BLUETOOTH DOC	Date / Year-Month-Day 2008-12-18	Approved	Revision V11r00	Document No SAP_SPEC
Prepared Car WG	e-mail address Car-feedback@bluetooth.org			N.B.

SIM ACCESS PROFILE

Interoperability Specification

Abstract:

This document defines the features and procedures that are required for the SIM Access Profile. The scope of this profile includes the following layers/protocols/profiles: Bluetooth® Baseband, Link Manager Protocol, L2CAP, Service Discovery Protocol, Serial Port Profile and the Generic Access Profile.

Revision History

Revision	Date	Comments
0.1	08-Sep-00	First draft
0.2	29-Nov-00	Alignment with Specification Description; Procedures described in more detail; Comments from Raghunandan Sanjeev added.
0.3	29-Jan-01	Serial Port and Generic Access Control Profile Interoperability Requirements rewritten; Comments from J. Pulido added.
0.31	05-Feb-01	Comments from P. Breyer and K. Ulery added.
0.4	13-Mar-01	Features and Procedures reorganized: - "Transfer of PPS result" removed, - "Card Holder Type" extended to "Card Reader Status", - "Verify CHV" added, - "Server initiated SIM reactivate" added. Parameter list and Message coding added.
0.45	04-Apr-01	Comments from Bilbao face-to-face meeting added. Document reorganized for better readability.
0.49	16-Apr-01	Test Strategy added. Renaming from Remote Authentication Access to SIM Access Profile done. Message coding changed. Proposal for 0.5 version.
0.50 (preBARB)	28-May-01	Editorial changes after Car WG review Proposal for review by BARB
0.50	19-Jun-01	Editorial changes after BARB review
0.60	20-July-01	Changes in the procedures after discussion in the July 19th phone conference
0.61	30-July-01	All changes accepted; other comments from WG members added
0.65	01-August-01	Editorial changes in document: Connection setup and Status Report procedures modified
0.66	29-August-01	State Machine introduced Better definitions of ResultCode and StatusChange added Payload of ERROR_RESP simplified Byte ordering conventions added
0.69	14-Sept-01	Changes in Sections 7.3 Link Manager Interoperability Requirements and 7.4 Link Control Interoperability Requirements Protocol Stack (Section 2.1) and Message Example (Section 5.4) added Editorial changes in Sections 4.6 - 4.8 and 4.13
0.699	26-Sept-01	Changes after comments from Raghu and Michael
0.70	27-Sept-01	Document approved as 0.70 by the Car Working Group

0.80	20-Nov-01	Editorial changes: • Section "Profile Dependencies" moved from Section 2.1 to 1.2 • Editorial changes in Sections 1 and 2 Changes WRT. the features "Power SIM on/off", "Reset SIM" and "Transfer ATR".
0.81	17-Dec-01	Changes after review during San Francisco f-2-f meeting
0.90	21-Dec-01	Draft version for Working Group approval
0.90a	04-Jan-02	Further improvements of the 0.90 draft: "Power SIM off" procedure has been made optional
0.90b	10-Jan-02	Comments from Jesus Pulido on Rev. 0.90a incorporated
0.90c	01-Feb-02	Comments from BARB review incorporated
0.95VD	22-Mar-02	Voting Draft
0.95VD b	18-Apr-02	Voting Draft with changes in Security Section (2.5)
0.95VD c	16-May-02	Voting Draft with changes after BARB, BQRB and BTI review
0.95VD d	17-Sep-02	Updates to allow access to UICC as well
0.95VD e	03-Oct-02	Updated to use generic term for all cards; Updated to allow access to R-UIM also
0.95VD f	13-Nov-02	Changed generic term Module to Subscriber Module
1.00 VD	22-Dec-04	Voting Draft
D10r01	02-Feb-05	Updated for technical editing
D10r02	15-Feb-05	Updates after BARB review
V10r03	12-May-05	Adopted by the BoD
D11r04	30-Aug-07	Updates for core spec 2.1+EDR
D11r05	15-May-08	Update SDP version number and solution for spec errata 2564
D11r06	16-May-08	Updates for errata 2564
D11r07	28-May-08	Change profile dependency chart and address TB comments
D11r08-12	01-July-08	Minor corrections and comments addressed
D11	12-Dec-08	Prepare for publication.
V11r00	18-Dec-08	Adopted by the Bluetooth SIG Board of Directors

Contributors

Name	**Company**
Penny Breyer	Cambridge Silicon Radio Ltd.
Björn Bunte	Nokia Corp.
Lowell Campbell	Denso Corp.
Patrick Clauberg	Nokia Corp.
Christian Gehrmann	Ericsson Mobile Communications AB
Holger Krummel	Nokia Corp.
Holger Lenz	Berner & Mattner Systemtechnik GmbH
Tony Mansour	Motorola, Inc.

