SIM Access Profile User Guide

80000ST10029a Rev. 2 - 16/01/09

Making machines talk.

This document is related to the following products:

APPLICABILITY TABLE

PRODUCT	PART NUMBER	APPLICABILITY
GT863-PY	3990150471	
GT864-QUAD	4990150069	√
GT864-PY	4990150070	√
GM862-GPS	GM862GPS***-***	√
GM862-QUAD-PY	GM862PYT***-***	√
GM862-QUAD	GM862QUD***-***	√
GC864-QUAD	GC864QUD***-***	√
GC864-PY	GC864PYT***-***	√
GC864-QUAD-C2	GC864QC2***-***	√
GC864-PY-C2	GC864PC2***-***	√
GC864-QUAD w/SIM holder	GC864QUH***-***	√
GC864-PYw/SIM holder	GC864PUH***-***	√
GE863-GPS	GE863GPS***-***	√
GE863-PY	GE863PYT***-***	√
GE863-QUAD	GE863QUD***-***	√
GE863-SIM	GE863SIM***-***	√
GE863-PRO3 without OS	GE863PR3***-***	√
GE863-PRO3 with Linux OS	GE863PR3***	√
GE863-PRO3 64MB w/o OS	GE863PR3***	√
GE863-PRO3 64MB w Linux OS	GE863PR3***	√
GE864-PY	GE864PYT***-***	√
GE864-QUAD	GE864QUD***-***	√
GE864-QUAD Automotive	GE864AUT***-***	√

The suffix "***-***" depends on the module HW/SW configuration. Please contact your Telit representative for details

Contents

DISCLAIMER

The information contained in this document is the proprietary information of Telit Communications S.p.A. and its affiliates (“TELIT”). The contents are confidential and any disclosure to persons other than the officers, employees, agents or subcontractors of the owner or licensee of this document, without the prior written consent of Telit, is strictly prohibited.

Telit makes every effort to ensure the quality of the information it makes available. Notwithstanding the foregoing, Telit does not make any warranty as to the information contained herein, and does not accept any liability for any injury, loss or damage of any kind incurred by use of or reliance upon the information.

Telit disclaims any and all responsibility for the application of the devices characterized in this document, and notes that the application of the device must comply with the safety standards of the applicable country, and where applicable, with the relevant wiring rules.

Telit reserves the right to make modifications, additions and deletions to this document due to typographical errors, inaccurate information, or improvements to programs and/or equipment at any time and without notice. Such changes will, nevertheless be incorporated into new editions of this application note.

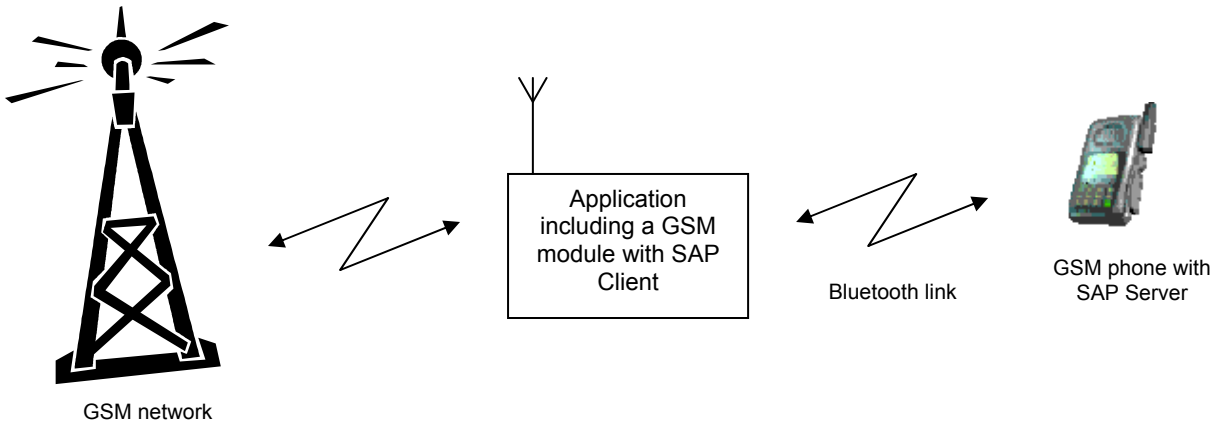
1 Introduction

1.1 Scope of document

The scope of the present document is to describe the Telit implementation of SAP (SIM Access Profile).

