Renesas RYZ024

Use Cases for AT Commands

Contents

1. General Introduction 6

2. Network Connection 6

2.1 Check that the SIM Card is Ready 6

2.1.1 Feature Description 6

2.1.2 Use Cases 7

2.1.2.1 Select the SIM Slot 8

2.1.2.2 Power on the SIM Slot 8

2.1.2.3 Check the SIM Card Status after Powering on the SIM Slot 8

2.1.2.4 Enable SIM Lock with PIN Code 8

2.1.2.5 Disable SIM Lock with PIN Code 9

2.1.2.6 Enter PIN Code to Unlock SIM 9

2.1.2.7 Enter PUK Code to Unlock SIM 10

2.1.3 Error Handling 10

2.2 Configure the Operator Mode 11

2.2.1 Feature Description 11

2.2.2 Use Cases 12

2.2.2.1 Check the Currently Configured Operator Mode 12

2.2.2.2 Limit the Number of Bands 12

2.2.2.3 Define Preferred EARFCN to be Scanned in Priority 13

2.2.2.4 Select a specific operator mode 15

2.2.3 Error Handling 15

2.3 Connect to the Network and Check Attach is Done 15

2.3.1 Feature Description 15

2.3.2 Use Cases 16

2.3.2.1 Attach to the Network. 16

2.3.2.2 Check the Network's Registration Status 16

2.3.2.3 Check the PDP Context Configuration 17

2.3.2.4 Activate a PDP Context 17

2.3.2.5 Check the IP Address 18

2.3.2.6 Check the RSRP and RSRQ Values 18

2.3.2.7 Detach from the Network 18

2.3.2.8 Force an Attachment to a Specific Operator (AT+COPS) 19

2.3.3 Error Handling 20

3. How to Manage TLS Certificates 22

3.1 Feature Description 22
3.2 Use Cases with Certificates 23
3.2.1 Add Certificate at Index 19 24
3.2.2 Read Certificate at Index 0 24
3.2.3 Remove Certificate at Index 19 24
3.3 Use Cases with Private Keys 24
3.3.1 Upload a Private Key at Index 1 24
3.3.2 Read the Private Key at Index 1 25
3.3.3 Remove the Private Key at Index 1 25
3.4 Use Cases to Setup a Security Profile 25
3.4.1 With a Private Key Stored in the Non-Volatile Memory (NVM) 25
3.4.2 With a Private Key Stored in a Host Crypto Engine 27
3.5 Error Handling 29

4. Renesas' Proprietary FOTA 29
4.1 Feature Description 29
4.2 Use Cases 30
4.2.1 Synchronous Upgrade using HTTPS Protocol 30
4.2.2 Synchronous Upgrade using HTTPS Protocol with Certificates 30
4.2.3 Asynchronous Upgrade using HTTPS Protocol 31
4.2.4 Cancel Asynchronous Upgrade with HTTPS Protocol 32
4.2.5 Asynchronous Upgrade using FTP Protocol 32
4.2.6 Cancel Asynchronous Upgrade 33
4.2.7 Asynchronous Upgrade though FTP using a Specific Port 33
4.2.8 Upgrade from local file 34
4.3 Error Handling 34

5. Factory Reset 34
5.1 Feature Description 34
5.2 Use Cases 35
5.3 Error Handling 35

6. Data over UART 35
6.1 How to Send Data with UDP 36
6.1.1 Feature Description 36
6.1.2 Use Cases in Online Mode 37
6.1.3 Use Cases in Command Mode 38
6.1.4 Accept Any Remote Option 38
6.1.4.1 Receive Data from a Different Server 38
6.1.4.2 Send Data to Different Server within the Same Socket 39
6.1.5 Error Handling 40
6.2 How to Send Data with TCP 40

6.2.1 Feature Description 40
6.2.2 Use Cases in Online Mode 41
6.2.3 Use Cases in Command Mode with Text Data 42
6.2.4 Use Cases in Command Mode with Hex Data 43
6.2.5 Error Handling 44
6.3 How to Setup a Secure Socket Connection 44
6.3.1 Feature Description 44
6.3.2 Use Cases 44
6.4 How to Send Data on a HTTP(S) Connection 46
6.4.1 Feature Description 46
6.4.2 Use Cases in Synchronous Mode with +SQNHTTP Commands 46
6.4.2.1 Send a GET Request 46
6.4.2.2 Send POST request with AT+SQNHTTPSND 47
6.4.2.3 Notes on <post-param> and <extra-header-line> Parameters 47
6.4.2.4 Test with Certificate Validation 48
6.4.2.5 Test with no Certificate in Filesystem 51
6.4.3 Use Case with +SQNFGET Command 51
6.4.4 Use Case with +SQNFPUT Command 52
6.4.5 Use Case in Asynchronous Mode with +SQNHTTP Command 53
6.4.6 Error Handling 54
6.5 How to Use TFTP AT Commands 55
6.5.1 Feature Description 55
6.5.2 Use Case 55
6.6 How to Use FTP(S) AT Commands 55
6.6.1 Feature Description 55
6.6.2 Use Cases 56
6.6.2.1 Synchronous Mode 56
6.6.2.2 Asynchronous mode 56
6.7 How to Use MQTT(S) Commands 57
6.7.1 Feature Description 57
6.7.1.1 AT Commands 57
6.7.1.2 MQTT and TLS 57
6.7.2 MQTT Server 57
6.7.2.1 Mosquitto 57
6.7.2.2 AWS IoT 57
6.7.2.3 Cloud IoT Core 59
6.7.3 Use Cases 60
6.7.3.1 Non-Encrypted 60
6.7.3.2 Encrypted 61
6.7.3.3 Encrypted and Client Certificate Required 63
6.7.4 Error Handling 65

6.8 How to Use CoAP(S) Commands 65
6.8.1 Setup Preparation 65
6.8.2 Use Case 66

7. SMS 67
7.1 How to Send and Receive SMS in Text Mode 69
7.1.1 Feature Description 69
7.1.2 Use Cases 69
7.1.2.1 Read SMS 69
7.1.2.2 Send SMS 70
7.1.2.3 Send SMS 70
7.1.2.4 Send a SMS in Korean Characters 72
7.2 How to Send and Receive a SMS in PDU Mode 72
7.2.1 Feature Description 72
7.2.2 Use Cases 73
7.2.2.1 Send SMS 73
7.2.2.2 Receive SMS 73
7.3 How to Manage SMS Storage 73
7.3.1 Feature Description 73
7.3.2 Use Cases 74
7.3.2.1 Find the Number and the Maximum Number of Messages 74
7.3.2.2 Select SIM as the Message Storage Area to be Used for SMS Receiving and Reading 74
7.3.2.3 Delete the SMS in the Modem 75
7.3.3 Error Handling 76

8. Low Power with eDRX and PSM 77
8.1 How to Use eDRX Feature 77
8.1.1 Feature Description 77
8.1.2 Use Cases 79
8.1.2.1 Enable eDRX, Set and Query eDRX Cycle and PTW Value 79
8.1.2.2 Disable eDRX 79
8.2 How to Use the PSM Feature 80
8.2.1 Feature Description 80
8.2.2 Use Case 81
8.3 eDRX and PSM Troubleshooting 82
8.4 Maximum Transmission Power Reduction 83

9. Informal Network Scan 83
9.1 Feature Description 83
9.2 Use Cases 83
9.2.1 AT+SQNINS Usage 83
9.2.2 AT+SQNMONI Usage 84

9.2.3 Error Handling 84

10. Hardware Configuration 84
10.1 UART Interfaces on RYZ024 84
10.2 How to Configure the RING Signal 84
10.2.1 Feature Description 84
10.2.2 Use Cases 85
10.3 How to Configure Modem Alarms 85
10.3.1 Feature Description 85
10.3.2 Use Cases 85
10.3.2.1 Get current time/date 85
10.3.2.2 Set alarm, in format date-time 86
10.3.2.3 Set an alarm recurring every day 86
10.3.2.4 Set an Alarm Recurring on Selected Days 86
10.3.2.5 Overwrite an Expired Alarm with the Same Alarm ID IS Possible 87
10.3.2.6 Delete an alarm 87

11. Manufacturing 88
11.1 How to Configure GPIOs Alternate Functions 88
11.1.1 Feature Description 88
11.1.2 Use Cases 88
11.1.2.1 PS_STATUS 88
11.1.2.2 Wake 89
11.1.2.3 Status_led 90
11.1.2.4 RING0 91
11.1.2.5 Antenna Tuning 92
11.1.2.6 SPI Configuration 93
11.1.2.7 I²C Configuration 94
11.1.2.8 JTAG 94
11.1.2.9 SIM Interface Configuration 94
11.1.2.10 TxIndicator 96
11.1.2.11 Low Power Mode Configuration 97
11.1.2.12 UART Configuration 97
11.1.2.13 ADC 98
11.1.2.14 GPIO Configuration 98
11.1.2.15 Behavior at Factory Reset 99
11.1.3 Error Handling 100
11.2 How to Set GPIO and Wake Signals 100
11.2.1 Setting GPIOs 101
11.2.1.1 Example with GPIO as Output 101
11.2.1.2 Example with GPIO as Input 101
11.2.2 Reading WAKE Signals 101

11.3 Continuous Wave 102
11.4 How to Check Module's Identities 102

12. System Features 103
12.1 Time Synchronisation 103
12.2 Battery Monitoring 104
12.3 Temperature Monitoring 105

13. Glossary and Abbreviations 106

Revision History 108

1. General Introduction

The host MCU can interact with the RYZ024 modem using:

- AT commands
  - This is the purpose of the current document.
- PPP protocol
  - Please refer to the PPP User Guide for more details on PPP connection setup with RYZ024 modules.

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

Please refer to the *System Integration Guide* for more information on AT commands types and AT parser implementation advice.

2. Network Connection

By default, the modem boots in the `+CFUN=0` state with minimal 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 connect your RYZ024-based device to the network, going through these simple steps:

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

2.1 Check that the SIM Card is Ready

2.1.1 Feature Description

Any RYZ024 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 lock or unlock the SIM card using the PIN or PUK code.

2.1.2 Use Cases

Command	Response	Comment
Power up the module		
	+SYSSTART	
Check the number of supported SIM slots. If response is +CSUS: 1, skip the following steps, since 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		
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?	208019706849013 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 change persists through reboots

2.1.2.1 Select the SIM Slot

Note: 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 SW upgrades.

2.1.2.2 Power on the SIM Slot

Pick one function mode amongst 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 `+SQNSIMST` URC		
AT+SQNSIMST=1	OK	Enable SIM state URC
AT+CFUN=4	OK	Set the modem to airplane mode 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 state with 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 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 with the "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 the 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 now 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 while in `CFUN=0` state returns `ERROR`.

If the SIM card is not present or not detected, check that the SIM card is inserted properly into the SIM slot and start again.

Command	Response	Comment
Enable 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 `+CSUS` command requires the UE to be in the `CFUN=0` state. If you get an error while using the `+CSUS` command, first check how many SIM slots are supported by the module, and then confirm an active `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

RYZ024 modules support up to 19 LTE bands. Scanning all the bands takes several minutes. As cell detection duration per candidate EARFCN is 30 ms, scanning the full 19 bands thus requires 186 seconds.

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 and a list of preferred EARFCN to be scanned with `AT+SQNEARFCNSEL`.

Several standard operator modes are preloaded by default in the module. The operator mode can be selected with the `AT+SQNCTM` command. For products using MVNO SIM cards and operating on several networks, it is recommended to keep the operator mode set to standard mode. Other operator modes are reserved for products targeting a specific operator, using the operator's SIM card, and requiring the operator's certification. The settings applicable to each operator mode are listed in the specification document of each operator the module is certified for.

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

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

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

Note: Please refer to 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 for 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 which are configured for each operator modes.		

Command	Response	Comment
AT+SQNBANDSEL?	+SQNBANDSEL: 0,3gpp-conformance,"" +SQNBANDSEL: 0,att,"2,4,12" +SQNBANDSEL: 0,docomo,"1,19" +SQNBANDSEL: 0,kddi,"18,26" 0,standard,"1,2,3,4,5,8,12,13,17, 18,19,20,25,26,28,66" +SQNBANDSEL: 0,verizon-no-roaming,"4,13" +SQNBANDSEL: 0,verizon,"13,4,5,12,17,20" OK	17 bands are configured for the standard operator mode.
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 Define Preferred EARFCN to be Scanned in Priority

Command	Response	Comment
AT+SQNEARFCNSEL?	+SQNEARFCNSEL: 0,3gpp-conformance,"" +SQNEARFCNSEL: 0,att,"" +SQNEARFCNSEL: 0,docomo,"" +SQNEARFCNSEL: 0,kddi,"" +SQNEARFCNSEL: 0, standard, "6200, 6300, 6400, 3700, 1444, 5035, 5110, 5230, 8615, 6100, 3750, 276, 252, 348, 475, 8890, 2500, 2600, 1350, 5900, 8750" +SQNEARFCNSEL: 0,tmo, "" +SQNEARFCNSEL: 0,verizon-no-roaming,"" +SQNEARFCNSEL: 0,verizon,"" OK	Check the preferred EARFCN defined for each operator mode by default
AT+SQNEARFCNSEL=0, "standard", "6200, 6300, 6400,3 700, 1444, 5035, 5110, 5230, 8615, 6100, 3750, 276, 252, 348, 475, 8890, 2500, 2600, 1350, 5900, 8750, 6250, 6350, 6351"	OK	Add EARFCNs to the list, up to 24. Copy/paste the list of default EARCFCN already provisioned and add new ones.
AT+SQNEARFCNSEL?	+SQNEARFCNSEL: 0,3gpp-conformance,"" +SQNEARFCNSEL: 0,att,"" +SQNEARFCNSEL: 0,docomo,"" +SQNEARFCNSEL: 0,kddi,"" +SQNEARFCNSEL: 0, standard, "6200, 6300, 6400, 3700, 1444, 5035, 5110, 5230, 8615, 6100, 3750, 276, 252, 348, 475, 8890,	

Command	Response	Comment
	2500, 2600, 1350, 5900, 8750, 6250, 6350, 6351" +SQNEARFCNSEL: 0,tmo,"" +SQNEARFCNSEL: 0,verizon-no-roaming,"" +SQNEARFCNSEL: 0,verizon,"" OK	
AT+SQNEARFCNSEL=0, "standard", "6200, 6300, 6400, 3700, 1444, 5035, 5110, 5230, 8615, 6100, 3750, 276, 252, 348, 475, 8890, 2500, 2600, 1350, 5900, 8750, 6250, 6350, 6450"	ERROR	Adding an EARFCN part of a band that is not supported by the module will return error (EARFCN 6450 is part of band 21)
AT+SQNEARFCNSEL=0, "standard", "6200, 6300, 6400, 3700, 1444, 5035, 5110, 5230, 8615, 6100, 3750, 276, 252, 348, 475, 8890, 2500, 2600, 1350, 5900, 8750, 6250, 6350, 6400, 6401, 6402"	OK	Adding more than 24 EARFCN will return OK. The additional EARFCNs are silently ignored
AT+SQNEARFCNSEL?	+SQNEARFCNSEL: 0,3gpp-conformance,"" +SQNEARFCNSEL: 0,att,"" +SQNEARFCNSEL: 0,docomo,"" +SQNEARFCNSEL: 0,kddi,"" +SQNEARFCNSEL: 0, standard, "6200, 6300, 6400, 3700, 1444, 5035, 5110, 5230, 8615, 6100, 3750, 276, 252, 348, 475, 8890, 2500, 2600, 1350, 5900, 8750, 6250, 6350, 6400" +SQNEARFCNSEL: 0,tmo,"" +SQNEARFCNSEL: 0,verizon-no-roaming,"" +SQNEARFCNSEL: 0,verizon,"" OK	EARFCN 6401 and 6402 are not configured. Note that the command does not detect doubles either (6400 was entered twice here)
Any EARFCN not part of configured band list configured with AT+SQNBANDSEL will be silently ignored during scanning operations		
AT+SQNEARFCNSEL=0,"standard",""	OK	Enter an empty list to reset the EARFCN list to the default values
AT+SQNEARFCNSEL?	+SQNEARFCNSEL: 0,3gpp-conformance,"" +SQNEARFCNSEL: 0,att,"" +SQNEARFCNSEL: 0,docomo,"" +SQNEARFCNSEL: 0,kddi,"" +SQNEARFCNSEL: 0, standard, "6200, 6300, 6400, 3700, 1444, 5035, 5110, 5230, 8615, 6100, 3750, 276, 252, 348, 475, 8890, 2500, 2600, 1350, 5900, 8750" +SQNEARFCNSEL: 0,tmo,"" +SQNEARFCNSEL: 0,verizon-no-roaming,"" +SQNEARFCNSEL: 0,verizon,"" OK	

Command	Response	Comment
Configuration is stored in non-volatile memory, persistent at device reboot and software upgrade. New configuration is applied at next re-connection to network (AT+CFUN=1).		

