Figure 7. Behavior in PSM

When the device is dormant, the UE is not reachable from the network. However, it remains registered to the network and there is no need to re-attach or re-establish PDN connections at wake up. A UE in PSM can be reached by the network when it is in connected mode (period 2) and for the following short idle window (period 3).

The connected mode (period 2) is caused by a mobile originated event such as data transfer or signaling, for example, after a periodic TAU/RAU procedure. PSM is intended for UEs that are expecting infrequent mobile originating services.

Two timers are used to activate PSM:

- T3324 defines the short idle window (period 2) during which the device is reachable.
- T3412 defines the duration between two TAUs (Tracking Area Updates) during which the device can be dormant (period 1).

Table 5 presents the mapping for the T3324 timer. Bits 4 to 0 represent the binary coded timer value and bits 5 to 7 define the timer value unit for the GPRS timer.

Table 3. Bitmap for Unit of T3324 Timer

	Bits		
7	**6**	**5**	**Unit**
0	0	0	Value is incremented in multiples of 2 seconds
0	0	1	Value is incremented in multiples of 1 minute
0	1	0	Value is incremented in multiples of decihours
1	1	1	Value indicates that the timer is deactivated.

Table 6 presents the mapping for the T3412 timer. Bits 4 to 0 represent the binary coded timer value and bits 5 to 7 define the timer value unit for the GPRS timer.

Table 45. Bitmap for Unit of T3412 Timer

Bits			
7	**6**	**5**	**Unit**
0	0	0	Value is incremented in multiples of 10 minutes
0	0	1	Value is incremented in multiples of 1 hour
0	1	0	Value is incremented in multiples of 10 hours
0	1	1	Value is incremented in multiples of 2 seconds
1	0	0	Value is incremented in multiples of 30 seconds
1	0	1	Value is incremented in multiples of 1 minute
1	1	0	Value is incremented in multiples of 320 hours (see note [1])
1	1	1	Value indicates that the timer is deactivated (see note [2]).

Note: 1. This timer value unit is only applicable to the T3312 extended value IE and the T3412 extended value IE (see 3GPP TS 24.301 [120]). If it is received in an integrity protected message, value shall be interpreted as multiples of 320 hours. Otherwise value shall be interpreted as multiples of 1 hour.

2. This timer value unit is not applicable to the T3412 extended value IE. If this timer value is received, the T3412 extended value IE shall be considered as not included in the message (see 3GPP TS 24.301 [120]).

Related AT commands are:

- AT+CPSMS
- AT+CEREG
- URC +CEREG

Note: In order to optimize the power consumption, it is strongly recommended to set the value of T3412 to a value **higher than the duration between two waking-ups of the modem by the external MCU** (to send data for instance). A device in PSM should not wake-up for TAU, to get the most efficient power management.

8.1.2 Use Case

Command	Response	Comment
Enable PSM and configure requested T3412 Extended and T3324 timers		
AT+CPSMS=1,,,"10100011","0 0100001"	OK	1: Enable the use of PSM "10100011": Requested Periodic TAU timer (T3412 Extended), 3 minutes "00100001": Requested Active timer (T3324), 1 minute
Query current configured T3412 Extended and T3324 requested value **Note:** T3412 (extended) and T3324 value are decided by the network. They may differ from the values configured in the UE.		
AT+CPSMS?	+CPSMS: 1,,,"10100011","00100001" OK	1: Enable the use of PSM "10100011": Requested Periodic TAU timer (T3412 Extended), 3 minutes here "00100001": Requested Active timer (T3324), 1 minute
Query current used T3412 Extended and T3324 value:		
AT+CEREG=4	OK	4: For a UE that wants to apply PSM, enable network registration and location information unsolicited result code +CEREG
AT+CFUN=1	OK	
After successful attach or completed TAU, check the URC +CEREG		
	+CEREG: 1,"0002","01A2D004",7,,,"00000101", "00010010"	7: E-UTRAN (Cat-M1 mode) Active time(T3324), 10 seconds Periodic TAU timer (T3412 (extended)), 180 minutes
Retrieve the used value manually after type AT+CEREG=4		
AT+CEREG?	+CEREG: 4,1,"0002","01A2D002",7,,, " 00000101", "0000010" OK	7: E-UTRAN Active time(T3324), 10 seconds Periodic TAU timer (T3412 (extended)), 180 minutes
Disable PSM configuration		
AT+CPSMS=0	OK	0: Disable the use of PSM

8.2 PSM Troubleshooting

When the UE is dormant, the AT UART becomes unresponsive. The external host MCU can decide to wake the modem up to send some data. In that case, the UE will take some time to initialize the UART ports again. If the host MCU supports hardware flow control, the command will be buffered. If the host MCU does not support hardware flow control, it should first toggle the WAKE line to wake the platform up and then wait for the PS_STATUS line to be at 1 before sending any command.