Ganesh Pattabiraman	Qualcomm Inc.
Jesus-Angel Gonzalez Pulido	Ericsson España, S.A.
Daniel S. Rokusek	Motorola, Inc.
Raghunandan Sanjeev	Motorola, Inc.
Burch Seymour	Continental Automotive Systems
Kazu Suzuki	Denso Corp.
Michael Svob	Motorola, Inc.
Yoichiro Takeuchi	Toshiba Corp.
Dmitri Toropov (owner)	Siemens AG
Patrick Reinelt	Siemens AG
Kreg Ulery	Agere Systems
Monica Wifvesson	Ericsson Mobile Communications AB
Joachim Mertz	Berner & Mattner

Disclaimer and Copyright Notice

The copyright in this specification is owned by the Promoter Members of *Bluetooth*® Special Interest Group (SIG), Inc. (“*Bluetooth* SIG”). Use of these specifications and any related intellectual property (collectively, the “Specification”), is governed by the Promoters Membership Agreement among the Promoter Members and *Bluetooth* SIG (the “Promoters Agreement”), certain membership agreements between *Bluetooth* SIG and its Adopter and Associate Members (the “Membership Agreements”) and the *Bluetooth* Specification Early Adopters Agreements (1.2 Early Adopters Agreements) among Early Adopter members of the unincorporated *Bluetooth* SIG and the Promoter Members (the “Early Adopters Agreement”). Certain rights and obligations of the Promoter Members under the Early Adopters Agreements have been assigned to *Bluetooth* SIG by the Promoter Members.

Use of the Specification by anyone who is not a member of *Bluetooth* SIG or a party to an Early Adopters Agreement (each such person or party, a “Member”), is prohibited. The legal rights and obligations of each Member are governed by their applicable Membership Agreement, Early Adopters Agreement or Promoters Agreement. No license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

Any use of the Specification not in compliance with the terms of the applicable Membership Agreement, Early Adopters Agreement or Promoters Agreement is prohibited and any such prohibited use may result in termination of the applicable Membership Agreement or Early Adopters Agreement and other liability permitted by the applicable agreement or by applicable law to *Bluetooth* SIG or any of its members for patent, copyright and/or trademark infringement.

THE SPECIFICATION IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, SATISFACTORY QUALITY, OR REASONABLE SKILL OR CARE, OR ANY WARRANTY ARISING OUT OF ANY COURSE OF DEALING, USAGE, TRADE PRACTICE, PROPOSAL, SPECIFICATION OR SAMPLE.

Each Member hereby acknowledges that products equipped with the *Bluetooth* technology ("*Bluetooth* products") may be subject to various regulatory controls under the laws and regulations of various governments worldwide. Such laws and regulatory controls may govern, among other things, the combination, operation, use, implementation and distribution of *Bluetooth* products. Examples of such laws and regulatory controls include, but are not limited to, airline regulatory controls, telecommunications regulations, technology transfer controls and health and safety regulations. Each Member is solely responsible for the compliance by their *Bluetooth* Products with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for their *Bluetooth* products related to such regulations within the applicable jurisdictions. Each Member acknowledges that nothing in the Specification provides any information or assistance in connection with securing such compliance, authorizations or licenses**. NOTHING IN THE SPECIFICATION CREATES ANY WARRANTIES, EITHER EXPRESS OR IMPLIED, REGARDING SUCH LAWS OR REGULATIONS.**

ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS OR FOR NONCOMPLIANCE WITH LAWS, RELATING TO USE OF THE SPECIFICATION IS EXPRESSLY DISCLAIMED. BY USE OF THE SPECIFICATION, EACH MEMBER EXPRESSLY WAIVES ANY CLAIM AGAINST *BLUETOOTH* SIG AND ITS PROMOTER MEMBERS RELATED TO USE OF THE SPECIFICATION.