2.2.2.4 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: ("standard", "3gpp-conformance", "verizon", "verizon-no-roaming", "att", "docomo", "kddi") 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 users only: The `AT+SQNBANDSEL` command can be used 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 `AT+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

`AT+SQNBANDSEL` only limits the number of bands to be scanned with respect to the default configuration. It is not possible to add a new band to scan with this command. Any band given to the `AT+SQNBANDSEL` outside the standard set of a specific operator is ignored: the command does not return any error, but the band is not scanned.

2.3 Connect to the Network and Check 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`

Check the signal quality. In the response below, the first four values are not relevant for E-UTRA cells. The 5th parameter represents the RSRQ (Reference signal received quality), and the 6th parameter is the RSRP (Reference signal received power). Please refer to AT Commands User's Manual for details on values and levels.		
AT+CESQ	+CESQ: 99,99,255,255,8,45	If the RSRP is low, change to a different position and try again.

- `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 attaches 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 the 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 the current PDP context activation state		
AT+CGACT?		
	+CGACT: 1,1 +CGACT: 2,0 +CGACT: 3,0 +CGACT: 4,0 OK	The PDP context with cid 1 is activated

2.3.2.4 Activate a PDP Context

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

2.3.2.5 Check the IP Address

Command	Response	Comment
List the IP addresses of all cids		
AT+CGPADDR	+CGPADDR: 1,"192.168.6.3","32.1.4.104.48.6.0.3.32.1.4.104.48.6.0.3" +CGPADDR: 2 +CGPADDR: 3,"192.168.11.2" +CGPADDR: 4 OK	cid 1, IPv4 and IPv6 addresses; cid 2, not activated, no IP address; cid 3, IPv4 address only
Query the IP address of cid=1		
AT+CGPADDR=1	+CGPADDR: 1,"192.168.6.3","32.1.4.104.48.6.0.3.32.1.4.104.48.6.0.3" OK	cid 1, IPv4 and IPv6 addresses

2.3.2.6 Check the RSRP and RSRQ Values

The RSRP (Reference Signal Received Power) is the average of the power of the Resource Elements which carry cell-specific Reference Signal within the measurement frequency bandwidth. In other words, it represents the averaged received power of a Reference Signal per Resource Element.

The RSRQ (Reference signal received quality) is defined as RSRQ = N · RSRP/(LTE carrier RSSI),

- where N is the number of Resource Blocks in the current bandwidth
- RSSI is the total received power on the whole bandwidth including signal, noise and interference

The RSRQ provides a cell-specific signal quality metric.

Check the signal quality. In the response below, the first four values are not relevant for E-UTRA cells. The 5th parameter represents the RSRQ (Reference signal received quality), and the 6th parameter is the RSRP (Reference signal received power). Please refer to *AT Commands User's Manual* for details on values and levels.		
AT+CESQ	+CESQ: 99,99,255,255,8,45	If the RSRP is low, change to a different position and try again.

2.3.2.7 Detach from the Network

Command	Response	Comment
AT+CFUN=0	OK	Power-off the 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 `CFUN=0` command

2.3.2.8 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 to the AT&T network
	+CEREG: 2	
	+CEREG: 5,"0936","0C702F0F",7	

It is also possible to wait for the UE to go into Idle mode and send the COPS command. To check the UE status, you can refer to the CEINFO output.

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 +CEREG: 1,"CDA4","01704905",7	
Check the UE status: connected or idle		
AT+CEINFO?	+CEINFO: 0,1,C,8,32,-99,-3 OK	C means that the UE is connected, COPS cannot be used yet
AT+CEINFO?	+CEINFO: 0,0,I,0,0,-100,-4 OK	The UE received the RRC connection release message from the network and is not in idle mode. COPS command can be sent
AT+COPS=1,2,"310410",7	OK	Force the modem to attach on AT&T network
	+CEREG: 2	
	+CEREG: 5,"0936","0C702F0F",7	

2.3.3 Error Handling

If 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

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.

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

Command	Response	Comment
AT+CEREG?		Query network registration status
	+CEREG: 2,3 OK	

Command	Response	Comment
Possible causes: Illegal mobile equipment IMSI unknown at HLR (Home Location Register) PLMN not allowed		
Actions: Check if the right SIM card and the right device is used Check if the 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

If `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 `CEREG?` returns status 80, a PLMN loss indication is received from RRC. Most of the time, this means that the network rejected the modem.

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

In LTE-M, an APN auto configuration is sufficient in most cases, and 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 that mentioned in the above examples, the SMS service does not work.

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

3. How to Manage TLS Certificates

3.1 Feature Description

For best security, Renesas strongly advise to use TLS connections. TLS connections need a client certificate and the corresponding private key:

- The client certificate contains a public key and can be stored on the modem's Flash ROM in PEM format
- The private key should ideally be saved in a secure enclave responsible of message digest signature

Several private key storage and TLS server challenge signature strategies are supported:

- NVM: Private key stored in Non-Volatile Memory.
  - The TLS stack running on the modem CPU takes care of the message digest signature generation.
  - This mode corresponds to the legacy solution deployed on Monarch and RYZ024 modules
- HCE: Private key stored in Hosted Crypto Engine managed by host MCU
  - In this mode, the crypto engine can be embedded inside the host MCU or connected to a host MCU that is implementing an ECC pass through role.
  - The typical architecture is: **Module ↔ Host MCU ↔ ECE**
  - Host/Modem communication is done using AT commands: an URC is generated by the modem to request the message digest signature generation. The host MCU sends the signature using an AT command.
  - This mode can be activated on RYZ024 modules.

For secured socket connection it is necessary to write beforehand the certificate or the private key 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 the `AT+SQNSNVW` write command is issued, the user sends the 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 RYZ024 module has 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 RYZ024 module is preloaded with default certificates needed by some operator specific LwM2M servers.

To avoid erasing preloaded certificates, it is highly recommended to use slots 9 to 20 only.

In case of Hosted Crypto Engine, AT commands are defined to manage the message signature delegation to the host MCU:

- `+SQNHCESIGN` notification (URC) to request message signature
- `AT+SQNHCESIGN` to send back computed signature to modem

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 Unix (LF) encoding to get the right size of the certificate:

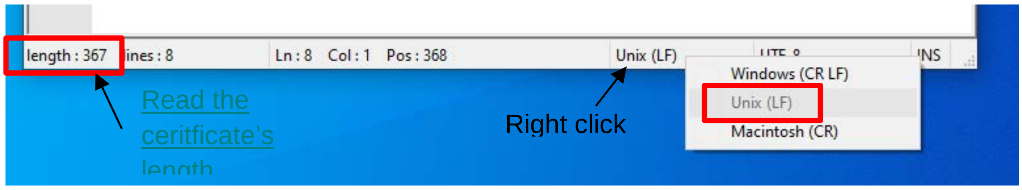

Figure 1. Select Unix (LF) Encoding

Command	Response	Comment
RYZ024 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","00000000000000000000000000000000000000000000000","/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","000","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","00","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","00","sha1","4418290c0af661843b28c70f4eb728f4cc462960" +SQNSNVR: "certificate",4,"/CN=root/OU=Service Platform Development department/O=SoftBank Corp./L=Minato-ku/C=JP","0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000","/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","0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000","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.		

3.2.1 Add Certificate at Index 19

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	

3.2.2 Read Certificate at Index 0

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/emailAd dr ess=roger@atchoo.org","0000000000000000000000000000000000000000000000000000000000000000000000000000000(...) 00000000000000000000000000000000000000000000000000","/C=GB/ST=United Kingdom/L=Derby/O=Mosquitto/OU=CA/CN=mosquitto.org/emailAd dr ess=roger@atchoo.org","12/06/29 22:11:59","22/06/27 22:11:59","sha1RSA","00000000000000000000","sha1","1d214e93 1ab1da59c 1e08f025f268d2783a51f0a" OK	

3.2.3 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",1,1 679		
	>	

Command	Response	Comment
After prompt '>', enter the data from certificate file and press Enter at the end.		
-----BEGIN RSA PRIVATE KEY----- MIIEpQIBAAKCAQEA0DeexyAY2TP1LeRL/MR7nVXzq+eQysfvZCzZVy39KXPtSaGL 5gHjlGS2ufB9ZB3KgOxSMlF+W7oqB6xa5FLMD4YQfgQiUux6kmuQZ4r3yvCUlOxD (...) 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 the prompt '>', enter the data from certificate file and type enter in the end.		

Command	Response	Comment
-----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 private key type file with size 1679 bytes into file system.		
AT+SQNSNVW="privatekey",0,1679		
	>	
After the 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, 19, 18, 0, "", ""	+SQNSPCFG: 1, 3, "", 1, 19, 18, 0, "", "" OK	By default, the last parameter <*storageId*> is set to 0 to indicate that the private key is stored in the NVM

3.4.2 With a Private Key Stored in a Host Crypto Engine

Command	Response	Comment
First, the user should generate a client certificate (public key) and private key pair and store the private key in the hosted crypto engine. The user needs to identify the private key index with an ID which is used by the module to pick the key during message signature. If HCE can only manage a single private key, the index can be set to any number. It is recommended to set it to 0. If the HCE can manage several private keys, the index shall be set in such way that host can easily map this number to the requested crypto engine key entry.		
Upload the client certificate (public key) into the module at index 19.		
AT+SQNSNVW="certificate",19,1078		
	>	
After the 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	

Command	Response	Comment
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	
Setup the security profile with both certificates stored on the NVM and the private key on the HCE 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=3,2,"",0,18,19,0,"","",1	+SQNSPCFG: 3,2,"",0,18,19,0,"","",1 OK	The last parameter `<storageId>` is set to 1 to indicate that the private key is stored in the HCE
This security profile needs then to be associated to the data connection configuration using either `AT+SQNSSPCFG` for secured sockets, `AT+SQNHTTPCFG`, `AT+SQNFGET`, `AT+SQNSMQTTCFG`, `AT+SQNCOAPCREATE`		
AT+SQNHTTPCFG=2,"ec2-3-134-42-3.us-east-2.compute.amazonaws.com",5061,0,"","",1,20,1,3		For example, to secure an HTTP connection, using security profile 3 defined above
	OK	
AT+SQNHTTPCONNECT=2		Open a secured HTTP connection
	OK	
The module generates `+SQNHCESIGN` URC for signature request to the host Wait URC '`+SQNHCESIGN`' for 30 seconds		
	URC: +SQNHCESIGN: 0,0,32,2eeba7aa6315f6f2739073099f0030099f979422e7d642bd7a3587feebb794a8	
Then host returns the signature with `AT+SQNHCESIGN` for TLS handshake		
AT+SQNHCESIGN=0,0,64,"7d04810fb275fea493bff24d73dfde4becb0129f5344cb917a8272123738b41b84a27bdc3106e5e4825f43fc4b759b5060883995d5e9f64381aecbb251733216"		
	OK	

3.5 Error Handling

AT+SQNSNVW can return +CME ERROR: operation not supported when the certificate is not correctly formatted or the length specified in the command does not match the content of the certificate including <CR>, <LF>, 'space' and so on. To get the exact file size, use Linux command "ls -l filename", or DOS command "dir", or open file with Notepad to check its length.

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 will display only the first certificate in the chain.

When using AT+SQNSNVW, if you get ERROR (CME_ERROR 4), first make sure that the certificate is valid. If the certificate is confirmed valid, please check that you use 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, when using <CR><LF> ("\r\n") as terminator, it would not affect most 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 stay in the buffer and be treated as input data. When sending data in text mode, the module does 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 ATS3 command, please refer to *AT Commands User's 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. Renesas' Proprietary FOTA

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

4.1 Feature Description

Three steps are enough to upgrade the firmware:

- Get the differential firmware packages from Renesas's release
- Upload the differential firmware packages on an external server.
- Execute AT+SQNSUPGRADE command to upgrade. The module will upgrade automatically.

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 filesystem 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 *diff DUP* (a .dup file including a differential upgrade). The differential FOTA upgrade allows the customer to upgrade the firmware over-the-air to a new version or revert to an old version as well. Before upgrading the firmware, the customer needs to prepare the firmware package which contains only the changes between the old and new firmware version. This reduces the amount of data transmitted and speeds up the process.

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

The FW upgrade can be launched in foreground (synchronous upgrade) or in background (asynchronous upgrade) as specified by <command> parameter. The user can cancel the upgrade by sending cancel <command> value '2' any time before the device's reboot when using the background upgrade. After a crash (^EXIT URC), the module automatically restarts and triggers the SW upgrade.

When the image is not already on the device filesystem, 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 has been 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 it 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.amazonaws.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

Command	Response	Comment
	+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 Asynchronous Upgrade using HTTPS Protocol

Sets the URL of the firmware, reboots automatically after the firmware is installed, reports 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		
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

Command	Response	Comment
	+SQNSUPGRADE: “rebooting”	Device is rebooting and will enter updater mode to finish the upgrade
	+SQNSUPGRADE: “installed”	Device is upgraded to the new SW
	+SYSSTART	

4.2.4 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”	

4.2.5 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://ftpuser: 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	

4.2.6 Cancel Asynchronous Upgrade

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

4.2.7 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://ftpuser: 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	

4.2.8 Upgrade from Local File

Command	Response	Comment
The firmware image is first downloaded and stored on the device filesystem		
AT+SQNFGET="http://sequans.cloud/45700_to_45701_PACK.dup",1,"/fs/sqn/45700_to_45701_PACK.dup"		
	OK	The image is downloaded and stored in the device filesystem under "/fs/sqn/45700_to_45701_PACK.dup"
AT+SQNSUPGRADE="file:///fs/sqn/45700_to_45701_PACK.dup"		
	OK	
	+SQNSUPGRADE: "rebooting" +SQNSUPGRADE: "installed" +SYSSTART	

4.3 Error Handling

If an error (code:529) is received while the modem is trying to download the firmware files or to verify the downloaded firmware, 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 by this feature.

If an error (code:529) is received when the modem is trying to apply a 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 the FOTA upgrade, check that the modem attaches to the network before starting the FOTA upgrade. If the modem loses the network connection, it tries to reattach only ten times before giving up and sending `ERROR`.

The modem cannot be powered down during a firmware download. Doing so causes a failed download that has to be restarted from scratch later with a new FOTA upgrade command.

If the modem lost the network connection during the firmware download (error code:531), the download needs to 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 back, 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 filesystem and the PSI (Platform Specific information) are brought back to factory state. This means:

- All the parameters that were modified with the `AT+SQNHWCFG` command after the restoration point was created
- The entire filesystem including:
  - The low power settings
  - The operator mode and the bands to be scanned

Note: Device reboot is required to complete the operation. It can be triggered using `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 device's manufacturing using the command `AT+SQNFACTORYSAVE`. 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 partially resets 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 points and shall not be used.

5.2 Use Cases

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

5.3 Error Handling

When calling `AT+SQNSFACTORYRESET`, you may get an `ERROR`. The most likely reason is that there is no OEM restoration point.

Command	**Response**	**Comment**
AT+SQNSFACTORYRESET	ERROR	
AT+CFUN=5	OK	
AT+SQNFACTORYSAVE ="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 using various protocols (UDP, TCP, HTTP, TFTP, FTP, MQTT and COAP). RYZ024 modules contain a TLS stack to secure data sockets if needed.

A maximum of six sockets can be opened in parallel, with one session per socket. Sockets are opened by the RYZ024 module and not by the host MCU. UDP and TCP sockets can be opened 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 concludes with `CTRL+Z` to confirm the data to send or `ESC` to cancel.
- `AT+SQNSSENDEXT`: in that case, the host MCU defines the size of the payload to be sent and the modem escapes automatically once the defined number of bytes is reached.

In online mode, all data is treated as pure data and is transferred verbatim. In this mode, the UART is not able to send AT commands. The host MCU must use the escape sequence +++ to switch back to command mode. The socket remains open. The +++ escape pattern should comply with the requirements illustrated below. Other timing configuration will lead the sequence to be sent as raw data.

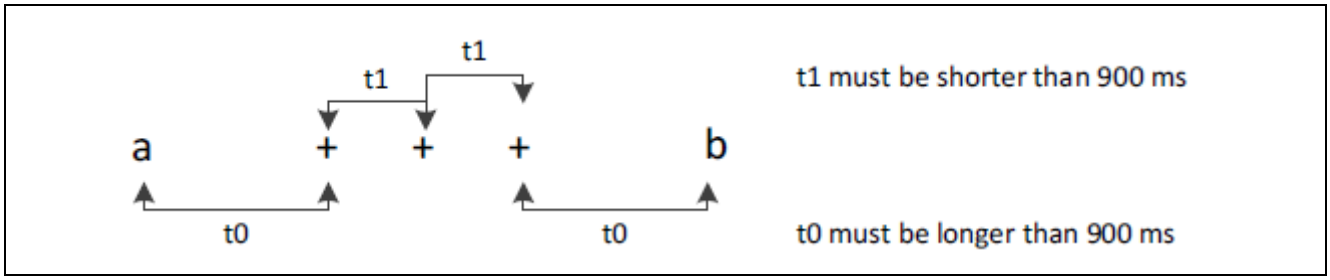

Figure 2. Escape Sequence from Online Mode to Command Mode

You can resume the socket mode at any moment (unless the socket inactivity timer times out) by using the `AT+SQNSO` command with the corresponding `<connId>`. Sockets support both text data and HEX data formats. The TCP/UDP listening port is supported in a 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: 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.