PSM features need to be supported on both the UE and network side. Please note that some operators do not support PSM features, especially when using MVNO SIM cards. When the features are supported on network side, it can use different cycle/timer values than the one requested by the UE.

- In PSM the final timer values will be given in the +CEREG URC:
  `+CEREG: 1,"0002","01A2D004",7,,,"00000101","00010010"`

The following conditions need to be fulfilled to enter Deep Sleep mode during PSM sleep period:

- All wake sources are released:
- All UART buffers are empty
  - Every URC on all the UART configured as AT ports have been read by the host MCU
- The estimated sleep duration is long enough
  - RYZ014 modules do not enter Deep Sleep mode if a timer is scheduled to fire within a few tenths of a second

8.3 Maximum Transmission Power Reduction

To save still more power, it is possible to limit the Tx power with the following commands:

- AT+SQNDPR
- AT+SQNTXPWR

These commands can also be used to support the Specific Absorption Rate (SAR) reduction feature or for thermal mitigation.

Note: These settings should be re-entered after each reboot.

Command	Response	Comment
AT+CFUN=0	OK	
AT+SQNDPR=0,1	OK	
AT+SQNTXPWR=0,20,2200,0	OK	Limit to 22 dBm
AT+CFUN=1	OK	

9. Informal Network Scan

9.1 Feature Description

Two different AT commands can be used to get information on the serving and neighboring cells.

- AT+SQNINS
  This command can be used only when +CFUN status is 0 or 4.
- AT+SQNMONI

The modem will scan all the supported bands.

9.2 Use Cases

9.2.1 AT+SQNINS Usage

Command	Response	Comment
AT+CFUN=0	OK	
Report on all bands, fast informal network scanning (reporting of information extracted from Master information Block and System Information Block 1).		
	+SQNINS: 0,4,7,"0","0000","000000",2000,155,1.4,-92.00,-13.80 +SQNINS: 0,12,7,"1A2D001","0001","00101",5095,1,5,-78.10,-5.00 +SQNINS: 0,28,7,"0","0000","000000",9560,357,1.4,-84.80,-14.20 +SQNINS: 0,28,7,"1BE1A11","2B5C","46605",9260,151,10,-82.00,-13.50 +SQNINS: 0,3,7,"0","0000","000000",1550,18,1.4,-81.60,-11.50 +SQNINS: 0,1,7,"0","0000","000000",50,155,1.4,-92.20,-13.40 +SQNINS: 0,8,7,"0","0000","000000",3650,414,1.4,-91.10,-15.30 +SQNINS: 0,8,7,"0","0000","000000",3650,422,1.4,-90.40,-15.50 +SQNINS: 0,3,7,"0","0000","000000",1275,357,1.4,-97.10,-20.30 +SQNINS: 0,3,7,"3453A21","2E19","46692",1750,422,20,-99.30,-17.30 +SQNINS: 0,3,7,"3453A17","2E19","46692",1750,430,20,-101.00,-20.40 +SQNINS: 0,20,7,"0","0000","000000",6170,357,1.4,-85.20,-15.40 +SQNINS: 0,3,7,"0","0000","000000",1400,422,1.4,-98.00,-13.60 +SQNINS: 0,3,7,"0","0000","000000",1400,234,1.4,-103.90,-18.10 +SQNINS: 0,1,7,"0","0000","000000",525,414,1.4,-101.90,-18.20 +SQNINS: 0,1,7,"0","0000","000000",525,422,1.4,-98.00,-14.80 +SQNINS: 0,28,7,"0","0000","000000",9385,18,1.4,-75.10,-9.00 +SQNINS: 0,1,7,"0","0000","000000",275,4,1.4,-101.60,-17.50 +SQNINS: 0,1,7,"0","0000","000000",275,5,1.4,-99.70,-16.60 +SQNINS: 0,4,7,"0","0000","000000",2225,274,1.4,-102.10,-17.60 +SQNINS: 0,4,7,"0","0000","000000",2225,5,1.4,-100.50,-16.70 +SQNINS: 0,8,7,"0","0000","000000",3550,279,1.4,-87.50,-17.30 +SQNINS: 0,8,7,"0","0000","000000",3550,376,1.4,-93.50,-23.10 +SQNINS: 0,8,7,"0","0000","000000",3750,400,1.4,-113.80,-16.70	
AT+SQNINS=0	OK	