Bluetooth SIG reserve the right to adopt any changes or alterations to the Specification as it deems necessary or appropriate.

Document Terminology

The Bluetooth SIG has adopted Section 13.1 of the IEEE Standards Style Manual, which dictates use of the words ``shall'', ``should'', ``may'', and ``can'' in the development of documentation, as follows:

- The word *shall* is used to indicate mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).
- The use of the word *must* is deprecated and shall not be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.
- The use of the word *will* is deprecated and shall not be used when stating mandatory requirements; *will* is only used in statements of fact.
- The word *should* is used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain course of action is deprecated but not prohibited (*should* equals *is recommended that*).
- The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted*).
- The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

Contents

1 Introduction

1.1 Scope

This SIM Access Profile defines the protocols and procedures that shall be used to access a GSM SIM card, a UICC card or an R-UIM card via a Bluetooth link. Unless otherwise specified the term “Subscription module” shall be used to refer to the GSM SIM card, a UICC card or an R-UIM card.

With the SIM Access Profile, the user can personalize his/her car-embedded phone with a subscription module in an external device, which is connected via a Bluetooth wireless link. The external device can either be a simple SIM card holder or a portable phone, which is brought into the car.

The SIM Access Profile builds on the well-defined interface between the telephone and a subscription module (see [3] and [6]). It also enables multiple card operations as defined in [4], [8] and [11].

1.2 Profile Dependencies

Figure 1.1 shows the Bluetooth profile structure and the dependencies of the profiles. A profile is dependent upon another profile if it re-uses parts of that profile, by implicitly or explicitly referencing it. Dependency is illustrated in the figure below: a profile has dependencies on the profile(s) in which it is contained directly or indirectly.

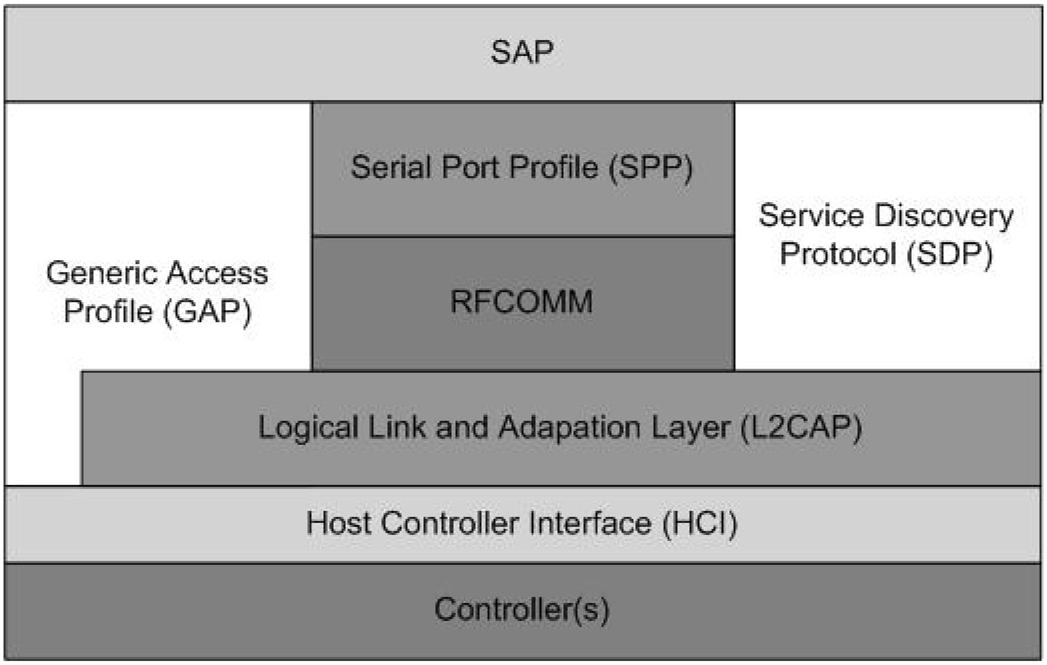
SAP
Serial Port Profile (SPP)
Generic Access Profile (GAP)
RFCOMM
Service Discovery Protocol (SDP)
Logical Link and Adapation Layer (L2CAP)
Host Controller Interface (HCI)
Controller(s)

Figure 1.1: Profile Dependencies

1.3 Symbols and Conventions

1.3.1 Requirement Status Symbols

In this document, the following symbols are used:

"M" for mandatory to support (used for capabilities that shall be used in the profile);

"O" for optional to support (used for capabilities that can be used in the profile);

"C" for conditional support (used for capabilities that shall be used in case a certain other capability is supported);

"X" for excluded (used for capabilities that may be supported by the unit but shall never be used in the profile if this is the only active profile);

"N/A" for not applicable (in the given context it is impossible to use this capability).