The RYZ024 SW has a TLS stack for secure socket connection. Certificates and private keys can be stored to the non-volatile memory using 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, and the user can proceed with another action. Progress and results are communicated using 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 continuing.

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 the data will be lost.

6.1 How to Send Data with UDP

6.1.1 Feature Description

The user can open a UDP socket and send the data either in online 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 the local IP address/port is accepted and a `+SQNSRING` URC is generated for the host MCU. Any other packet is dropped. It is possible to disable this filtering and accept incoming messages from different remote IP address/port (source IP address/port) with the `<acceptAnyRemote>` parameter in `AT+SQNSD` command.

Note: With the UDP protocol, there is no URC to inform the host MCU that a UDP packet was sent 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), AT+SQNSRECV must be used to receive the data. Otherwise, the data buffer remains full, and all following 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 the socket with default configuration
AT+SQNSCFGEXT=1,0,0,0	OK	Configure the extra socket parameters with default configuration
AT+SQNSD=1,1,4000,"192.168.13.1",0,4004,0		Configure the socket connection id 1 and open a socket connected to 192.168.13.1
	CONNECT	Connected to server
	Got again	Type the string to send
	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 the 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 the first socket.
AT+SQNSRECV=1,100		Receive up to 100 bytes from the first socket.
	+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 the socket with default configuration.
AT+SQNSCFGEXT=1,0,0,0	OK	Configure the extra socket parameters with default configuration.
AT+SQNSD=1,1,4000,”192.168.13.1”,0,4004,1	OK	Configure the socket connection id 1 and open a socket connected 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 the message size. Note: Maximum size is 1500.
	> Hello extend from client	
	+SQNSRING: 1	There is incoming connection on the first socket.
AT+SQNSRECV=1,100		Receive up to 100 bytes from the first socket.
	+SQNSRECV: 1,24 Hello extend from client OK	24 bytes are received.
AT+SQNSH=1	OK	Shutdown connection.

6.1.4 Accept Any Remote Option

The examples below show how to receive packets coming from any 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 remote than <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 by the modem when receiving the packet

Command	Response	Comment
AT+SQNSRECV=1,6	+SQNSRECV: 1,6,11111 OK	Read the buffered data
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 match the 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 to any other remote than <IPaddr>:<rPort> within the same socket family using +SQNSSEND command.
Run below 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_ERROR 4), please make sure first that the data to send is valid. If the data is confirmed valid, please check if you used 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 User's 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 using AT+SQNSCFGEXT. When the AT+SQNSCFGEXT parameter <srMode> is set to 2, the Unsolicited Response Code is +SQNSRING: <connId>,<recData>,<data>. Data can be read from the URC, but this does flush the bytes from the buffer. Not flushing the buffer with the AT+SQNSRECV command triggers an ERROR when the receive buffer becomes full, and all subsequent incoming data are lost. The received bytes are not flushed until explicitly read using the AT+SQNSRECV command.

Internal buffering is limited and +SQNSRING notification is suspended until the host starts reading the data with the AT+SQNSRECV command. The URC resumes when enough data has been read and data keep arriving.

6.2 How to Send Data with TCP

6.2.1 Feature Description

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

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 is not flushed, and all following data is lost.

The related AT commands are:

- AT+SQNSD
  - Use parameter <TxProt> 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 3.

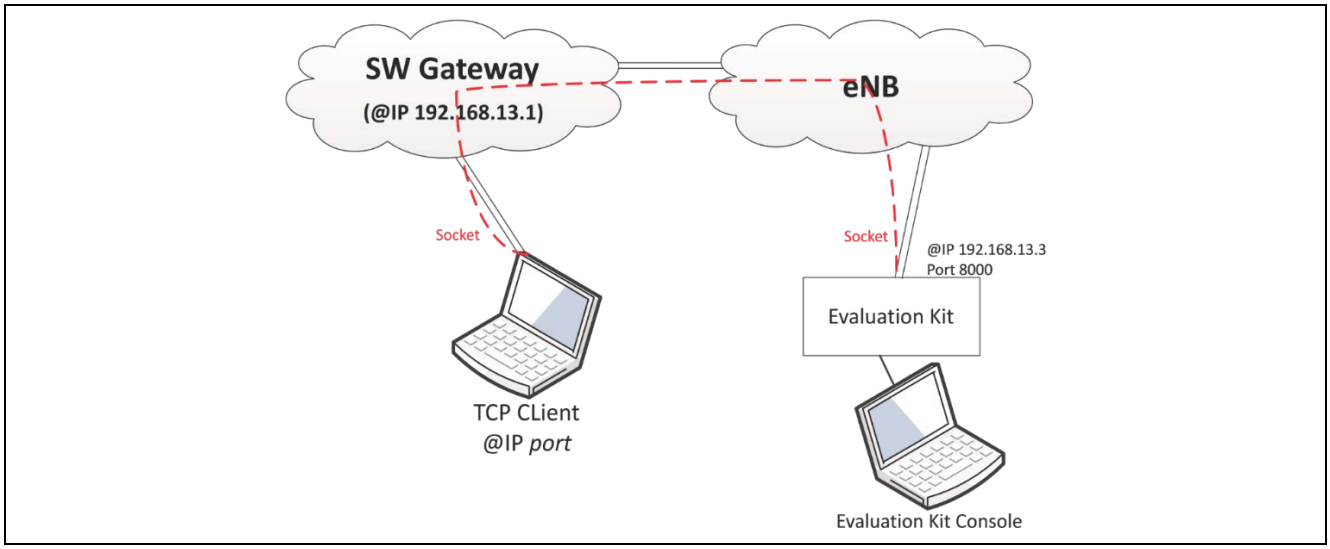

Figure 3. Typical TCP Setup

Note: In the following examples, 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 entered manually.

6.2.2 Use Cases in Online Mode

Command	Response	Comment
Ensure that UE is attached to LTE network. 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 `<commMode>` is 0 for online mode. `<TxProt>=0` for TCP.
	CONNECT	Intermediate result code if the 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.

Command	Response	Comment
	+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. No more than 1500 bytes can be received in one query.
	+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 it to 192.168.13.1
AT+SQNSSEND=1		
	> Hello extend from client	Send data in command mode using 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

Command	Response	Comment
maximum possible number 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	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 for the 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> indicates 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.
Should see message code on client 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 used 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 ERROR immediately as "\n" is an invalid HEX char

When sending data in text mode, the module does not return ERROR, but the server receive data that starts with "\n", and this may cause other problems.

The terminator char can be changed with ATS3 command, please refer to *AT Commands User's 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>. Data is part of the URC, but the corresponding bytes are not flushed from the buffer. Not flushing the buffer with the +SQNSRECV command triggers an ERROR when the receive buffer becomes full, and all subsequent incoming data is lost. Received bytes are not flushed until explicitly read by the +SQNSRECV command.

The internal buffering capability is limited and the +SQNSRING notification is suspended until the host starts reading new data using the AT+SQNSRECV command. The URC is sent again when enough data has been read and new data keep coming.

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 will be needed in that case:

- 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

The 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/VuZZMfsRnreeJm CjOO suKc=-----END CERTIFICATE-----		

Command	Response	Comment
	OK	
AT+SQNSNVW="privatekey",4,167 5	>	
-----BEGIN RSA PRIVATE KEY----- MIIEowIBAAKCAQEA5Y9oi8GwKg3FOx8ZnqLtWaUN3IAKRVgWO7/bmzkNN6HYJTxvp3v+4jGPkkLKiA+b (…) mT4lEcd4I5X00w82tdpIxobIH9UUBJlrZ2YLQ+nBAEy0zLYY532ZQwJXAI0rzejOanzMvwd+pXzwwPt -----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;0x35;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.		
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.us-east-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 a HTTP(S) Connection

6.4.1 Feature Description

RYZ024 modules embed an HTTP stack. The user can send data on HTTP(S) connections either in synchronous mode or asynchronous mode. HTTP(S) connections are 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)

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

The user can make an HTTPS connection with or without certificate validation. When you access a website using HTTPS, a certificate chain should be provided. Renesas' 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, AT command returns an 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 the query succeeds before the timeout, a URC is sent : the file is found and its length is 13011.		
	+SQNHTTPRING: 0,200,"text/html; charset=utf-8",13011	

Command	Response	Comment
AT+SQNHTTPRCV=1,0		RCV command to get it:
Then the file is dumped on the screen, with an “OK” status as 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 parameters and press CTRL+Z to conclude.		
foo=bar		
	OK	In case of success, 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 Notes on <post-param> and <extra-header-line> Parameters

In `AT+SQNHTTPSND`, the parameter `<post_param>` is optional. Only `POST` requests use it and it is related to `<Content-Type>` in the HTTP header. In the example above, the ‘0’ default value is used. HTTP packets include, in the header `Content-Type: application/x-www-form-urlencoded.` You might want to define `charset` to `text/plain`, or `boundary` to `multipart/form-data`. In these cases, you need the following extension

- Set charset to `us-ascii`:
  - Set `<post_param>` to “`1:charset=us-ascii`”. The request then contains the “`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 the “`Content-Type: multipart/form-data; boundary=—-WebKitFormBoundaryv9K2Q6NJOnI5kAZX`” header line.:

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

In the example above, the data length is 336. After the ">" prompt, enter 336 bytes with the boundary string as a separator.