9.2.2 AT+SQNMONI Usage

Command	Response	Comment
Report on serving cell only.		
AT+SQNMONI=0	+SQNMONI: Orange F Cc:208 Nc:01 RSRP:-104.90 RSRQ:-17.50 TAC:52644 Id:196 EARFCN:6400 PWR:-79.62 PAGING:64 CID:0x1707308 BAND:20 BW:10000 OK	
Report information for the serving cell only with RSRP/CINR on main antenna.		
AT+SQNMONI=9	+SQNMONI: Orange F Cc:208 Nc:01 RSRP:-104.40 CINR:-6.10 RSRQ:-18.60 TAC:52644 Id:196 EARFCN:6400 PWR:-78.02 PAGING:64 CID:0x1707308 BAND:20 BW:10000 OK	

9.2.3 Error Handling

During PSM sleep, the UE is not monitoring the network, therefore AT+SQNMONI will return ERROR. In that case, it is recommended to make sure that the UE attaches to the network with a ping (AT+PING="www.Renesas.com",1,32 for example).

Note: AT+SQNINS cannot provide cell identity information such as the CID, the PLMN or the TAC for non-Cat-M1 cells. A Cat M1 modem can decode 4G MIBs, however it cannot decode SIB1 for non-Cat-M1 cells.

10. Hardware Configuration

10.1 UART Interfaces

RYZ014 modules can be controlled via a serial interface UART using standard AT commands. The serial AT interface can be connected using HW flow control or not. Please refer to the *System Integration Guide* for more details.

The RYZ014-based modem is designed to be used as DCE (Data Communication Equipment). It communicates with the customer application (DTE for Data Terminal Equipment) based on DCE-DTE convention.

Note: Please refer to the module's datasheet for more details on UART interfaces.

10.2 How to Configure the RING Signal

10.2.1 Feature Description

RING is a pre-defined signal which is used to notify the Host that there is an URC, or Data, or SMS coming from the network. RING should be monitored especially during the following specific cases:

- Immediate URC presentation is impossible, for instance UART running a long AT command or in online data connection mode
- Immediate data transmission to host when AT channel in data mode (PPP, transparent socket) is impossible
- Host not ready to receive on UART interface (RTS line high level or in sleep mode)

RING behavior can be configured by using the AT command AT+SQNRICFG.

10.2.2 Use Cases

Command	Response	Comment
All events are indicated by activated RING0 line of the UART0 interface, whatever event AT channel origin.		
AT+SQNRICFG=1,3	OK	
AT+SQNRICFG?	+SQNRICFG: 1,3,1000 OK	
RING activation triggered by general URC events only, and only the event on UART0 triggers RING signal.		
AT+SQNRICFG=2,1	OK	
AT+SQNRICFG?	+SQNRICFG: 2,1,1000 OK	
Change the duration to 2s, and keep others default settings.		
AT+SQNRICFG=2000	OK	
AT+SQNRICFG?	+SQNRICFG: 2,3,1000 OK	

10.3 How to Configure Modem Alarms

10.3.1 Feature Description

In some cases, MCU needs to set timers in the module and get an alarm when expired.

AT+CALA and AT+CALD are 3GPP standard AT commands defined in specification 27.007.

The related AT commands are:

- AT+CALA
- AT+CALD
- URC +CALV
- AT+CCLK

10.3.2 Use Cases

10.3.2.1 Get Current Time/Date

Command	Response	Comment
The time set in the AT is absolute time. A timer is usually based on current time. Get the time as follows.		
AT+CCLK?		
If the module is attached to a network, the current time/date is retrieved from network during attachment.		
	+CCLK: "22/04/26,17:14:55+32" OK	
If the module is NOT attached to network, read a time/date set from the start of Jan. 1st of 1970. In this case, set a time manually, or use this time/date for tests.		
	+CCLK: "70/01/01,00:00:10+00" OK	