Some excluded capabilities are capabilities that, according to the relevant Bluetooth specification, are mandatory. These are features that may degrade operation of devices following this profile. Therefore, these features should not be activated while a unit is operating as a unit within this profile.

1.3.2 Signaling Diagram Conventions

The following arrows are used in diagrams describing procedures (see Figure 1.2):

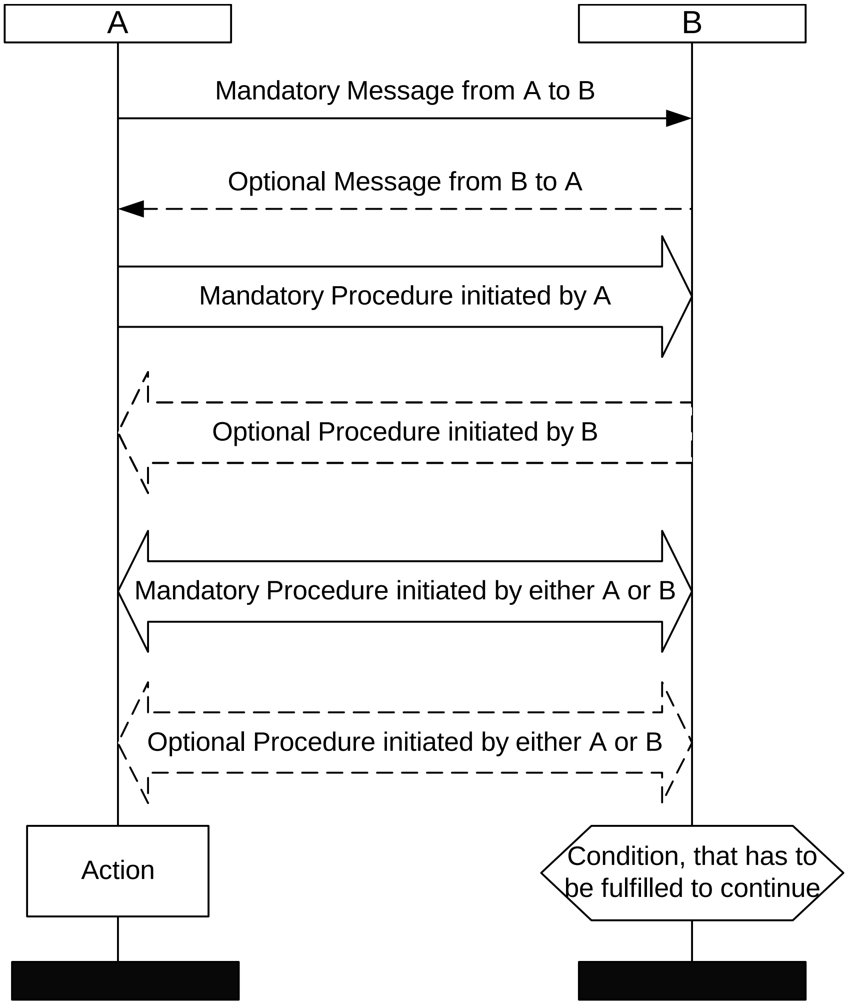
A
B
Mandatory Message from A to B
Optional Message from B to A
Mandatory Procedure initiated by A
Optional Procedure initiated by B
Mandatory Procedure initiated by either A or B
Optional Procedure initiated by either A or B
Action
Condition, that has to be fulfilled to continue

Figure 1.2: Arrows Used in Signaling Diagrams

1.1.1 Byte Ordering Convention

When multiple byte fields are contained in this specification, the standard network byte order (Big endian), with more significant (high-order) bytes being transferred before less-significant (low-order) bytes, is used.

2 Profile Overview

2.1 Profile Stack

Figure 2.1 shows the protocols and entities used in this profile.