Both `AT+SQNHTTPSND` and `AT+SQNHTTPQRY` commands support the optional parameter `<extra_header_line>`. It allows an additional HTTP header line to be included. The `'@'` character is used to identify the header line ending. If you want to include a '@' char in a header, double it. 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@"
```

6.4.2.4 Test with Certificate Validation

To retrieve the right SSL certificate from a secured portal, enter a portal URL with https on your browser:

1. Click on the lock button and then on **Connection is secure.**

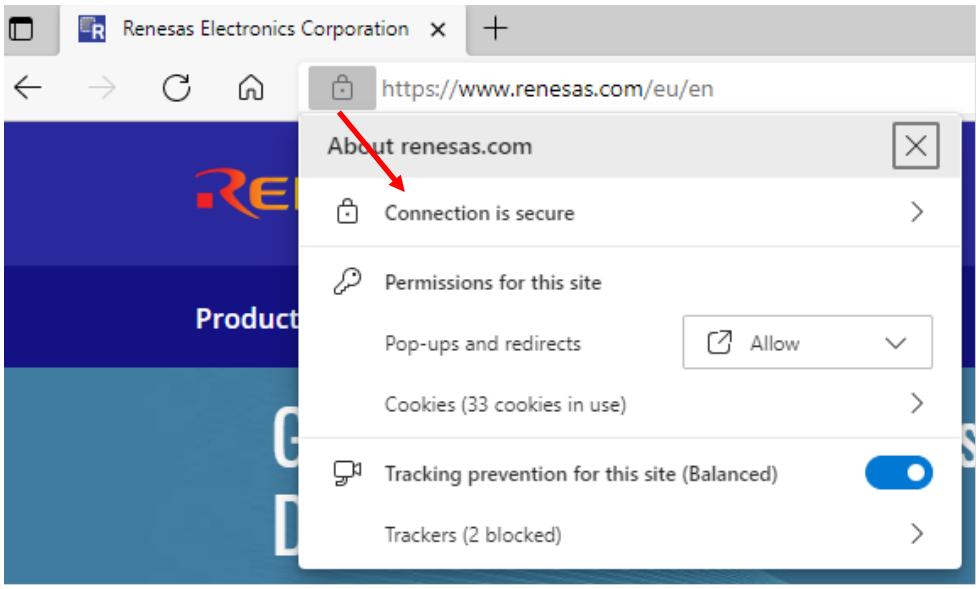

Figure 4. Connection is Secure

2. Then click on the certificate button to show the certificate.

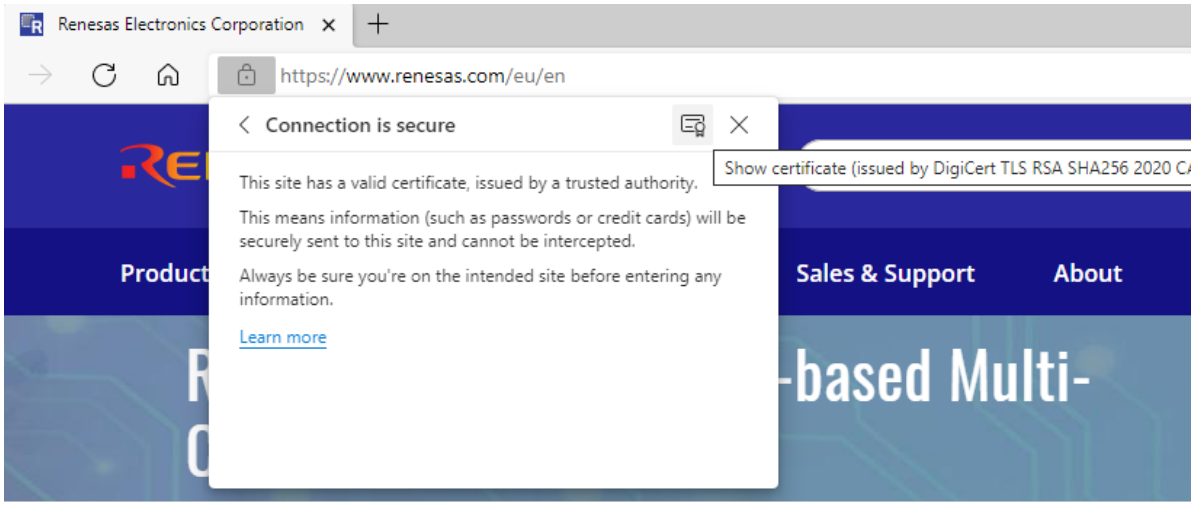

Figure 5. Show Certificate

3. It opens the following pop-up window. Click on the **Certification Path** tab to see the certificate chain and double-click on the parent certificate. Then click on **View Certificate.**

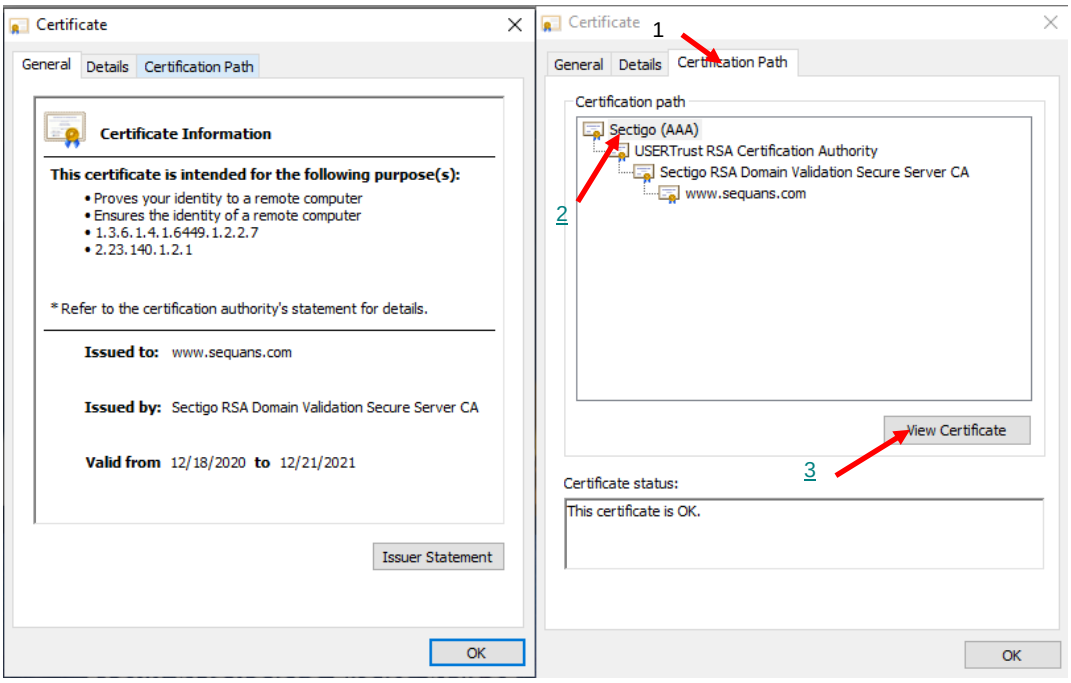

Figure 6. View Certificate

4. On the new pop-up window, click on **Details**, **Copy to File**. The certificate export wizard will open. Click on **Next**, select **Base-64 encoded** certificate and click on **Next.**

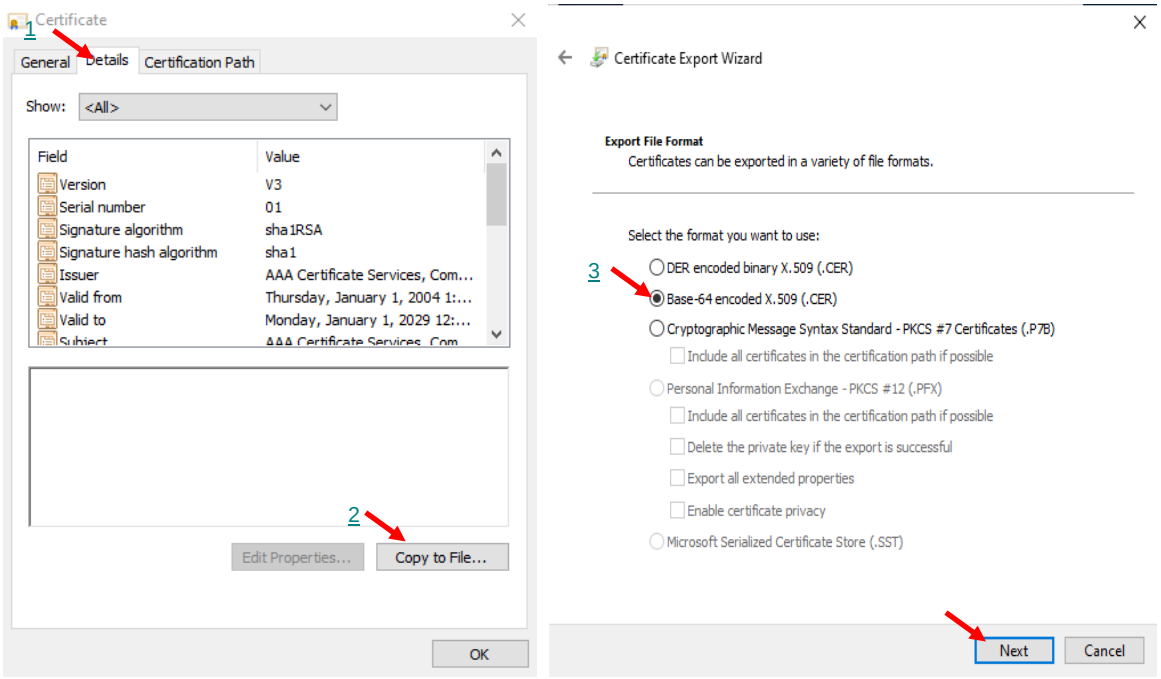

Figure 7. Download Certificate to File

5. Choose the directory in which the certificate needs to be saved and click **Save**. Click **Finish** and the message **The Export was successful** appears. Click **OK.**

Command	**Response**	**Comment**
Type below command to set certificate:		
AT+SQNSNVW="certificate",19,1696		
	>	You see a prompt
As example, copy the Wikipedia certificate on the UART interface, and press <enter> at the end		
-----BEGIN CERTIFICATE----- MIIEtjCCA56gAwIBAgIQDHmpRLCMEZUgkmFf4msdgzANBgkqhkiG9w0BAQsFADBs MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3 (...) c63YlC3k8wyd7sFOYn4XwHGeLN7x+RAoGTMCAwEAAaOCAUkwggFFMBIGA1UdEwEB/wQIMAYB Af8CAQAwDgYDVR0PAQH/BAQDAgGGMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEF BQcDAjA0BggrBgEFBQcBAQQoMCYwJoVWNWlZopCJwqjyBcdmdqEU79OX2olHdx3ti6G8MdOu42vi/hw 15 UJGQmxg7kVkn8TUoE6smftX3eg== -----END CERTIFICATE-----		
	OK	You would see OK if succeed to write the certificate into device filesystem
If there is already a certificate with index 19, remove it from the device's filesystem as described in section 3.2.4		
Configure SSL/TLS security profile 1 (certificate validation level: 7, certificate id: 1):		
AT+SQNSPCFG=1,2,"",7,19		
	+SQNSPCFG: 1,2,"",5,19,,,"" OK	
Configure http profile 0 (cid: 1, security profile: 1):		
AT+SQNHTTPCFG=0,"github.com",443,0,"","",1,120,1,1		
	OK	
AT+SQNHTTPQRY=0,0,"/"	OK	Send a HTTP “Get” query on profile 0:
If the Get query succeeds, an URC is sent later:		
	+SQNHTTPRING: 0,200,"text/html; charset=utf-8",0	
AT+SQNHTTPRCV=0,0		Read the body of http response:
A prompt ”<<<” is sent, followed by the whole data, then a final OK.		
	<<< ... OK	Note that +SQNHTTPRCV returns error when there is no body (only a header) in the data received.

6.4.2.5 Test with no Certificate in Filesystem

The following test is the same as the previous test with certificate validation.

Command	Response	Comment
Remove certificate from device filesystem.		
AT+SQNSNVW="certificate",1,0	OK	The third parameter 0 means removing the appointed certificate.
AT+SQNHTTPQRY=0,0,"/"	OK	Send a HTTP “Get” query on profile 0:
Result status, and URC which indicates no HTTP response:		
	+SQNHTTPRING: 0,0,"",0	
Configure SSL/TLS security profile 1 with no certificate validation:		
AT+SQNSPCFG=1,2,"",0		
	+SQNSPCFG: 1,2,"",0,,,,"" OK	
AT+SQNHTTPQRY=0,0,"/"	OK	Send a HTTP “Get” query on profile 0:
If the result status is OK, an URC will be received:		
	+SQNHTTPRING: 0,200,"text/html",74711	
AT+SQNHTTPRCV=0,0		Read the body of the HTTP response:
	<<< ... OK	Note that +SQNHTTPRCV returns error when there is no body (only a header) in the data received.

6.4.3 Use Case with +SQNFGET Command

Command	Response	Comment
AT+SQNFGET="http:/192.168.13.1/index.html"		By default, use synchronous downloading. In case the `<local_filename>` parameter is not specified; this AT command switches the AT channel to data mode and outputs the downloaded binary octet stream to the host. In this scenario, the host is responsible for error handling.

Command	Response	Comment
	<!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 the server. When an answer from the HTTP server is received, the +SQNHTTPRING URC is sent with information.

The fifth parameter, <post_param>, differs from the +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 ignores the fourth parameter <filename>. Instead, some event logs will be sent to the server. The use of this parameter is limited to specific use cases. In general, please specify the <filename> value and avoid using <post_param>.

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 on the device's filesystem to the server. Use HTTP commands to upload files from the host MCU's filesystem.
	+SQNHTTPRING: 0,200,"application/json",77 OK	Response OK with status 200

6.4.5 Use Case in Asynchronous Mode with +SQNHTTP Command

Command	Response	Comment
Configure an HTTP profile (no SSL)		
AT+SQNHTTPCFG=0,"httpbin.org",80,0,"","",0,120,1,1,0		
	OK	
AT+SQNHTTPCFG?		
	SQNHTTPCFG: 0,"httpbin.org",80,0,"","",0,120,1,1,0 +SQNHTTPCFG: 1,"ec2-3-134-42-3.us-east-2.compute.amazonaws.com",80,0,"","",0,120,1,1,0 +SQNHTTPCFG: 2,"",80,0,"","",0,120,1,1,0 OK	
AT+SQNHTTPCFG=1,"ec2-3-134-42-3.us-east-2.compute.amazonaws.com",80,0,"","",0,120,1		
	OK	
AT+SQNHTTPCONNECT=0		
	OK +SQNHTTPCONNECT: 0,0	
AT+SQNHTTPCONNECT=1		
	OK +SQNHTTPCONNECT: 1,0	
Query a test file (HTTP connection remaining open) and read the body of the HTTP response		
AT+SQNHTTPQRY=0,0,"/",,0		
	OK +SQNHTTPRING: 0,200,"text/html;charset=utf-8",9593	
AT+SQNHTTPRCV=0,0		
	<<<<!DOCTYPE html> <html lang="en">> ... OK	
Performs a HTTP POST request to the server		
AT+SQNHTTPSND=1,0,"/cgi-bin/handler.php?/test.txt",10		

Command	Response	Comment
	> AAAAAAAAAA OK +SQNHTTPRING: 1,200,"text/html; charset=UTF-8",0	
Performs a HTTP POST request with file content to server		
AT+SQNFPUT=1,0,"/cgi-bin/handler.php?/rde/100K.txt","/fs/100K.txt","application/octet-stream"		
	OK +SQNHTTPRING: 1,200,"text/html; charset=UTF-8",0	
HTTP connection close		
AT+SQNHTTPDISCONNECT=0		
	OK +SQNHTTPDISCONNECT: 0	
AT+SQNHTTPDISCONNECT=1		
	OK +SQNHTTPDISCONNECT: 1	

6.4.6 Error Handling

`AT+SQNHTTPSND` is a synchronous command. The modem does not accept any other AT commands or send any URC while the command is being performed. Completion time depends on the network conditions. Under a poor RF environment, the command can be slow. The user can define a timeout for this command using `AT+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 the 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 `ERROR` immediately as "`\n`" is an invalid HEX char

When sending data in text mode, the module does not return `ERROR`, but the server receive data that start with "`\n`", and this may cause other problems.

The terminator char can be changed with `ATS3` command, please refer to *AT Commands User's 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 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 connections in two different modes: asynchronous and synchronous. The related AT commands 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+SQNFGET="tftp://192.168.13.1/test.txt",0		Start downloading by TFTP
	OK	
	+SQNFGETREPORT: "started" +SQNFGETRING: 114 +SQNFGETREPORT: "downloading"	Receive the “download status” URC and the “download size” URC:
AT+SQNFGETDATA		Read the received data
The data is dumped, followed by a result status.		
	[Data] OK	
When all the data are received, the download status URC indicates 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 an FTP(S) connection in two different modes, asynchronous mode and synchronous mode. The AT commands for FTP(S) 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 the `AT+SQNFGET` command is used as the name of the file to store the data into, for example, `/fs/local_filename`. If the `<local_filename>` parameter is not provided, then the received data is placed in an internal FIFO, waiting to be read using the `AT+SQNFGETDATA` command.

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 to the device’s file system.		
AT+SQNFGET="ftp://192.168.10.1/testfile",1,"mylocalfile"		
	OK	
The possible status are ‘started’, ‘downloading’, ‘error’, ‘complete’ and ‘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 to 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 held in an internal buffer
	OK	
	+SQNFGETREPORT: "started" +SQNFGETRING: 200 +SQNFGETREPORT: "downloading" +SQNFGETREPORT: "complete"	Data can only be read with `AT+SQNFGETDATA` once the `+SQNFGETRING` URC is received, sending `AT+SQNFGETDATA` before receiving the URC ends up in ERROR
AT+SQNFGETDATA		Read the internal buffer, the default parameter is 0, which dumps all contents
	[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 an 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`

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

6.7.1.2 MQTT and TLS

MQTT is built over TCP, which means that, by default, the connection does not use an encrypted communication. To encrypt the MQTT transaction, most MQTT brokers allow TLS in addition to the standard username/password authentication.

Although it is enough for the server to use a private/public key pair to establish a secure connection, some clients possess their own public/private key pairs 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 has been validated. The server verifies the identity of the client and aborts the handshake if the verification of the client certificate fails. This allows for 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 use this paradigm.