10.3.2.2 Set Alarm, in Format Date-Time

Command	Response	Comment
Set the time		
AT+CCLK="19/01/01,00:00:00+00"	OK	
Set alarm timer		
AT+CALA="19/01/01,00:01:00+00",0,0,"first alarm"		
	OK	
	+CALV: 0 first alarm	60 seconds later

10.3.2.3 Set Alarm Time Recurring All Days

Command	Response	Comment
Set date/time with +CCLK		
AT+CCLK="22/01/01,00:01:00+00"	OK	
Set alarm timer		
AT+CALA="00:01:30+00",1,0,"second","0",1		
	OK	
Check alarm timer		
AT+CALA?	+CALA: "22/01/01,00:01:00",0,0,"first alarm",0 +CALA: "22/01/01,00:01:30",1,0,"second","1,2,3,4,5,6,7",1 OK	
	+CALV: 1	30 s. later. Due to “silent” is 1, no text is displayed here
Check the date is shifted for next day ('tomorrow').		

Command	Response	Comment
AT+CALA?	+CALA: "22/01/01,00:01:00",0,0, "first alarm",0 +CALA: "22/01/02,00:01:30",1,0,"second ", "1,2,3,4,5,6,7",1 OK	Compared with above date, it is now “22/01/02”.

10.3.2.4 Set Alarm - Format Time Recurring Selected Days

Command	Response	Comment
AT+CCLK="22/01/01,00 :01:00+00"	OK	Set date/time by +CCLK
AT+CALA="00:02:00+00 ",2,0, "third alarm","2,7",0	OK	Set alarm timer
Check alarm timer		
AT+CALA?	+CALA: "22/01/01,00:01:00",0,0,"first alarm",0 +CALA: "22/01/02,00:01:30",1,0,"second","1,2,3,4,5,6,7",1 +CALA: "22/01/01,00:02:00",2,0,"third alarm","2,7",0 OK	
	+CALV: 2 third alarm	60 s. later
Check that the date is shifted according to recurrence days.		
AT+CALA?	+CALA: "22/01/01,00:01:00",0,0, "first alarm",0 +CALA: "22/01/02,00:01:30",1,0,"second”, "1,2,3,4,5,6,7",1 +CALA: "22/01/06,00:02:00",2,0, "third alarm","2,7",0 OK	Date is now “22/01/06”.

10.3.2.5 Overwrite Expired Alarm with the Same Alarm ID IS Possible

Command	Response	Comment
Check current alarm config		
AT+CALA?	+CALA: "19/01/01,00:01:00",0,0,"first alarm",0 +CALA: "19/01/02,00:01:30",1,0,"second","1,2,3,4,5,6,7",1 +CALA: "19/01/06,00:02:00",2,0,"third alarm","2,7",0 OK	
Overwrite timer #0 by set command		
AT+CALA="19/02/01,05 :05:05+00",0 ,0, "first alarm edited"	OK	
Check the timer again		

Command	Response	Comment
AT+CALA?	+CALA: "19/02/01,05:05:05",0,0,"first alarm edited",0 +CALA: "19/01/02,00:01:30",1,0,"second","1,2,3,4,5,6,7",1 +CALA: "19/01/06,00:02:00",2,0,"third alarm","2,7",0 OK	

10.3.2.6 Delete alarm

Command	Response	Comment
Delete alarm index 0		
AT+CALD=0	OK	
Delete alarm index 1		
AT+CALD=1	OK	
Delete alarm index 2		
AT+CALD=2	OK	
Check alarms		
AT+CALA?	OK	

11. Manufacturing

11.1 How to Configure GPIOs Alternate Functions

11.1.1 Feature Description

Several of the RYZ014 module GPIO signals have alternate functions that can be configured with AT+SQNHWCFG. The following functions can be achieved on RYZ014 module pins:

- Wake signal detection (wakeId = "wake0", "wake1", "wakeRTS0", "wakeRTS1", "wakeSim0") function control
- Antenna tuning (antennaTuning) function control
- TxIndicator
- Low-power mode
- Change UART configuration (uartId: uart0, uart1, uart2) function control

The configuration is non-volatile, unchanged by device reboots and software upgrades. Any modification in configuration needs a module's reboot to be effective.

The information returned by a read command corresponds to the configuration applicable after the next reboot. The active configuration will be overridden by the pending changes, if any.