1.2 Using a remote SIM card

The SIM Access Profile (SAP) defines a protocol and related procedures that allow access to a remote SIM card through the serial port or, through an additional hardware, using Bluetooth. For instance, this feature allows the user to access the SIM of its handheld mobile phone, while using the car phone.
The basic system configuration includes a SAP Client implemented in the module, and SAP Server, implemented in the handheld phone. The SAP Server has the electrical access to the SIM and therefore it acts as a SIM card reader. It supports the SAP Client in accessing and controlling the SIM.
The SAP Client accesses the information and services contained in the SIM as if it was directly connected to SAP Client, in this case the GSM module. Therefore, this feature allows the registration of the module in the GSM network using all the subscription information stored in the SIM. It is also possible to access the phonebook and making a call from the SAP Client using the information held in the SIM.
This feature is available enabling a special AT Command on a virtual port of the CMUX interface.



2 Applicable documents

[1] Digital Cellular Telecommunications Systems (Phase 2+); AT Command set for GSM Mobile Equipment (ME); GSM 07.07 Version xxxx, Release xxxx

[2] Digital Cellular Telecommunications Systems (Phase 2+); Terminal Equipment to Mobile Station (TE-MS) "Multiplexer Protocol"; ETSI TS 101 369 V7.1.0 (1999-11), GSM 07.10 Version 7.1.0, Release 1999

[3] Digital Cellular Telecommunications Systems (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface; GSM 11.11 Version xxxx, Release xxxx

[4] CMUX Product Specification, Telit Communication SpA Document Id. 30268ST10299A

[5] Bluetooth SIG Specification: SIM Access Profile, Interoperability Specification ; Version 10, Release 00

3 Technical caracteristics

3.1 Product architecture

The SAP feature allows the module to use the SIM of a remote SIM Server. This feature is implemented using special AT Command on a Virtual circuit of the CMUX interface.

3.2 Implementation feature

- SAP is based on 7.10 CMUX Basic Option used
- SAP command are supported only on one User Selected virtual interface
- Only SAP Client features (defined as mandatory in Bluetooth specification) are supported
- Logic hardware flow control shall be used on the Virtual instance selected for the SAP command.

4 AT Command Description

4.1 Remote SIM Enable - #RSEN

#RSEN – Remote SIM Enable	
AT#RSEN=<mode>, **[<sapformat>],** **[<role>],** **[<muxch>],** **[<beacon>]**	Set command is used to enable/disable the Remote SIM feature. The command returns **ERROR** if requested on a non multiplexed interface Parameter: **<mode>** 0 - disable 1 - enable **<sapformat>** 0 - X-SAP (unsupported) 1 - binary SAP (default) **<role>** 0 - remote SIM Client (default) 1 - remote SIM Server (unsupported) **<muxch>** - MUX Channel Number; mandatory if **<mode>=1** and **<sapformat>=1** 1..3 **<beacon>** - retransmition timer of SAP Connection Request 0 - only one transmition (default) 1..100 - timer interval in seconds. NOTES: If the module has a SIM inserted, when it receives the enable Command: - de-register from the actual network - de-initialize the current SIM. NOTE for **<sapformat>=1** (binary SAP): while RSEN is activate SAP connection status is signalled with following URC: **#RSEN: <conn>** where **<conn>** - connection status 0 - disconnected 1 - connected
AT#RSEN?	Read command returns the connection status of Remote SIM feature
AT#RSEN=?	Test command returns all supported values of Remote SIM Enable command

5 Remote SIM Message Command Description

The module sends request commands to the client application through a binary message that is crowned in the CMUX message. The client application shall extract the message and send it to the SAP server, through the appropriate protocols (e.g. by RFCOMM, that is the Bluetooth serial port emulation entity).
The client application shall extract all the messages sent by SAP server and put them in the CMUX message, to sent to the module.

The module satisfies the following feature requirements:

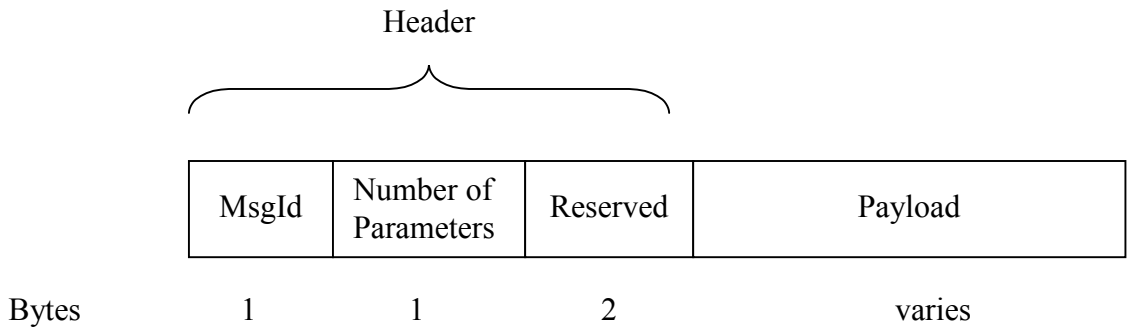
- Connection management
- Transfer APDU
- Transfer ATR
- Power SIM on
- Report Status
- Error Handling