The command `AT+SQNSNVW` uploads the certificates on the device. The command `AT+SQNSPCFG` sets the security profile parameters required to configure the SSL/TLS connections properties.

6.7.2 MQTT Server

The AWS IoT platform, Cloud IoT Core, Microsoft Azure, or any other MQTT server can be used for tests and usage. `Mosquitto` https://test.mosquitto.org/ is another possibility.

6.7.2.1 Mosquitto

Mosquitto is an MQTT open-source test server: https://test.mosquitto.org/. This server can run locally. To test the MQTTS connection, `openssl` is used to generate certificate and keys.

6.7.2.2 AWS IoT

Please refer to Sequans ’video available on the Sequans’s YouTube channel: https://www.youtube.com/watch?v=81hMqN7z4oE

AWS IoT provides a secure, bidirectional communication link 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 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) and a registration at https://aws.amazon.com/iot/. For detailed information about AWS IOT, please refer to http://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html.

You then need to create an AWS IOT Thing for your device as follows. Log into your AWS IOT console and register your device in the AWS IOT registry. AWS IOT provides 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’s 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 opted for, the 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 you don't have any specific needs, you can choose the RSA 2048 bit key: Amazon Root CA 1.

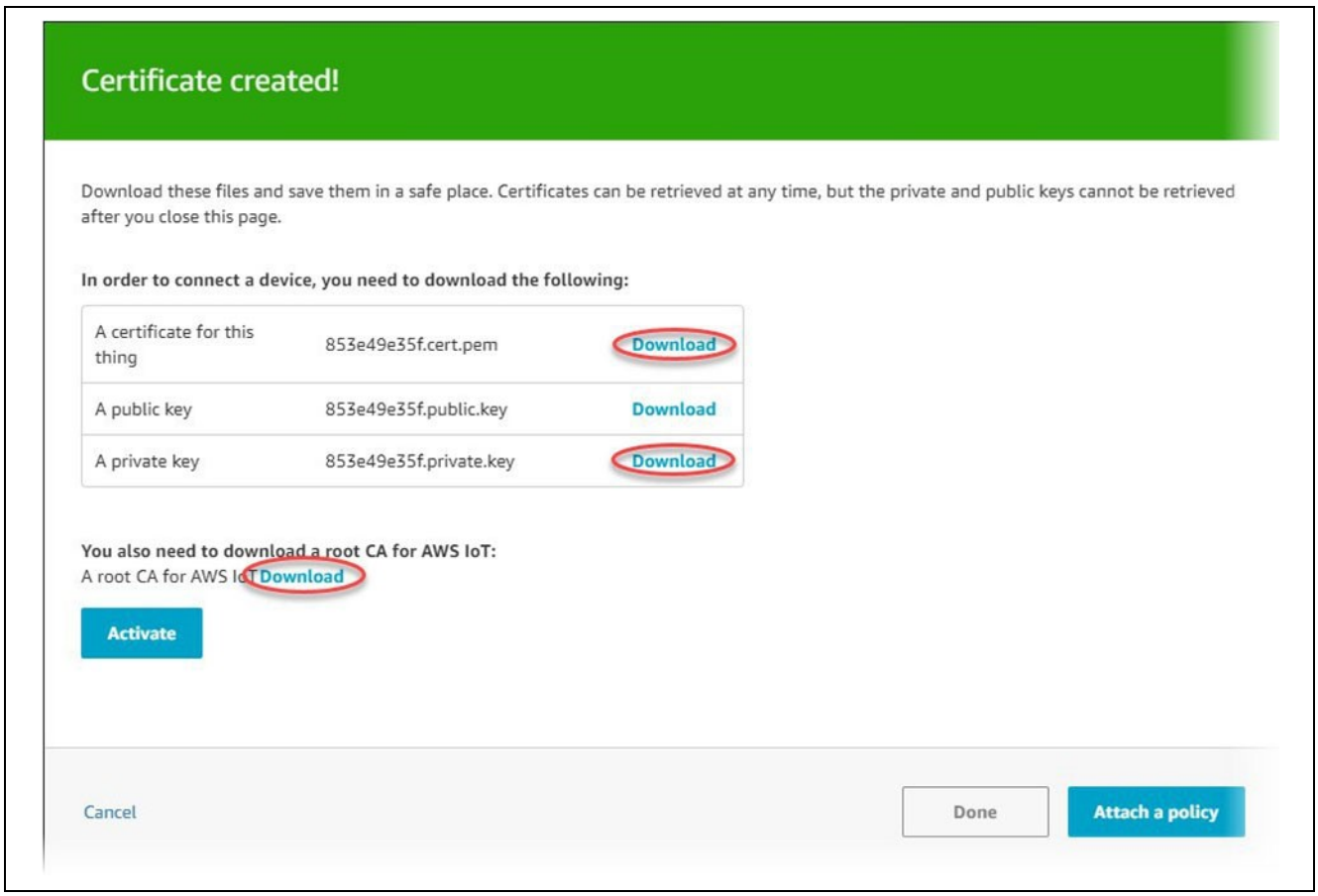

Figure 8. Creating a Certificate

Once this is done, the two certificates and the private key need being uploaded into your device using the `AT+SQNSNVW` commands. Then, a security profile must be set (with `AT+SQNSPCFG`) using these two certificates and private key.

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 used 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 for the `AT+SQNSMQTTCONNECT` command is called 'endpoint' by AWS.
- The URL to be used is retrieved from '**WS IOT → manage → Things → Select the thing you created → Interact**. Then select the URL corresponding to **Update your Thing Shadow using this Rest API Endpoint**.
- The format of the end point parameter is '`identifier`.iot.`region`.amazonaws.com'.

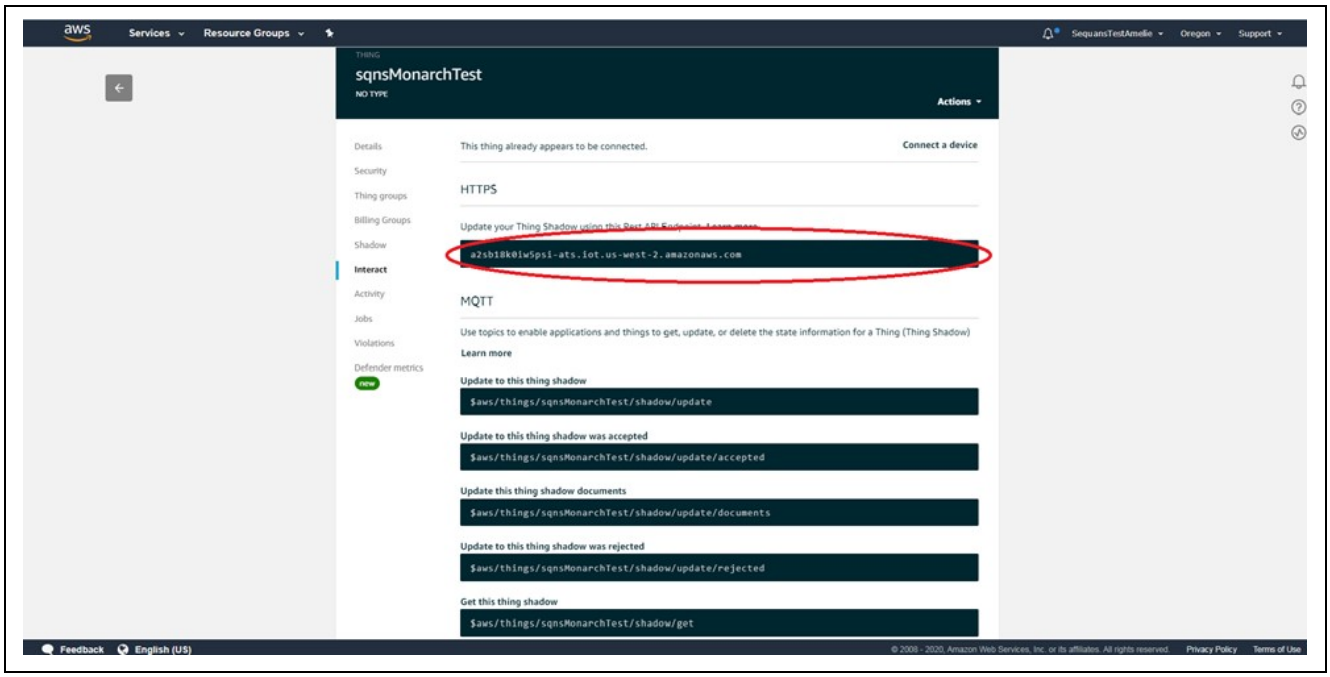

Figure 9. End-Point Parameter Format

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 provide to `AT+SQNSMQTTPUBLISH` is the one you want (for example `myTopic`)

6.7.2.3 Cloud IoT Core

Please refer to Sequans's video available on Sequans's *YouTube*™ channel: https://www.youtube.com/watch?v=f9xDOXB1gg4

Cloud IoT Core is a fully managed service that allows you to connect, handle, and process data from millions of globally dispersed devices easily and securely. You can get an overview of this cloud service 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 UNIX/Linux type OS) needed to authenticate your device on the cloud. On *Windows*™, you can use *PUTTYgen*. 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 at https://cloud.google.com/iot/docs/how-tos/mqtt-bridge#downloading_mqtt_server_certificates. To start, you should choose the complete Google root CA certification package (https://pki.goog/roots.pem) and upload it in the module with the `AT+SQNSNVW` command.

Then, set a security profile (with `AT+SQNSPCFG`) using the certificate and the private key just uploaded. Please refer to section 0 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 like this:

`projects/`*`project_id`*`/locations/`*`region`*`/registries/`*`registry_id`*`/devices/`*`device_id` –* where `project_id` is the name you chose for your project (`MyFirstProject` for example)

- `region` is the region selected when the registry was created (`europe-west1` for example)
- `registry_id` is the name chosen when the registry was created (`myRegistry` for example)
- `device_id` is the name chosen when the device was created (`myDevice` for example)

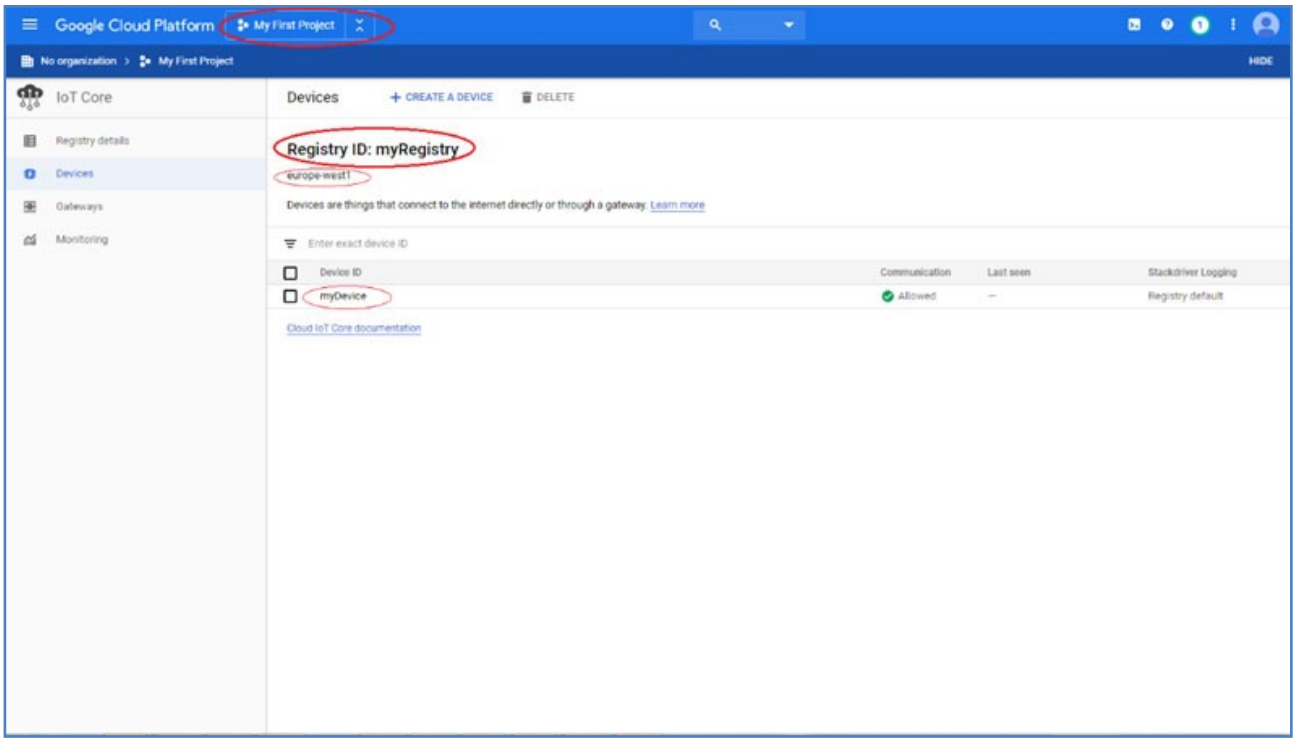

Figure 10. Registry ID

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 `AT+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 a new connection with client id 0 to the test Mosquitto broker using the 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 the test Mosquitto broker previously connected.		
AT+SQNSMQTTSUBSCRIBE=0,"sqn/ test",1	OK	
	+SQNSMQTTONSUBSCRIBE:0,"sqn/test",0	Notification that subscribing operation is finished.

Command	Response	Comment
Publish a payload into a topic on a test Mosquitto broker. The command displays a ‘>’ 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"}		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 <qos>=0 +SQNSMQTTONMESSAGE URC.		
	+SQNSMQTTONMESSAGE :0,"sqn/test",32,1,1	Notification about a newly received message which was stored into the internal message cache for client 0
AT+SQNSMQTTRCVMESSA GE=0,"sqn/test",1	{"msg": "hello from IoT device"} OK	Collect the message
AT+SQNSMQTTDISCONNE CT=0	OK	Disconnect from the test Mosquitto broker.
	+SQNSMQTTONDISCONNECT :0,0	Notification about the end of MQTT connection for client 0.

6.7.3.2 Encrypted

Command	Response	Comment
Upload the test Mosquitto broker certificate into file system, certificate index 0. Note: If there is a certificate with index 0 already, remove it using the same command with a length set to 0: AT+SQNSNVW=“certificate”,0,0 OK		
AT+SQNSNVW="certificate",0,1 326		
	>(copy the certificate here)	After the prompt '>', copy the certificate into the UART tool. If the length matches the one given in the command, the command ends automatically. If the last “\n” is not copied, you need to type <*Enter*> to end it. This configuration allows the UE to check the server’s 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. It is recommended to keep the list to a bare minimum to avoid ‘man in the middle’ attacks. 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 a new connection with client id 0 to test the Mosquitto broker using the 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	The URC notifies that connection operation has finished.
Subscribe to a topic “sqn/test” on test Mosquitto broker previously contacted with the SQNSMQTTCONNECT command.		
AT+SQNSMQTTSUBSCRIBE=0,"sqn/test",1	OK	
	+SQNSMQTTONSUBSCRIBE:0,"sqn/test",0	The URC notifies that subscribing operation is finished.
Publish a payload in a topic on a test Mosquitto broker. The command displays the prompt ‘>’ and waits for the data to send. The data is provided as a 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.

Command	Response	Comment
	+SQNSMQTTPUBLISH:0,2,0	The URC notifies that publishing operation is finished for client 0.
Receive a message by client id 0 or last received message in case <*qos*>=0 +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.
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. In order to comply, the client must have its own certificate (including public key) and a private key to upload using `AT+SQNSNVW`. You can configure a secure profile with `AT+SQNSPCFG`, and then use its index for an 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",0,1326	>	
	OK	After the prompt '>', copy the certificate into the UART tool. If the length matches that in the command, the command ends automatically. If the last “\n” is not copied, you need to type `<Enter>` to end it. This configuration allows the UE to verify the server connection.
AT+SQNSNVW="certificate",1,1545	>	(copy the certificate here)
	OK	
AT+SQNSNVW="privatekey",0,1675	>	(copy client private key here)
	OK	

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. It is recommended to keep the list to a bare minimum to avoid ‘man in the middle’ 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 sends everything at the certificate/private key 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 TLS 1.3. If the list of supported cipher suites does not include that you need to set to connect to the MQTT server, you should leave the third 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.		
AT+SQNSMQTTCFG=0,"sqn/gm01 q",,,2	OK	Please refer to section 6.8.2.2 and 6.8.2.3 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 6.8.2.2 and 6.8.2.3 to get the domain names to be used for AWS and IoT Core. <port> 8883 is for test with MQTT encrypted
	+SQNSMQTTONCONNECT:0,0	The URC notifies that connection operation is done.
Subscribe to a topic “sqn/test” on test Mosquitto broker previously connected with `SQNSMQTTCONNECT` command.		
AT+SQNSMQTTSUBSCRIBE=0,"sqn/test",1	OK	
	+SQNSMQTTONSUBSCRIBE:0,"sqn/test",0	The URC notifies that subscribing operation is done.
Publish a payload in a topic on a test Mosquitto broker. The command displays the prompt ‘>’ and waits for the data to send, which is provided as length-defined multi-line. 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.

Command	Response	Comment
	+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 the end of the MQTT connection for client 0.

6.7.4 Error Handling

You must wait for the `+SQNSMQTTONCONNECT:0,0` URC after sending the `AT+SQNSMQTTCONNECT` command. It means that the connection was successfully established. 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 double check the certificates that you are using and the cloud settings.

6.8 How to Use CoAP(S) Commands

The RYZ024-based module embeds a CoAP client and supports AT commands to connect to a remote server. Application servers usually allow using CoAP to send telemetry data. CoAP has the advantage of being UDP based so has lower overhead than MQTT or HTTP.

The following example details a basic GET test with an open CoAP server (`libcoap`). The connection will be made using DTLS.

6.8.1 Setup Preparation

Setup and install `libcoap` server on a Linux machine as follow.

Install `libcoap` as follows:

```
$ git clone https://github.com/obgm/libcoap.git --recursive
$ cd libcoap
$ ./autogen.sh
$ ./configure --with-openssl --disable-shared
--disable-documentation
$ make
$ sudo make install
```

Generate certificates/keys. This can be done with a script `generate-CA.sh`

```
$ cd ~
$ mkdir myCA
$ cd myCA
$ wget https://github.com/owntracks/tools/raw/master/TLS/generate-CA.sh .
$ chmod +x generate-CA.sh
# Then generate CA certificate, server certificate and private key.
$ ./generate-CA.sh server
$ ls
ca.crt  ca.key  ca.srl  generate-CA.sh  server.crt  server.csr  server.key
```

You will get the following generated files:

```
ca.crt: CA certificate
server.crt: server certificate
server.key: server private key
```

Generate client certificate and private key.

```
$ ./generate-CA.sh client client1@sample.com In the output, you will get:
client1@sample.com.crt: client certificate • client1@sample.com.key: client
private key
```

Run the server, check the usage in detail with `$ coap-server --help`.

```
$ coap-server -c ~/myCA/server.crt -j ~/myCA/server.key -C ~/myCA/ca.crt
```

6.8.2 Use Case

In the following example, we assume that the modem has already attached to the network. Note that we use an IP address for the CoAP server. If you are using a URL, make sure to remove the (/) character to be compliant with the CoAP standard.

Command	Response	Comment
Write CA certificate (idx=7), client certificate (idx=8) and client private key (idx=9) into the RYZ024 module.		
AT+SQNSNVW="certificate",7,1330	-----END CERTIFICATE----- JgpRRhKotIsz8hC3ry54ceXDyJO4F6Rv2gOzimS OK	The third parameter length derives from the size of the files generated in the last step of section 6.9.1 above.
AT+SQNSNVW="certificate",8,1558	-----END CERTIFICATE----- JKes0f1U6nnwPrqATu+Q7yRh6DmK9C4hCwMr 76i OK	
AT+SQNSNVW="privatekey",9,1679	-----END RSA PRIVATE KEY----- 109oOsW0VkGD7slmXJxEkfedg== mBuYnDWu OK	
Configure the security profile: 1: ID; 2: TLS v1.2; "": cipherSpecs, keep empty to negotiate with server; 0: certValidLevel, set 0 here; 7: index of CA certificate ; 8: index of client certificate ; 9: index of client private key		
AT++SQNSPCFG=1,2,"",0,7,8,9	+SQNSPCFG: 1,2,"",0,7,8,9,"","",0 OK	

Command	Response	Comment
AT+SQNCOAPCREATE=0,"172.16.72.9",5684,,1,10,1,1	OK	0: prof id ; "172.16.72.9": Server ip address. (Domain name accepted) ; 5684: server port ; 1: dtls enabled ; 10: The time interval in seconds to wait for receiving response from CoAP server when sending a request before aborting the operation 1: cid ; 1: security profile ID
	+SQNCOAPCONNECTED: 0,"172.16.72.9",5684,0,1	After sending COAP Create AT, wait for this URC.
AT+SQNCOAPSEND=0,0,1,1		Wait for ">" before entering any data.
	> \ OK	
	+SQNCOAPRING: 0,43630,1,2,205,136	The second parameter of the URC is the *message_id.* Use this id to read the message.
AT+SQNCOAPRCV=0,43630	+SQNCOAPRCV: 0,43630,,1,2,205,136 This is a test server made with libcoap (see https://libcoap.net) Copyright (C) 2010--2021 Olaf Bergmann <bergmann@tzi.org> and others OK	
AT+SQNCOAPCLOSE=0	+SQNCOAPCLOSED: 0,"USER" OK	

7. SMS

The SMS service transfers short messages between UEs via an SMS service center. The SMS service center provides an interworking and relaying function to the UEs.

The supported transport layer for RYZ024 is SMS over NAS, also called SMS over SG, with 3GPP format. 3GPP2 format is not supported with SMS over NAS. It complies with 3GPP specification 27.005. There are two supported modes to send SMS:

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

SMS format can be selected with the `AT+CMGF` command. By default, the SMS format is set to PDU mode. It is possible to activate notifications (URC) on new SMS reception with `AT+CNMI`.

shows the SMS network architecture.

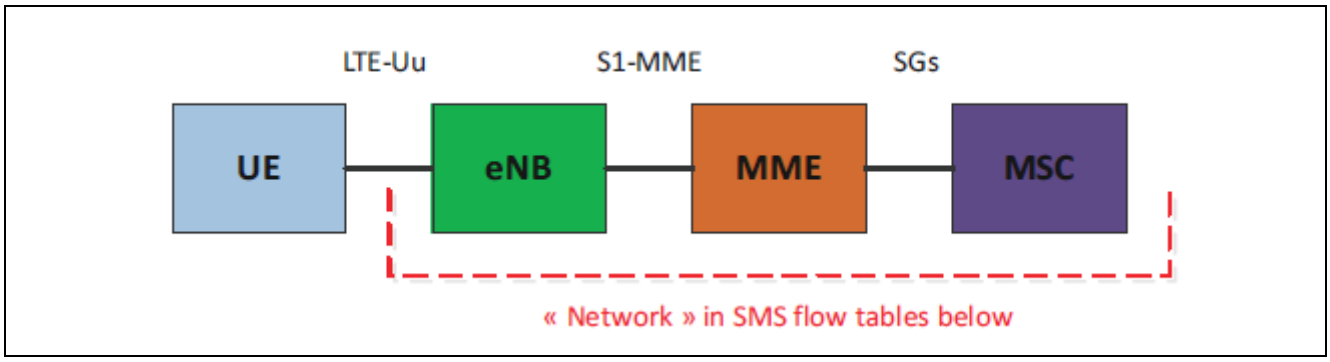

Figure 11. SMS Network Architecture

The following table shows the call flow for a mobile-originated SMS call.

#	**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)	→	

SMS service activation depends on the SIM card. Contact your SIM provider to know if the SMS service is enabled or not.

The table below shows the call flow for a mobile-terminated SMS call.

#	**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, with standard or Asian characters.

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

Renesas also have a set of private AT commands that can be used to send and receive SMS in text mode:

- `AT+SQNSMSSEND`
- `AT+SQNSMSREAD`
- `AT+SQNSMSMLSEND`
- `AT+SQNSMSLIST`
- `AT+SQNSMSDELETE`
- `AT+SQNSMSCOUNT`

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	
It is also possible to read a SMS with the SQNSMSREAD command		
AT+SQNSMSREAD=0	+SQNSMSREAD:1,"STO UNSENT", "UNUSED", "+11484848484", "00/00/00,00:00:00+00", "00/00/00,00:00:00+00", 0, "" 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 the UE to work under SMS text mode		
AT+CMGF=1	OK	
Query the SMS service centre address to confirm it is already correctly configured.		
AT+CSCA?	+CSCA: "+886932400851",145 OK	
Configure SMS service centre address in case it is not correctly configured. Note: Contact your service provider to get the SMS service centre address.		
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 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 the UE to work under SMS text mode		
AT+CMGF=1	OK	
Query the SMS service centre address to confirm it is already correctly configured.		
AT+CSCA?	+CSCA: "+886932400851",145 OK	
Configure SMS service centre address in case it is not correctly configured.		

Command	Response	Comment
Note: Contact your service provider to get the SMS service centre address.		
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	
SMS can also be sent using SQNS proprietary AT commands		
AT+SQNSMSSEND="+886932123456","Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum."		
	+SQNSMSSEND: ID,0 +SQNSMSSEND: ID,1 +SQNSMSSEND: ID,2 +SQNSMSSEND: ID,3 … OK	The text is very long, the auto-segmentation feature splits it into several SMS
	+SQNSMSSEND: SENT OK,0,127 +SQNSMSSEND: ACK OK,0 +SQNSMSSEND: SENT OK,1,128 +SQNSMSSEND: ACK OK,1 +SQNSMSSEND: SENT OK,2,129 +SQNSMSSEND: ACK OK,2 +SQNSMSSEND: SENT OK,3,130 +SQNSMSSEND: ACK OK,3	Two URCs are generated for each SMS: - one with the sending attempt status - and one with the network response
AT+SQNSMSMLSEND= "+886932123456"	> Hello, >how are you?	Enter <CTRL+Z> when finished
	+SQNSMSMLSEND: ID,89 OK	
	+SQNSMSSEND: SENT OK,89,151 +SQNSMSSEND: ACK OK,89	Two URCs are generated, on with the sending attempt status and one with the network response

7.1.2.4 Send a 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.		
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 can send binary information in 7 bit or 8-bit format. This is useful 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 can 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=3707918405210077F70414D1ECB6FB0D8FCBE7F4BA1D00 0090103180949240106136 1C1D76D7DB65797A0C9A36A <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

On a RYZ024-based device, the SMS can be stored:

- On the SIM card
- On the modem or device itself

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

- Select which storage area is 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 out of 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
Self-send the message ”aaaa” (to number +11000000151, assumed to be one’s own number)		
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
AT+CPMS="ME","ME","SM"	+CPMS: 1,10,1,10,0,20 OK	Configure storage area to SIM
AT+CMGS="+11000000151"	> bbbb <CTRL-Z>	Self-send two more messages
	+CMGS: 4 OK	
	+CMTI: "SM",1	
AT+CPMS?	+CPMS: "ME",1,10,"ME",1,10,"SM",1,20 OK	

Command	Response	Comment
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 messages. The first message saved in ME is displayed		
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	

Command	Response	Comment
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" CommunicationsCommunicationsCommunications	
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 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 sometimes split the message in 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 to avoid any potential overflow that could lead to a loss of messages (text or PDU-mode).

8. Low Power with eDRX and PSM

8.1 How to Use eDRX Feature

8.1.1 Feature Description

eDRX (extended Discontinuous Reception) in RRC Idle State provides two enhancements, compare to "regular" DRX:

- The DRX cycle is extended up to and beyond 10.24 s in idle mode, with a maximum value of 2621.44 s. (43.69 minutes). For NB-IoT, the maximum value of the DRX cycle is 10485.76 s. (2.91 hours).
- The UE monitors paging for the duration of the Paging Time Window within an eDRX Cycle.

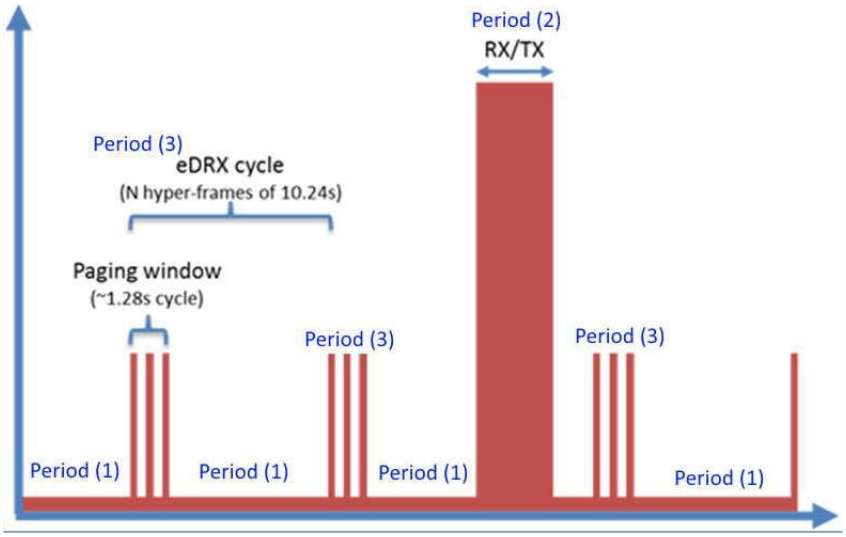

Figure 12. eDRX Paging Window

The related AT commands are:

- `AT+CEDRXS`
- `AT+SQNEDRX`
- URC `+CEDRXP`

Note: RYZ024 modules support both the legacy 3GPP command (`AT+CEDRXS`) and a Renesas's proprietary AT command (`AT+SQNEDRX`) to configure eDRX. It is recommended to use `AT+SQNEDRX` as it provides more options such as the possibility to change the value of the paging time window (PTW).

The following table presents the mapping between the bits and eDRX cycle and PTW value, as retrieved from *3GPP specification 24.008 v14.07.00 §10.5.5.32*.

Bit				E-UTRAN eDRX cycle length duration	WB-S1 PTW Value	NB-S1 PTW Value
3	**2**	**1**	**0**			
0	0	0	0	5.12 seconds (see note [1])	1.28 seconds	2.56 seconds
0	0	0	1	10.24 seconds (See note [1])	2.56 seconds	5.12 seconds
0	0	1	0	20.48 seconds	3.84 seconds	7.68 seconds
0	0	1	1	40.96 seconds	5.12 seconds	10.24 seconds
0	1	0	0	61.44 seconds (see note [2])	6.4 seconds	12.8 seconds
0	1	0	1	81.92 seconds	7.68 seconds	15.36 seconds
0	1	1	0	102.4 seconds (see note [2])	8.96 seconds	17.92 seconds
0	1	1	1	122.88 seconds (see note 2)	10.24 seconds	20.48 seconds
1	0	0	0	143.36 seconds (see note 2)	11.52 seconds	23.04 seconds
1	0	0	1	163.84 seconds	12.8 seconds	25.6 seconds
1	0	1	0	327.68 seconds	14.08 seconds	28.16 seconds
1	0	1	1	655.36 seconds	15.36 seconds	30.72 seconds
1	1	0	0	1310.72 seconds	16.64 seconds	33.28 seconds
1	1	0	1	2621.44 seconds	17.92 seconds	35.84 seconds
1	1	1	0	5242.88 seconds (see note 3)	19.20 seconds	38.4 seconds
1	1	1	1	10485.76 seconds (see note 3)	20.48 seconds	40.96 seconds

1. The value is applicable only in WB-S1 mode. If received in NB-S1 mode it is interpreted as if the Extended DRX parameters IE were not included in the message by this version of the protocol.
2. The value is applicable only in WB-S1 mode. If received in NB-S1 mode it is interpreted as 0010 by this version of the protocol.
3. The value is applicable only in NB-S1 mode. If received in WB-S1 mode it is interpreted as 1101 by this version of the protocol.

8.1.2 Use Cases

8.1.2.1 Enable eDRX, Set and Query eDRX Cycle and PTW Value

Command	Response	Comment
Enable eDRX and set requested eDRX cycle to 20.48 s, requested PTW to 2.56 s		
AT+SQNEDRX=2,4,"0010","0001"	OK	4: E-UTRAN (WB-S1 mode) eDRX cycle 20.48 s PTW 2.56 s
AT+SQNEDRX?	+SQNEDRX:2,4,”0010”,”0001” OK	
Get used eDRX cycle and PTW value, check the URC +CEDRXP		
	+CEDRXP: 4,"0010","0010","0011"	4: E-UTRAN (WB-S1 mode) Requested eDRX cycle (20.48 s) Network provided eDRX cycle (20.48 s) PTW (10.24 s)
Query current configured eDRX parameters Note: The eDRX cycle used and the PTW value may differ from the ones configured with AT+SQNEDRX (AT+CEDRXS). Get the values set by the network only through the URC +CEDRXP.		
AT+CEDRXS?	+CEDRXS: 4,"0001" OK	4: E-UTRAN (WB-S1 mode) Requested eDRX cycle (10.24 s)

8.1.2.2 Disable eDRX

Command		Response	Comment
AT+SQNEDRX=0	OK		0: Disable the use of eDRX

8.2 How to Use the PSM Feature

8.2.1 Feature Description

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

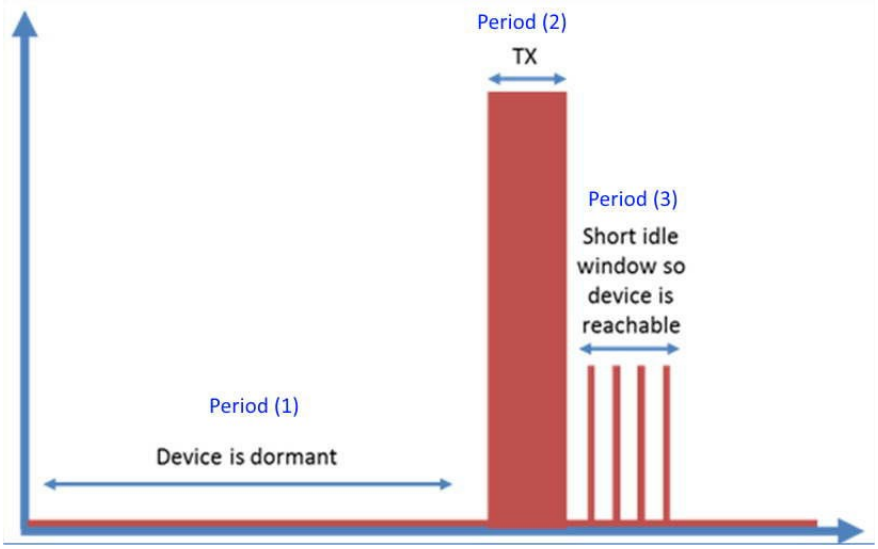

Figure 13. PSM Timing

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).

The following table 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.

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.

The following table 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.

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]).

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, the value shall be interpreted as multiples of 320 hours. Otherwise, value shall be interpreted as multiples of 1 hour.

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]).

The related AT commands are:

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

In order to optimize the power consumption, it is strongly recommended to set T3412 to a value **higher than the interval 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.

8.2.2 Use Case

Command	**Response**	**Comment**
Enable PSM and configure requested T3412 Extended and T3324 timers		
AT+CPSMS=1,,,"10100011","00100001"	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

Command	Response	Comment
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 a successful attach or a 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 configured value manually after AT+CEREG=4		
AT+CEREG?	+CEREG: 4,1,"0002","01A2D002",7,,,"00000101","00010010" 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

8.3 eDRX and 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 takes some time to bring the UART ports up again. If the host MCU supports hardware flow control, the command is 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 a rising edge on the `PS_STATUS` line before sending any command.

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

In eDRX, the final cycle value is advertised in the `+CEDRXP` URC:

```
+CEDRXP:  4,"0010","0010","0011"
```

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 eDRX 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
  - RYZ024 module does not enter deep sleep mode if a timer is scheduled to fire within a few tenths of a second

8.4 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 neighbouring cells.

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

The modem scans 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 only).		
AT+SQNINS=1	+SQNINS: 1,3,7,"0","0000","000000",1825,154,1.4,-90.70,-9.40 +SQNINS: 1,3,7,"0","0000","000000",1825,211,15,-97.30,-17.40 +SQNINS: 1,1,7,"0","0000","000000",100,154,1.4,-100.90,-15.30 +SQNINS: 1,4,7,"0","0000","000000",2050,154,1.4,-101.90,-15.60 +SQNINS: 1,3,7,"0","0000","000000",1650,214,1.4,-82.40,-14.60 +SQNINS: 1,1,7,"0","0000","000000",450,268,1.4,-104.50,-16.50 +SQNINS: 1,1,7,"0","0000","000000",450,212,1.4,-100.60,-13.10 +SQNINS: 1,1,7,"0","0000","000000",450,218,20,-103.50,-15.30 +SQNINS: 1,3,7,"0","0000","000000",1275,414,15,-89.80,-9.50 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	
Report information for all cells		
AT+SQNMONI=7	+SQNMONI: AT&T Cc:310 Nc:410 RSRP:-99.30 RSRQ:-12.30 TAC:27207 Id:467 EARFCN:5110 PWR:-79.22 PAGING:128 +SQNMONI: RSRP:-101.30 RSRQ:-15.00 Id:459 EARFCN:5110 PWR:-78.52 +SQNMONI: RSRP:-112.30 RSRQ:-21.90 Id:366 EARFCN:5110 PWR:-82.62	

9.2.3 Error Handling

During PSM sleep and eDRX 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.sequans.com",1,32` for example).

Important: `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 on RYZ024

RYZ024 modules can be controlled via a serial interface UART using standard AT commands. The serial AT interface can be managed using hardware flow control or not. Please refer to the *System Integration Guide* for more details.

RYZ024-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.

Please refer to RYZ024 module's data sheet 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 an URC, Data or SMS are waiting to be read. RING should be monitored especially during the following specific cases:

- Immediate URC presentation is impossible, for instance when the UART is 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 the 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 the RING signal.		
AT+SQNRICFG=2,1	OK	
AT+SQNRICFG?	+SQNRICFG: 2,1,1000 OK	
Change the duration to 2 s 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, the MCU needs to set timers in the module and get warned when they fire. 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 parameter of the AT uses the absolute notation. 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: "19/04/26,17:14:55+32" OK	
If the module is NOT attached to network, the time/date starts Jan. 1st, 1970. In this case, adjust the clock manually, or use it as is for tests.		
	+CCLK: "70/01/01,00:00:10+00" OK	

10.3.2.2 Set Alarm, in Format Date-time

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

10.3.2.3 Set an Alarm Recurring Every Day

Command	Response	Comment
AT+CCLK="19/01/01, 00:01:00+00"	OK	Set date/time by +CCLK
AT+CALA="00:01:30+ 00",1,0,"second","0",1	OK	Set alarm timer
AT+CALA?	+CALA: "19/01/01,00:01:00",0,0,"first alarm",0 +CALA: "19/01/01,00:01:30",1,0,"second","1,2,3,4,5,6,7",1 OK	Check alarm timer
	+CALV: 1	30 s later. Because “silent” is 1, no text is displayed here
Check the date is shifted for next day ('tomorrow').		
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 OK	Compared with above date, it is now “19/01/02”.

10.3.2.4 Set an Alarm Recurring on Selected Days

Command	Response	Comment
AT+CCLK="19/01/01,0 0:01:00+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 the alarm timer		

Command	Response	Comment
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: " 19/01/01,00:02:00",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: "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	Compared with above date, it is now “19/01/06”.

10.3.2.5 Overwrite an 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 with command		
AT+CALA="19/02/01,05:05:05+00",0,0,"first alarm edited"	OK	
Check the timer again		
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 an alarm

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

11. Manufacturing

11.1 How to Configure GPIOs Alternate Functions

11.1.1 Feature Description

Several of the RYZ024 module's GPIO signals have alternate functions that can be configured with `AT+SQNHWCFG`. The following functions can be activated on RYZ024 module pins:

- PS_STATUS function control
- Wake signal detection (wakeId = "wake0", "wake1", "wake2", "wake3", "wake4", "wakeRTS0", "wakeRTS1", "wakeSim0") function control
- STATUS_LED function control
- RING function control
- Antenna tuning (antennaTuning) function control
- SPI interface function control
- I²C interface function control
- JTAG function control
- UICC interface (simItf: sim0, sim1, sim2) function control
- TX Indicator function control
- Change UART configuration (uartId: uart0, uart1, uart2, uart3) function control
- Modem UART I/O configuration (dcd, dsr and dtr lines)
- ADC function control
- GPIO function control
- Boot source function control (Boot from Flash or Boot from Host)

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

Note: 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 Datasheet 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 PS_STATUS

This power saving status signal indicates that the module needs to be woken-up with either RTS0, RTS1, WAKE0, WAKE1, WAKE2 or WAKE3 signal before sending data or commands through one of the UART interface.

`PS_STATUS` function is multiplexed on `GPIO2`. Please check the *System Integration Guide* for more details on the `PS_STATUS` signal.

Command	Response	Comment
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG="ps_status"	+SQNHWCFG: ps_status: enable OK	The write command issued with <function> parameter only is equivalent to the read command output filtered out for selected <function>. Read the function (enabled by default)
AT+SQNHWCFG="ps_status" ,"disable"	OK	Disable the function
Reboot the device		

Command	Response	Comment
AT^RESET	OK	
	+SYSSHDN +SYSTART	
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG="ps_status"	+SQNHWCFG: ps_status: disable OK	Read the function (disabled)
Then the module power saving status by the defined GPIO is deactivated.		

11.1.2.2 Wake

WAKE0, WAKE1, WAKE2, WAKE3, 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 will prevent it to enter 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.

Command	Response	Comment
AT+CFUN=5	OK	Switch to manufacturing mode
Check wake sources configuration.		
AT+SQNHWCFG?	(…) +SQNHWCFG: wake0: disable +SQNHWCFG: wake1: disable +SQNHWCFG: wake2: disable +SQNHWCFG: wake3: disable +SQNHWCFG: wake4: disable +SQNHWCFG: wakeRTS0: enable +SQNHWCFG: wakeRTS1: enable (…) OK	The read command returns the list of supported pin functions state and detailed configuration (when applicable). wake0, wake1, wake2 and wake3 are all disabled, wakeRTS0 and wakeRTS1 are both enabled with inverted polarity.
Enable wake1 with inverted polarity (negative polarity)		
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	

Command	Response	Comment
	+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	

11.1.2.3 Status_led

This configures the device status indication function control. This function is disabled by default (pin configured in input mode). It is multiplexed with GPIO1.

Command	Response	Comment
AT+CFUN=5	OK	Switch to manufacturing mode
AT+SQNHWCFG="status_led"	+SQNHWCFG: status_led: disable OK	status_led is disabled by default.
AT+SQNHWCFG="status_led", "enable"	OK	Enable the function with normal polarity
Reboot the device		
AT^RESET	OK	
	+SYSSHDN +SYSTART	
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG="status_led"	+SQNHWCFG: status_led: enable, polarity: normal OK	Read the function (enabled)

Once the function is enabled, the device status indication function needs to be configured with `AT+SQNLED=1` command. The LED turns on or off under these conditions:

CFUN Mode	System State	LED Status
CFUN=0 or CFUN=4	ME stopped/airplane mode	Permanently off
CFUN=1	LTE PS data transfer	Permanently on
	ME registered to a network, No call, no data transfer (in RRC Idle)	1280 ms on/ 3840 ms off
	Limited Network Service (no SIM, no PIN, network search)	500 ms on / 500 ms off
	ME in extended SLEEP (eDRX or PSM)	Permanently off

11.1.2.4 RING0

The RING function is enabled by default. The default signal polarity is inverted (RING active at low level). RING function behavior can be configured with `AT+SQNRICFG` command as explain in section 10.2.

Command	Response	Comment
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG?	(…) +SQNHWCFG: ring0: enable, polarity: inverted (…) OK	The read command returns the list of supported pin functions state and detailed configuration (when applicable). RING0 is enabled by default with inverted polarity.
AT+SQNHWCFG="ring0",”disable”	OK	Disable the function
Reboot the device		
AT^RESET	OK	
	+SYSSHDN +SYSTART	
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG="ring0"	+SQNHWCFG: ring0: disable OK	Read the function (disabled)

11.1.2.5 Antenna Tuning

On small PCBs, it is difficult to design a proper antenna matching circuit for a wide range of frequencies. One option consists in tuning the antenna matching dynamically, according to the active RF band. On RYZ024 module, two pins are defined by default: `ANT_TUNE0` and `ANT_TUNE1`, which correspond to `GPIO34` and `GPIO35`.

The configuration command `AT+SQNHWCFG="antennaTuning"` can be used to activate, deactivate and configure the antenna tuner. In the example below, `GPIO34` and `GPIO35` 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**
GPIO34 (ANT_TUNE0)	0	1	1	0
GPIO35 (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","617,698,0x0,698,7 97,0x2,797,887,0x1,887,2200,0x3"	OK	"0x0" is the default value used for all frequencies outside the defined ranges. "617,698,0x0,….": A list of triplets. Each triplet defines one frequency range 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	

⚠ Frequency ranges must not overlap. The value of GPIO34 and GPIO35 is undefined on the overlapping segments.

11.1.2.6 SPI Configuration

The SPI interface is multiplexed with `GPIO7`, `GPIO8`, `GPIO9`, `GPIO10` and `GPIO11` pins.

Command	Response	Comment
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG="spi"	+SQNHWCFG: spi_mosi: disable +SQNHWCFG: spi_clk: disable +SQNHWCFG: spi_miso: disable +SQNHWCFG: spi_csn0: disable +SQNHWCFG: spi_csn1: disable OK	
AT+SQNHWCFG="spi","enable"	ERROR: spi_mosi BUSY (gpio7) ERROR: spi_clk BUSY (gpio9) ERROR: spi_miso BUSY (gpio8) ERROR: spi_csn0 BUSY (gpio10) ERROR: spi_csn1 BUSY (gpio11) ERROR	
Disable the GPIOs muxed with SPI interface.		
AT+SQNHWCFG="gpio7","disable"	OK	
AT+SQNHWCFG="gpio8","disable"	OK	
AT+SQNHWCFG="gpio9","disable"	OK	
AT+SQNHWCFG="gpio10","disable"	OK	
AT+SQNHWCFG="gpio11","disable"	OK	
AT+SQNHWCFG="spi","enable"	OK	
AT+SQNHWCFG="spi"	+SQNHWCFG: spi_mosi: enable +SQNHWCFG: spi_clk: enable +SQNHWCFG: spi_miso: enable +SQNHWCFG: spi_csn0: enable +SQNHWCFG: spi_csn1: enable OK	
Reboot the device		
AT^RESET	OK	
	+SYSSHDN +SYSTART	

11.1.2.7 I²C Configuration

The I²C interface is multiplexed with GPIO23, GPIO24 pins.

Command	Response	Comment
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG="i2c"	+SQNHWCFG: i2c_sda: disable +SQNHWCFG: i2c_scl: disable OK	
AT+SQNHWCFG="i2c","enable"	ERROR: i2c_sda BUSY (gpio23) ERROR: i2c_scl BUSY (gpio24) ERROR	
Disable the GPIOs multiplexed with the I²C interface.		
AT+SQNHWCFG="gpio23","disable"	OK	
AT+SQNHWCFG="gpio24","disable"	OK	
AT+SQNHWCFG="i2c","enable"	OK	
AT+SQNHWCFG="i2c"	+SQNHWCFG: i2c_sda: enable +SQNHWCFG: i2c_scl: enable OK	
Reboot the device		
AT^RESET	OK	
	+SYSSHDN +SYSTART	

11.1.2.8 JTAG

The JTAG interface is enabled by default and is not configurable.

Note: Once JTAG is disabled, it cannot be enabled again. Disabling JTAG is permanent.

Command	Response	Comment
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG="jtag"	+SQNHWCFG: jtag: enabled OK	
AT+SQNHWCFG="jtag","permanentDisable"	OK	

11.1.2.9 SIM Interface Configuration

RYZ024 modules support multiple card slots. By default, the SIM0 interface is enabled and SIM1 is disabled. The SIM1 slot must be configured at the hardware level using the `AT+SQNHWCFG` command before it can be activated with the `AT+CSUS` command. SIM1 signals are multiplexed with `GPIO25`, `GPIO26` and `GPIO27` pins.

Note: When the module is equipped with an iSIM, the SIM slot is SIM2 and can be enabled with the same procedure as the one described below (no need to disable GPIOs in that case)

Command	Response	Comment
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG="SIM0"	+SQNHWCFG: sim0_data: enable +SQNHWCFG: sim0_clk: enable +SQNHWCFG: sim0_resetn: enable +SQNHWCFG: sim0_detect: enable +SQNHWCFG: sim0: enable +SQNHWCFG: sim0: enable OK	
AT+SQNHWCFG="SIM1"	+SQNHWCFG: sim1_data: disable +SQNHWCFG: sim1_clk: disable +SQNHWCFG: sim1_resetn: disable +SQNHWCFG: sim1: disable +SQNHWCFG: sim1_pollinginterval: 0 OK	
AT+SQNHWCFG="SIM1","enable"	ERROR: sim1_detect UNSUPPORTED ERROR	There is no SIM detect signal on this SIM interface so SW polling needs to be enabled
AT+SQNHWCFG="sim1","enable","10000"	ERROR: sim1_data BUSY (gpio25) ERROR: sim1_clk BUSY (gpio26) ERROR: sim1_resetn BUSY (gpio27) ERROR: Failed to set pins ERROR	
Disable the GPIOs mixed with SIM1 interface.		
AT+SQNHWCFG="gpio25","disable"	OK	
AT+SQNHWCFG="gpio26","disable"	OK	
AT+SQNHWCFG="gpio27","disable"	OK	
AT+SQNHWCFG="sim1","enable","10000"	OK	
AT+SQNHWCFG="sim1"	+SQNHWCFG: sim1_data: enable +SQNHWCFG: sim1_clk: enable +SQNHWCFG: sim1_resetn: enable +SQNHWCFG: sim1: enable, polling +SQNHWCFG: sim1_pollinginterval: 10000 OK	

Command	Response	Comment
Reboot the device		
AT^RESET	OK	
	+SYSSHDN +SYSTART	

Once the SIM1 interface is enabled, it can be selected as the main interface for NAS layer using the AT+CSUS command

Command	Response	Comment
AT+CSUS?	+CSUS: 0 OK	SIM0 is selected
AT+CSUS=?	+CSUS: 2 OK	There are two available SIM slots
AT+CSUS=1	OK	Select SIM1 interface

11.1.2.10 TxIndicator

The transmission indicator (`TX_IND`, OUT) is used to warn the host that the modem is transmitting data. The `TX_IND` pin is multiplexed with the `GPIO33` pin. 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	

11.1.2.11 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	

11.1.2.12 UART Configuration

There are three UARTs available in RYZ024 module. 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: 115200, format: 8 bits, parity: none, stopbits: 1, application: at OK	
AT+SQNHWCFG="uart1"	+SQNHWCFG: uart1: enable, flowcontrol: rtscts, baudrate: 921600, format: 8 bits, parity: none, stopbits: 1, application: at OK	
AT+SQNHWCFG="uart2"	+SQNHWCFG: uart2: enable, flowcontrol: unsupported, baudrate: 115200, format: 8 bits, parity: none, stopbits: 1, application: console OK	
AT+SQNHWCFG="uart1","enable",,,,,"dcp"	OK	
Reboot the device		
AT^RESET	OK	
	+SYSSHDN +SYSTART	
AT+CFUN=5	OK	Switch to Manufacturing Mode

Command	Response	Comment
AT+SQNHWCFG="uart1"	+SQNHWCFG: uart1: enable, flowcontrol: rtscts, baudrate: 921600, format: 8 bits, parity: none, stopbits: 1, application: dcp OK	

11.1.2.13 ADC

The auxiliary ADC samples an analogue signal, converting it to a digital value. RYZ024 modules have one external line dedicated to the auxiliary ADC. ADC1 is on pad 72, it is disabled by default and can be enabled as follows:

Command	Response	Comment
AT+CFUN=5		Switch to Manufacturing Mode
	OK	
AT+SQNHWCFG="adc1",”enable”		Enable ADC1 line, this is the only available ADC line on RYZ024
	OK	
AT^RESET		Restart the modem
	OK SHUTDOWN SYSSTART	

Once ADC1 line is enabled, the ADC value can be read with the `AT+SQNADC` command:

Command	Response	Comment
AT+SQNADC=”adc1”		Read voltage in mV
	+SQNADC: adc1, 1023	1.023 V

11.1.2.14 GPIO Configuration

33 GPIOs are available on RYZ024 module: 28 named `GPIO1` to `GPIO28` and 5 named `GPIO31` to `GPIO35`. The GPIOs listed in the table below are not enabled by default.

GPIO Range	Enable State by Default
GPIO3 to GPIO11	Disabled
GPIO17 to GPIO28	Disabled
GPIO31 to GPIO32	Disabled

Command	Response	Comment
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG="gpio17"	+SQNHWCFG: gpio17: disable OK	
AT+SQNHWCFG="gpio17",”enable”	OK	
Reboot the device		

AT^RESET	OK	
	+SYSSHDN +SYSTART	
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG="gpio17"	+SQNHWCFG: gpio17: enable, polarity: normal, direction: input, value: low OK	

Once enabled, the GPIOS can be driven with the `SQNGPIO` command.

11.1.2.15 Behavior at Factory Reset

The hardware configuration is overwritten by a device factory reset (by `AT+SQNSFACTORYRESET`), unless it has been secured using `AT+SQNFACTORYSAVE =”OEM”`. The following example illustrates the behavior of the `txIndicator` signal.