Pins with unassigned functions are deactivated and configured in their default reset state. Refer to the module's data sheet for details.

Before setting up a specific function, it is mandatory to disable the GPIO pins settings on which this function is mapped.

11.1.2 Use Cases

11.1.2.1 Wake

WAKE0, WAKE1, RTS0 and RTS1 pins can be used as external sources to wake up the modem from low power mode.

The external wake sources have two different roles:

- If a wake signal is enabled, active and the platform wants to perform a LPM cycle, this wake signal prevents it from entering the low power state.
- If a wake signal is enabled, active and the platform is in low power, this wake signal wakes up the module.

WAKE inputs must last at least 100 µs in order to insure a reliable detection.

By default, WAKE0 and WAKE1 are configured as GPIOs (GPIO11 and GPIO12 respectively). The GPIO's function should first be deactivated before being able to use these pins as wake sources.

Command	Response	Comment
AT+CFUN=5	OK	Switch to manufacturing mode
Check wake sources configuration		
AT+SQNHWCFG?	(…) +SQNHWCFG: wake0: disable +SQNHWCFG: wake1: disable +SQNHWCFG: wakeRTS0: enable +SQNHWCFG: wakeRTS1: disable (…) OK	The read command returns the list of supported pin functions state and detailed configuration (when applicable). Wake0, wake1 and wakeRTS1 are disabled, wakeRTS0 is enabled (inverted polarity).
Enable wake1 with inverted polarity (negative polarity)		
AT+SQNHWCFG= "gpio12", "disable"		First, disable the GPIO function
AT+SQNHWCFG= "wake1", "enable", "inversed"	OK	If polarity parameter is omitted, it will be set to the signal's default polarity mentioned in the module's data sheet. Note that it is not possible to change the polarity of WakeRTS0 and WakeRTS1.
Reboot the device		
AT^RESET	OK	
	+SYSSHDN +SYSTART	
AT+CFUN=5	OK	Switch to manufacturing mode
Check the configuration		
AT+SQNHWCFG= "wake1"	+SQNHWCFG: wake1: enable, polarity: inversed OK	
Disable wakeRTS1		
AT+SQNHWCFG= "wakeRTS1", "disable"	OK	
Reboot the device		
AT^RESET	OK	
	+SYSSHDN +SYSTART	
AT+CFUN=5	OK	Switch to manufacturing mode
Check the configuration		
AT+SQNHWCFG= "wakeRTS1"	+SQNHWCFG: wakeRTS1: disable OK	

11.1.2.2 Antenna Tuning

On small PCBs, it is difficult to design a proper antenna matching circuit for a wide range of frequencies. One option consists of tuning the antenna matching dynamically, according to the active RF band. The configuration command AT+SQNHWCFG="antennaTuning" can be used to activate, deactivate and configure the antenna tuner. In the example below, RFDATA5 and RFDATA6 are used to control the RF switch as follows:

	617 MHz - 698 MHz	797 MHz - 887 MHz	887 MHz - 2200 MHz	698 MHz - 797 MHz
RFDATA6 (ANT_TUNE0)	0	1	0	1
RFDATA5 (ANT_TUNE1)	0	0	1	1

Command	Response	Comment
AT+CFUN=5	OK	Switch to Manufacturing Mode
Enable antenna tuning feature and configure it. The configuration is persistent.		
AT+SQNHWCFG="antennaTuning", "enable","0x0","617,698,0x00,698,797,0x80,797,887,0x40,887,2200,0xC0"	OK	"0x0"is the default value used for all frequencies outside the definition scope. "617,698,0x0,….": A list of triplets. Each triplet defines one frequency scope and related pin values.
Reboot the device		
AT^RESET	OK	
	+SYSSHDN +SYSTART	
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG="antennaTuning"		+SQNHWCFG: antennaTuning: enable, value: 0x0, [617-698]MHz: 0x0, [698-797]MHz: 0x2, [797-887]MHz: 0x1, [887-2200]MHz: 0x3

11.1.2.3 Tx Indicator

The transmission indicator (TX_IND, OUT) is used to warn the host that the modem is transmitting data. It is not possible to change the polarity of this signal.

Command	Response	Comment
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG="txIndicator"	+SQNHWCFG: txIndicator: disable OK	
AT+SQNHWCFG="txIndicator", "enable"	OK	
Reboot the device		
AT^RESET	OK	
	+SYSSHDN +SYSTART	

11.1.2.4 Low Power Mode Configuration

The low power mode is configurable using `AT+SQNHWCFG="lpm"[,("disable","enable")]` command. It is enabled by default.