Every feature needs some procedures support:

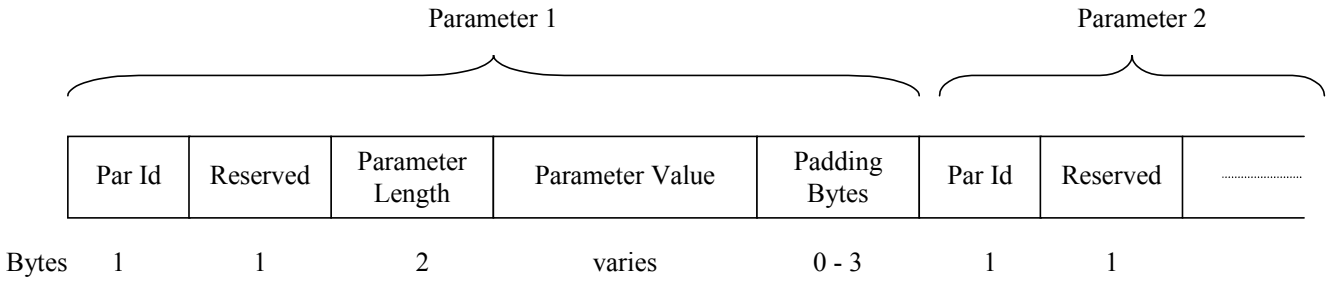
Feature	Procedure
Connection Management	Connect
	Report Status
	Transfer ATR
	Disconnection Initiated by the Client
	Disconnection Initiated by the Server
Transfer APDU	Transfer APDU
Transfer ATR	Transfer ATR
Power SIM on	Power SIM on
	Transfer ATR
Report Status	Report Status
Error Handling	Error Response

Report Status, Disconnection Initiated by the Server and Error Response are independent messages sent by server. The other procedures consist of couples of messages, started by client.

The format of the message is:



The message header consists of three fields. The number of parameters gives the parameters presented in the payload of the message. Each parameter is formatted as shown in the following figure:



The length of each parameter shall be a multiple of 4 bytes: some bytes are added after Parameter value, if needed.

Next table describes the messages sent by the Client (module).

Message Id	Message Description	Parameters Number	Parameter Value
0x00	Connection Request	1	Max Message Size
0x02	Disconnection Request	0	
0x05	Transfer APDU Request	1	APDU command
0x07	Transfer ATR Request	0	
0x0B	Power SIM on Request	0	

The server shall sent a response message after receiving a command message from the client. Moreover, it can send messages to indicate the SIM status, the will of disconnection and the presence of am invalid message from the Client.

Next table describes the message sent by the Server.

Message Id	Message Description	Parameters Number	Parameter Value
0x01	Connection Response	1 or 2	First Parameter is the connection status. The optional second parameter is the max message size supported by Server
0x03	Disconnection Response	0	
0x04	Disconnection Indication	1	Disconnection Type (Immediate type is the only supported)
0x06	Transfer APDU Response	1 or 2	First Parameter is the Result Code. Second parameter is the APDU message (present only if Result Code is OK)
0x08	Transfer ATR Response	1 or 2	First Parameter is the Result Code. Second parameter is the ATR message (present only if Result Code is OK)
0x0C	Power SIM on Response	1	Result Code
0x11	Status Indication	1	Remote Card Status
0x12	Error Response	0	

More details are available on [5].

6 Remote SIM Typical Activation Scenario

The AT command that is used to enable/disable the Remote SIM feature is AT#RSEN. Before issuing this command a multiplexed interface (CMUX) should be activated. In order to get more detailed information about CMUX please refer to the CMUX User Guide.

AT#RSEN=1,1,0,2,0 // Activate SAP
OK // SAP Connected

// On virtual COM 2
// → Connection Request with Max Message Size = 300

0x00	0x01	0x00	0x00	0x00	0x00	0x00	0x02	0x01	0x2C	0x00	0x00

// ← Connection Response: OK

0x01	0x01	0x00	0x00	0x01	0x00	0x00	0x01	0x00	0x00	0x00	0x00

…
…

#QSS: 1 // SIM is inserted

AT+CPIN? // Local SIM is Deactivated and Remote needs
+CPIN: SIM PIN // PIN
OK

AT+CPIN=1234
OK
#QSS: 2 // PIN Unlocked
...
...

#QSS: 3 // SIM READY (SMS and Phonebook access is possible)

7 Document Change Log

Revision	Date	Changes
ISSUE#0	23/03/07	Initial Release
ISSUE#1	04/09/07	updated applicability table
ISSUE#2	16/01/09	Updated applicability table with new P/Ns added GE863-SIM, GE863-PRO3 and GE864-QUAD Automotive