Command	Response	Comment
AT+CFUN=5	OK	Switch to Manufacturing Mode
Check txIndicator configuration		
AT+SQNHWCFG="txIndicator"	+SQNHWCFG: txIndicator: disable OK	txIndicator is disabled by default
AT+SQNHWCFG="txIndicator"," enable"	OK	Enable txIndicator. It is not possible to change the polarity of this signal
AT^RESET	OK	Reboot the device
	+SYSSHDN +SYSTART	
Check txIndicator configuration		
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG=" txIndicator "	+SQNHWCFG: txIndicator: enable OK	txIndicator is enabled
AT+SQNSFACTORYRESET	OK	Execute factory reset
AT^RESET	OK	Reboot the device
	+SYSSHDN +SYSTART	
Check txIndicator configuration		
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG="txIndicator"	+SQNHWCFG: txIndicator: disable OK	txIndicator is disabled again

Command	Response	Comment
Re-run the procedure above with AT+SQNFACTORYSAVE =”OEM” before the factory reset.		
AT+SQNHWCFG="txIndicator"," enable"	OK	Re-enable txIndicator
AT^RESET	OK	Reboot the device
	+SYSSHDN +SYSTART	
Check txIndicator configuration		
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG=" txIndicator "	+SQNHWCFG: txIndicator: enable OK	txIndicator is enabled
AT+SQNFACTORYSAVE =”OEM”	OK	Save the current configuration
AT+SQNSFACTORYRESET	OK	Execute factory reset
AT^RESET	OK	Reboot the device
	+SYSSHDN +SYSTART	
Check txIndicator configuration		
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SQNHWCFG="txIndicator"	+SQNHWCFG: txIndicator: enable OK	txIndicator is kept enabled

11.1.3 Error Handling

In case of an unsupported function or invalid configuration, AT commands return `ERROR` and the "`+CME ERROR: <err>`" notification is sent.

For pins shared by several functions (such as `PS_STATUS`), the activated function must be disabled before a new one is selected. Trying to enable a new function on a pin already assigned to another function raises `ERROR` and the "`+CME ERROR: <err>`" notification is sent.

If the `AT+SQNHWCFG?` command reports an "undefined" status for any signal of interest, please contact Renesas support team for help.

11.2 How to Set GPIO and Wake Signals

The RYZ024 platform supports two types of GPIOs:

- GPIO signals, that are set as input or output, with active level high or low.
- Wake signals that can be used to wake the platform up when it is in low power mode

The related AT commands are:

- `AT+SMGT` to drive GPIO signals
- `AT+SMGI` to drive GPIO signals
- `AT+SMWAKE` to read wake signals

Note: These commands can be used even if a pin is not enabled as GPIO or Wake signal with `AT+SQNHWCFG` command.

11.2.1 Setting GPIOs

`AT+SMGT` and `AT+SMGI` commands are used with GPIO.

11.2.1.1 Example with GPIO as Output

Command	Response	Comment
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SMGT=0,0,0x1,0,0,0x1	OK	Set GPIO 0 to High with normal polarity
AT+SMGT=0,0,0x1000000,0,0,0 x1000000,0,0,0x1000000	OK	Set GPIO 24 to High with inversed polarity
AT+SMGT=0,0x8,0,0,0x8,0	OK	Set GPIO 35 to High with normal polarity
AT+SMGT=0,0x1,0x1000000,0, 0x1,0 x1000000,0,0x1,0x1000000	OK	Set GPIO 32 and 24 to High with inversed polarity at the same time
AT+SMGT=0,0,0x1000000,0,0,0 ,0,0, 0x1000000	OK	Set GPIO 24 to Low, GPIO 32 is unchanged

Important: `AT+SMGT?` does NOT return meaningful values. Use an external equipment to read the output values of a GPIO.

11.2.1.2 Example with GPIO as Input

Command	Response	Comment
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SMGI=0,0,0x10	OK	Set GPIO 4 as input with normal polarity
Connect 1V8 to GPIO 4 and read GPIOs		
AT+SMGI?	+SMGI:0x0020 20000010 OK	Bit for GPIO 4 is set to 1
Connect 0V to GPIO 4 and read GPIOs		
AT+SMGI?	+SMGI:0x0020 20000000 OK	Bit for GPIO 4 is set to 0

11.2.2 Reading WAKE Signals

Command	Response	Comment
AT+CFUN=5	OK	Switch to Manufacturing Mode
AT+SMWAKE?	+SMWAKE: wake0 wake4 wakeRTS1 OK	
Open a Tera Term window on UART1 (that disables UART1 as a wake source).		
AT+SMWAKE?	+SMWAKE: wake0 wake4 OK	

11.3 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.

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

11.4 How to Check Module's Identities

RYZ024 modules are shipped with a preset IMEI as well as a calibration file. During the development phase, the IMEI and calibration file might get lost during a SW upgrade. It is possible to read the IMEI of the module as follows:

Command	Response	Comment
AT+CGSN=1	015770000056300 OK	

If the IMEI appears unset and the calibration file of the module seems lost, please contact your Renesas's representative for support.

Important: Regulations forbid overwriting the IMEI. It is written in an OTP (one time programmable) memory.

12. System Features

12.1 Time Synchronization

The Coordinated Universal Time (UTC) clock is set to the Epoch time (1970-01-01T00:00:00Z) at module cold boot (HW/SW reset, electrical power-on). The UTC clock is occasionally updated during the device lifetime using an external time reference provided either by the network or by application services.

Full modem operation is possible even if the absolute time is not set. Some application services, however, require a working UTC clock. Typically, precise time information is:

- Mandatory to verify security certificates' validity
- Mandatory to speed up GNSS initial time to fix (hot start)
- Mandatory to manage calendar events (reconnect to an application server at a given date and time) using alarm/timer framework
- Useful to timestamp sensor data or the system's log

It is worth noting that expected UTC time accuracy depends on the application type:

- Certificate validity checks require only approximate precision (few minutes or even hour precision is enough)
- GNSS hot start requires minute precision (< 2 mins)
- Applications required to respect a connection timeframe may require second precision

Time synchronization can be achieved in various ways:

- Cellular network native services can be enabled with `AT+CTZU` and `AT+CTZR` at no data plan cost
  - 3GPP System Information Block Type 16
    - The SIB16 information element contains information related to GPS time and Coordinated Universal Time (UTC).
    - SIB16 support is optional and, when supported by the network, the message is broadcasted periodically. Most of the Cat M1 networks do not broadcast SIB16.
  - Network Identity and Time Zone (NITZ) protocol
    - The NITZ is a mechanism for broadcasting local time and date, time zone and DST offset, as well as network provider identity information, to mobile devices over a wireless network.
    - NITZ support is optional. When supported by the network, the time information is delivered occasionally, typically during modem registration to the network or when crossing radio network boundaries.
- Non-cellular native solution
  - Network Time Protocol (NTP) and derivatives (SNTP, etc.) using the `AT+SQNNTP` command
    - NTP is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.
    - NTP time update is independent of cellular network capabilities and relies on thousands of free servers around the world.
  - Local interface
    - The application software can acquire local time its own way (RTC, NTP, GNSS, other) and set the cellular module's clock with the `AT+CCLK` command.

Renesas' recommendation is to enable cellular native solutions (SIB16, NITZ) to acquire local time, since these methods do not require any user action and do not involve a data plan cost. If the network does not support these protocols, NTP can be used to fetch the UTC time.

The application can trigger a NTP request as soon as the registration is complete, in order to update the clock after checking its validity (the clock can be considered invalid if it reports a date earlier than year 2022). Compared to an automatic solution, a manual request speeds up the time acquisition but comes at the risk of triggering a useless NTP session if SIB16 and/or NITZ information arrives in the meanwhile. Note that an NTP session (including DNS and NTP transactions) cannot be aborted once initiated.

Finally, if the local time is available on an external device (RTC, GNSS, etc.), it can be set using the `AT+CCLK` command.

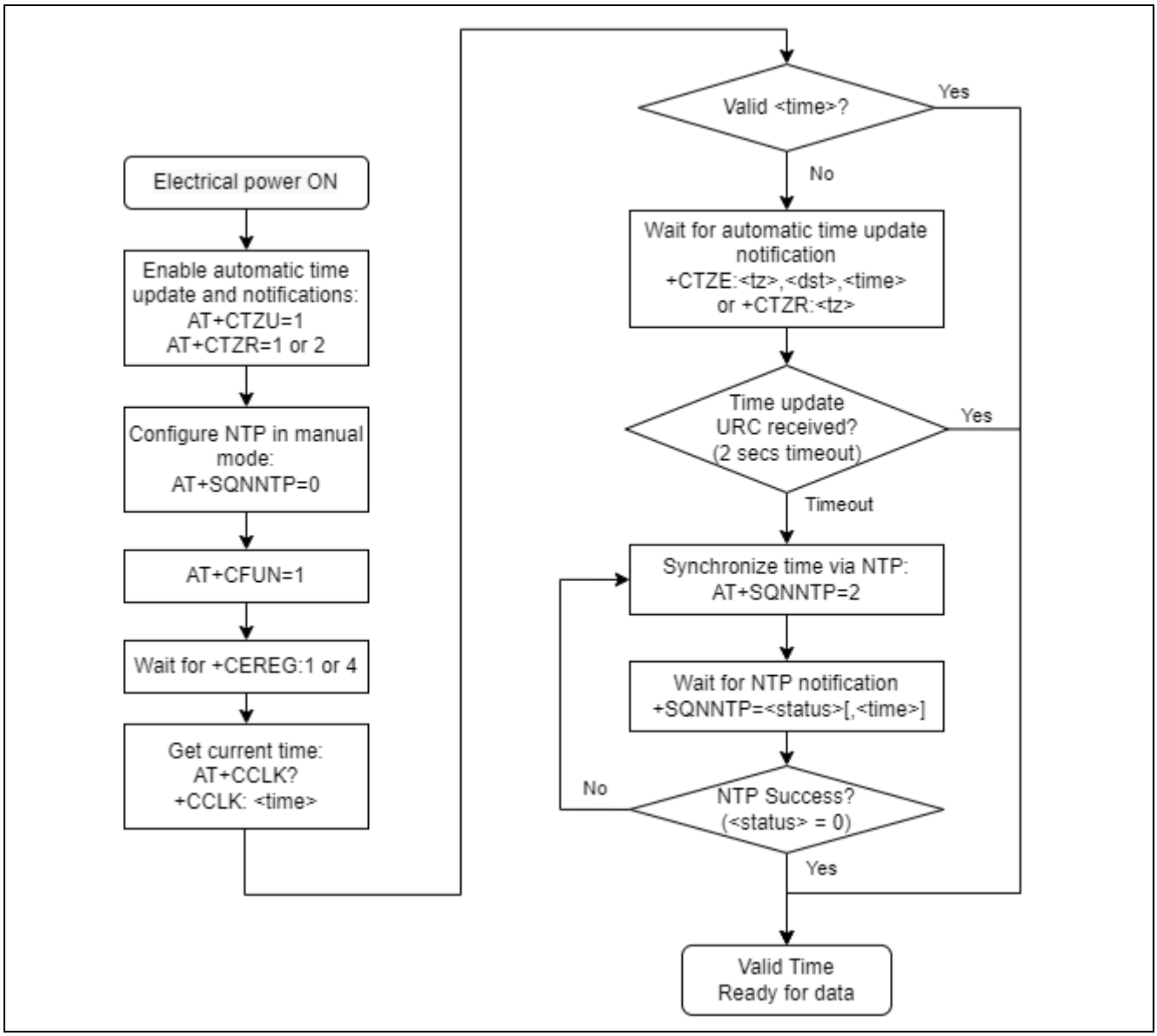

Figure 14. Time Synchronization at Power On

12.2 Battery Monitoring

When voltage monitoring is enabled, the module voltage is periodically checked by the internal voltage sensor. If the voltage goes below a predefined threshold, the `+SQNVMONS` notification is issued.

If the module's voltage is still below the threshold three seconds later and the automatic emergency shutdown is enabled, the device issues a new URC and triggers an emergency shutdown procedure.

Command	Response	Comment
AT+SQNVMON?	+SQNVMON: 0 OK	By default, voltage monitoring is disabled Voltage cannot be read in this mode
AT+SQNVMON=1,33,10	+SQNVMON: 1,0,3582 OK	Activate voltage monitoring. The power supply is set to 3.6V
Power supply is lowered to 3 V		

Command	Response	Comment
	+SQNVMONS: 1,1,2979	URC is sent when the power supply goes below 3.3 V for more than 10 seconds
Switch to mode 2 to enable automatic emergency shutdown. Power supply is set back to 3.6 V		
AT+SQNVMON=2,33,10	+SQNVMON: 2,0,3577	
Power supply is lowered to 3V		
	+SQNVMONS: 2,1,2979 OK	URC is sent when the power supply goes below 3.3 V for more than 10 seconds
	+SQNVM ONS: 2,10,2979	After 3 seconds, the emergency shutdown procedure is triggered, status 10 indicates that the shutdown procedure has started
	+SHUTDOWN	Modem shutdown, UART is not responding

12.3 Temperature Monitoring

When temperature monitoring is activated, the modem measures the temperature with the embedded sensor and sends URCs to the host MCU each time the temperature switches from one temperature range to another. The five temperature ranges defined are:

- -2: Low extreme temperature range
- -1: Low temperature range
- 0: Operational range
- 1: High temperature range
- 2: High extreme temperature range

If automatic emergency shutdown is enabled, the module triggers an emergency shutdown procedure when the temperature enters the high extreme temperature zone.

Command	Response	Comment
AT+SQNTMON?	+SQNTMON: 0,-40,-30,80,90,23 OK	By default, temperature monitoring is disabled Current temperature is 23 °C
AT+SQNTMON=1,-40,-30,30,40	+SQNTMONS: 1,0,25 OK	Enable temperature monitoring and change the thresholds
Module is in an oven; temperature is increasing and is above 30°C		
	+SQNTMONS: 1,1,32	Now in high temperature range
Temperature continues increasing, above 40 °C		
	+SQNTMONS: 1,2,43	Now in extreme temperature range. In mode 1, automatic shutdown is not enabled
Switch to mode 2 to enable automatic emergency shutdown		
AT+SQNTMON=2,-40,-30,30,40	+SQNTMONS: 2,2,42 OK	

Command	Response	Comment
	+SQNTMONS: 2,10,42	Receive timer expiration URC after 3s
	+SHUTDOWN	Modem shutdown, UART is not responding

13. 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 Renesas 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

Term	Description
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
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

Rev.	Date	Description	
		Page	Summary
0.95	Jun.10.22	—	Preliminary release document
0.96	Jun.22.22	14	2.2.2.3 Added “Define Preferred EARFCN to be Scanned in Priority”
		18	2.3.1 Added signal quality explanation
		20	2.3.2.6 Added “Check the RSRP and RSRQ Values”
		27	3.4.1 Changed example contents for Private Key Stored
		31	4.1 Changed explanation for FOTA
		36	5 Typo correction
		39	6.1.2 Changed Comment of Use cases
		70	7 Added SMS service
		71	7.1.1 Added private AT commands for SMS in text mode
		73	7.1.2.3 Added example of Send SMS
		88	9.2.2 Added more details on SQNMONI
		96	11.1.2.5 Changed Antenna Tuning Table
		99	11.1.2.9 Added explanation for SIM interface
1.00	Sep.22.22	—	Updated for NPI

General Precautions in the Handling of Microprocessing Unit and Microcontroller Unit Products

The following usage notes are applicable to all Microprocessing unit and Microcontroller unit products from Renesas. For detailed usage notes on the products covered by this document, refer to the relevant sections of the document as well as any technical updates that have been issued for the products.

1. Precaution against Electrostatic Discharge (ESD)

   A strong electrical field, when exposed to a CMOS device, can cause destruction of the gate oxide and ultimately degrade the device operation. Steps must be taken to stop the generation of static electricity as much as possible, and quickly dissipate it when it occurs. Environmental control must be adequate. When it is dry, a humidifier should be used. This is recommended to avoid using insulators that can easily build up static electricity. Semiconductor devices must be stored and transported in an anti-static container, static shielding bag or conductive material. All test and measurement tools including work benches and floors must be grounded. The operator must also be grounded using a wrist strap. Semiconductor devices must not be touched with bare hands. Similar precautions must be taken for printed circuit boards with mounted semiconductor devices.
2. Processing at power-on

   The state of the product is undefined at the time when power is supplied. The states of internal circuits in the LSI are indeterminate and the states of register settings and pins are undefined at the time when power is supplied. In a finished product where the reset signal is applied to the external reset pin, the states of pins are not guaranteed from the time when power is supplied until the reset process is completed. In a similar way, the states of pins in a product that is reset by an on-chip power-on reset function are not guaranteed from the time when power is supplied until the power reaches the level at which resetting is specified.
3. Input of signal during power-off state

   Do not input signals or an I/O pull-up power supply while the device is powered off. The current injection that results from input of such a signal or I/O pull-up power supply may cause malfunction and the abnormal current that passes in the device at this time may cause degradation of internal elements. Follow the guideline for input signal during power-off state as described in your product documentation.
4. Handling of unused pins

   Handle unused pins in accordance with the directions given under handling of unused pins in the manual. The input pins of CMOS products are generally in the high-impedance state. In operation with an unused pin in the open-circuit state, extra electromagnetic noise is induced in the vicinity of the LSI, an associated shoot-through current flows internally, and malfunctions occur due to the false recognition of the pin state as an input signal become possible.
5. Clock signals

   After applying a reset, only release the reset line after the operating clock signal becomes stable. When switching the clock signal during program execution, wait until the target clock signal is stabilized. When the clock signal is generated with an external resonator or from an external oscillator during a reset, ensure that the reset line is only released after full stabilization of the clock signal. Additionally, when switching to a clock signal produced with an external resonator or by an external oscillator while program execution is in progress, wait until the target clock signal is stable.
6. Voltage application waveform at input pin

   Waveform distortion due to input noise or a reflected wave may cause malfunction. If the input of the CMOS device stays in the area between V_{IL} (Max.) and V_{IH} (Min.) due to noise, for example, the device may malfunction. Take care to prevent chattering noise from entering the device when the input level is fixed, and also in the transition period when the input level passes through the area between V_{IL} (Max.) and V_{IH} (Min.).
7. Prohibition of access to reserved addresses

   Access to reserved addresses is prohibited. The reserved addresses are provided for possible future expansion of functions. Do not access these addresses as the correct operation of the LSI is not guaranteed.
8. Differences between products

   Before changing from one product to another, for example to a product with a different part number, confirm that the change will not lead to problems. The characteristics of a microprocessing unit or microcontroller unit products in the same group but having a different part number might differ in terms of internal memory capacity, layout pattern, and other factors, which can affect the ranges of electrical characteristics, such as characteristic values, operating margins, immunity to noise, and amount of radiated noise. When changing to a product with a different part number, implement a system-evaluation test for the given product.

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/.

© 2022 Renesas Electronics Corporation. All rights reserved.