Command	Response	Comment
`AT+CFUN=5`	`OK`	Switch to Manufacturing Mode
`AT+SQNHWCFG="lpm"`	`+SQNHWCFG: lpm: enabled` `OK`	
`AT+SQNHWCFG="lpm","disable"`	`OK`	
Reboot the device		
`AT^RESET`	`OK`	
	`+SYSSHDN` `+SYSTART`	
`AT+CFUN=5`	`OK`	Switch to Manufacturing Mode
`AT+SQNHWCFG="lpm"`	`+SQNHWCFG: lpm: disabled` `OK`	

11.1.2.5 UART Configuration

There are three UARTs available in RYZ014 modules, each of them is configurable.

Command	Response	Comment
`AT+CFUN=5`	`OK`	Switch to Manufacturing Mode
`AT+SQNHWCFG="uart0"`	`+SQNHWCFG: uart0: enable, flowcontrol: rtscts, baudrate: 921600, format: 8 bits, parity: none, stopbits: 1, application: at` `OK`	
`AT+SQNHWCFG="uart1"`	`+SQNHWCFG: uart1: enable, flowcontrol: unsupported, baudrate: 115200, format: 8 bits, parity: none, stopbits: 1, application: console` `OK`	
`AT+SQNHWCFG="uart2"`	`+SQNHWCFG: uart2: enable, flowcontrol: rtscts, baudrate: 921600, format: 8 bits, parity: none, stopbits: 1, application: dcp` `OK`	
`AT+SQNHWCFG="uart2","enable","rtscts","921600","8","none","1","at"`	`OK`	Configure UART2 with AT application if you need second AT port
`AT^RESET`	`OK`	Reboot the device
	`+SHUTDOWN` `+SYSTART`	
`AT+CFUN=5`	`OK`	Switch to Manufacturing Mode
`AT+SQNHWCFG="uart2"`	`+SQNHWCFG: uart2: enable, flowcontrol: rtscts, baudrate: 921600, format: 8 bits, parity: none, stopbits: 1, application: at` `OK`	

11.2 Continuous Wave

In non-signaling test mode, the modem can generate a continuous wake (Tx tone) or measure the power (RSSI) of an RF tone. Starting a new Tx continuous wave automatically cancels an ongoing one.

Important: As the minimum supported bandwidth is 5 MHz, if E1 is the lowest EARFCN of the band and E2 the highest, the tone EARFCN should be in the range of [E1+2.5; E2-2.5]. For example, B3 UL goes from EARFCN 19200 to 19449, a valid EARFCN for that band would be between 19203 and 19446.

Important: Because of the DC rejection, it is not possible to perform RX measurements at the center frequency. Use the AT command (AT+SMCWRX=mid channel) and set the signal generator at a ±100 kHz offset. For example, on band 19, use AT+SMCWRX=6075 (corresponding to a center channel frequency of 882.5 MHz) and set the signal generator at 882.6 MHz.

Command	Response	Comment
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SMCWTX=1,20175,1000	OK	Start Tx tone on EARFCN 20175 (Band 4, 1732.5MHz) at 10 dBm
AT+SMCWTX?	+SMCWTX: 1,20175,1000 OK	
AT+SMCWTX=0	OK	Stop Tx tone generation
AT+SMCWTX=1	OK	Restart Tx tone with previous settings
AT+SMCWTX?	+SMCWTX: 1,20175,1000 OK	
Check the detected power on EARFCN 2175 (Band 4, 2132.5 MHz)		
AT+SMCWRX=2175	+SMCWRX: -8986 OK	Measured RSSI is -89.86 dBm

12. Appendix. Glossary and Abbreviations

Term	Description
ADC	Analog to Digital Converter
Airplane mode	Device mode where the modem is ON, but the RF functions are OFF
AT	Prefix for AT commands. Historical prefix for Hayes commands, meaning“Attention”
DL	Downlink
DUP	File extension used for upgrade procedures
EPS	Evolved Packet System
FTP	File Transfer Protocol
Full function mode	Device mode where all the functions are ON
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IMSI	International Mobile Subscriber Identity
MCC	Mobile Country Code
MNC	Mobile Network Code
NAS	Non-Access Stratum
PDU	Packet Data Unit
PIN	Personal Identification Number
PUK	Personal Unblocking Key
RF	Radio Frequency
SIM	Subscriber Identity Module
SMS	Short Message Service
TAU	Target Acquisition and Tracking Unit
UE	User Equipment
UL	Uplink
URC	Unsolicited Response Command
DCE	Data Communications Equipment
DTE	Data Terminal Equipment
BIP	Bearer Independent Protocol
CTS	Clear To Send
RTS	Request To Send
eDRX	Extended Discontinuous Reception
PSM	Power Saving Mode
MCU	Microcontroller Unit
UART	Universal Asynchronous Receiver Transmitter

Term	Description
PPP	Point to Point Protocol
SMSC	SMS Center
GPIO	General Purpose Input Output
RRC	Radio Resource Control
PMU	Power Management Unit
LTE	Long Term Evolution
APN	Access Point Name
PDN	Packet Data Network
PLMN	Public Land Mobile Network
EARFCN	E-UTRA Absolute Radio Frequency Channel Number
IMEI	International Mobile Equipment Identity
IMSI	International mobile subscriber identity
HLR	Home Location Register
FOTA	Firmware Over The Air
TAU	Tracking Area Update
LwM2M	Lightweight Machine to Machine
PER	Packet Error Rate
USIM	Universal Subscriber Identity Module

Revision History

		Description	
Rev.	Date	Page	Summary
1.00	Apr.16.21	—	Initial release
1.50	Mar.15.22	—	Overall update
2.00	Aug.29.22	—	Updated section 5, section 6.3, 6.4, section 8.4, section 11. General updates overall.
2.10	Oct. 26.22	—	Updated section 8, deleted eDRX
2.20	May.16.23	—	Corrected +SQNSUPGRADE URC. T3324 definition typo corrected. Added section 11.2, Continuous Wave.

Notice

1. Descriptions of circuits, software and other related information in this document are provided only to illustrate the operation of semiconductor products and application examples. You are fully responsible for the incorporation or any other use of the circuits, software, and information in the design of your product or system. Renesas Electronics disclaims any and all liability for any losses and damages incurred by you or third parties arising from the use of these circuits, software, or information.
2. Renesas Electronics hereby expressly disclaims any warranties against and liability for infringement or any other claims involving patents, copyrights, or other intellectual property rights of third parties, by or arising from the use of Renesas Electronics products or technical information described in this document, including but not limited to, the product data, drawings, charts, programs, algorithms, and application examples.
3. No license, express, implied or otherwise, is granted hereby under any patents, copyrights or other intellectual property rights of Renesas Electronics or others.
4. You shall be responsible for determining what licenses are required from any third parties, and obtaining such licenses for the lawful import, export, manufacture, sales, utilization, distribution or other disposal of any products incorporating Renesas Electronics products, if required.
5. You shall not alter, modify, copy, or reverse engineer any Renesas Electronics product, whether in whole or in part. Renesas Electronics disclaims any and all liability for any losses or damages incurred by you or third parties arising from such alteration, modification, copying or reverse engineering.
6. Renesas Electronics products are classified according to the following two quality grades: “Standard” and “High Quality”. The intended applications for each Renesas Electronics product depends on the product’s quality grade, as indicated below.
   "Standard": Computers; office equipment; communications equipment; test and measurement equipment; audio and visual equipment; home electronic appliances; machine tools; personal electronic equipment; industrial robots; etc.
   "High Quality": Transportation equipment (automobiles, trains, ships, etc.); traffic control (traffic lights); large-scale communication equipment; key financial terminal systems; safety control equipment; etc.

   Unless expressly designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not intended or authorized for use in products or systems that may pose a direct threat to human life or bodily injury (artificial life support devices or systems; surgical implantations; etc.), or may cause serious property damage (space system; undersea repeaters; nuclear power control systems; aircraft control systems; key plant systems; military equipment; etc.). Renesas Electronics disclaims any and all liability for any damages or losses incurred by you or any third parties arising from the use of any Renesas Electronics product that is inconsistent with any Renesas Electronics data sheet, user’s manual or other Renesas Electronics document.
7. No semiconductor product is absolutely secure. Notwithstanding any security measures or features that may be implemented in Renesas Electronics hardware or software products, Renesas Electronics shall have absolutely no liability arising out of any vulnerability or security breach, including but not limited to any unauthorized access to or use of a Renesas Electronics product or a system that uses a Renesas Electronics product. RENESAS ELECTRONICS DOES NOT WARRANT OR GUARANTEE THAT RENESAS ELECTRONICS PRODUCTS, OR ANY SYSTEMS CREATED USING RENESAS ELECTRONICS PRODUCTS WILL BE INVULNERABLE OR FREE FROM CORRUPTION, ATTACK, VIRUSES, INTERFERENCE, HACKING, DATA LOSS OR THEFT, OR OTHER SECURITY INTRUSION (“Vulnerability Issues”). RENESAS ELECTRONICS DISCLAIMS ANY AND ALL RESPONSIBILITY OR LIABILITY ARISING FROM OR RELATED TO ANY VULNERABILITY ISSUES. FURTHERMORE, TO THE EXTENT PERMITTED BY APPLICABLE LAW, RENESAS ELECTRONICS DISCLAIMS ANY AND ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THIS DOCUMENT AND ANY RELATED OR ACCOMPANYING SOFTWARE OR HARDWARE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.
8. When using Renesas Electronics products, refer to the latest product information (data sheets, user’s manuals, application notes, “General Notes for Handling and Using Semiconductor Devices” in the reliability handbook, etc.), and ensure that usage conditions are within the ranges specified by Renesas Electronics with respect to maximum ratings, operating power supply voltage range, heat dissipation characteristics, installation, etc. Renesas Electronics disclaims any and all liability for any malfunctions, failure or accident arising out of the use of Renesas Electronics products outside of such specified ranges.
9. Although Renesas Electronics endeavors to improve the quality and reliability of Renesas Electronics products, semiconductor products have specific characteristics, such as the occurrence of failure at a certain rate and malfunctions under certain use conditions. Unless designated as a high reliability product or a product for harsh environments in a Renesas Electronics data sheet or other Renesas Electronics document, Renesas Electronics products are not subject to radiation resistance design. You are responsible for implementing safety measures to guard against the possibility of bodily injury, injury or damage caused by fire, and/or danger to the public in the event of a failure or malfunction of Renesas Electronics products, such as safety design for hardware and software, including but not limited to redundancy, fire control and malfunction prevention, appropriate treatment for aging degradation or any other appropriate measures. Because the evaluation of microcomputer software alone is very difficult and impractical, you are responsible for evaluating the safety of the final products or systems manufactured by you.
10. Please contact a Renesas Electronics sales office for details as to environmental matters such as the environmental compatibility of each Renesas Electronics product. You are responsible for carefully and sufficiently investigating applicable laws and regulations that regulate the inclusion or use of controlled substances, including without limitation, the EU RoHS Directive, and using Renesas Electronics products in compliance with all these applicable laws and regulations. Renesas Electronics disclaims any and all liability for damages or losses occurring as a result of your noncompliance with applicable laws and regulations.
11. Renesas Electronics products and technologies shall not be used for or incorporated into any products or systems whose manufacture, use, or sale is prohibited under any applicable domestic or foreign laws or regulations. You shall comply with any applicable export control laws and regulations promulgated and administered by the governments of any countries asserting jurisdiction over the parties or transactions.
12. It is the responsibility of the buyer or distributor of Renesas Electronics products, or any other party who distributes, disposes of, or otherwise sells or transfers the product to a third party, to notify such third party in advance of the contents and conditions set forth in this document.
13. This document shall not be reprinted, reproduced or duplicated in any form, in whole or in part, without prior written consent of Renesas Electronics.
14. Please contact a Renesas Electronics sales office if you have any questions regarding the information contained in this document or Renesas Electronics products.

(Note1) “Renesas Electronics” as used in this document means Renesas Electronics Corporation and also includes its directly or indirectly controlled subsidiaries.
(Note2) “Renesas Electronics product(s)” means any product developed or manufactured by or for Renesas Electronics.

(Rev.5.0-1 October 2020)

Corporate Headquarters

TOYOSU FORESIA, 3-2-24 Toyosu,
Koto-ku, Tokyo 135-0061, Japan
www.renesas.com

Trademarks

Renesas and the Renesas logo are trademarks of Renesas Electronics Corporation. All trademarks and registered trademarks are the property of their respective owners.

Contact information

For further information on a product, technology, the most up-to-date version of a document, or your nearest sales office, please visit:
www.renesas.com/contact/.