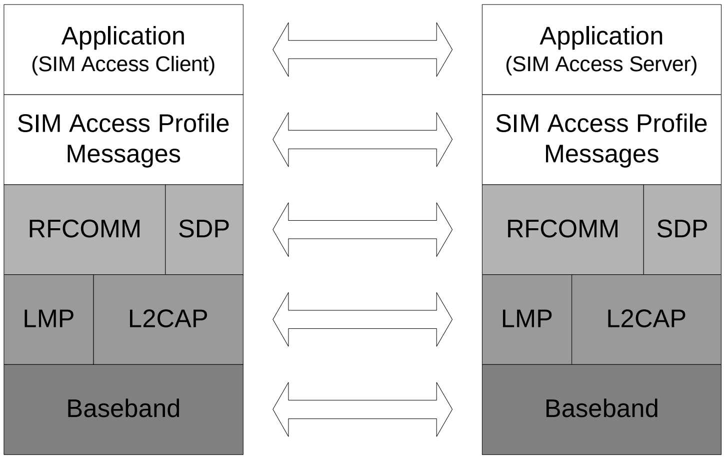

Figure 2.1: Protocol Stack

The Baseband, LMP and L2CAP are the OSI layer 1 and 2 Bluetooth protocols. RFCOMM is the Bluetooth serial port emulation entity. SDP is the Bluetooth Service Discovery Protocol. See [1] for more details on these topics.

The messages of the SIM Access Profile are defined in this document. It also contains the interoperability guidelines for the applications in the Client and Server.

2.2 Configuration and Roles

Figure 2.2 shows the basic system configuration, which is taken as a reference in this profile document:

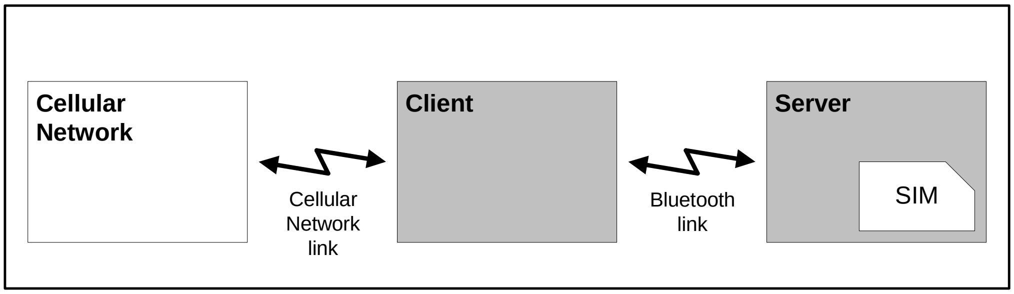

Figure 2.2: Basic System Configuration

The following two roles are defined for this profile:

Server—The SIM Access Server has direct (galvanic) access to a subscription module. It acts as a SIM card reader, which assists the Client in accessing and controlling the subscription module via the Bluetooth link.

Client —The SIM Access Client is connected via a Bluetooth link to the SIM Access Server. The Client accesses and controls the subscription module inside the Server via the Bluetooth link.

Typical examples of a Server are a simple SIM card holder or a portable phone in the car environment. A typical example of a Client is a car phone, which uses a subscription module in the Server for a connection to the cellular network.

Both the subscription module and the cellular network play an important role in the SIM Access Profile. However, the presence of either entity is not mandatory during the operation of the profile.

2.3 User Requirements and Scenarios

In general, the SIM Access Server functions as a SIM card reader for the SIM Access Client. The SIM Access Profile enables all scenarios that are also possible with wired SIM card readers.

Two scenarios are depicted here, as they serve as building blocks for other scenarios. Both scenarios will be referenced throughout the document.

2.3.1 Scenario 1: Subscription Module in the Server

As shown in Figure 2.2, the Server contains a Subscription Module, which is used by the Client. The Client accesses the files and services of the card subscription module as if the subscription module was directly contained in the Client or connected via a cable. For example, it is possible to

- Register the Client in the cellular network using the subscription information stored in the subscription module.
- Make a call from the Client using the subscription information stored in the subscription module.
- Use the Client to access phonebook data stored in the subscription module[1].

In this scenario, the ME-SIM interface (as specified in [3] and [6]) is extended over the Bluetooth link.

2.3.2 Scenario 2: Proactive SIM in the Client and Additional SIM in the Server

Figure 2.3 below shows a scenario, in which the Client contains a proactive subscription module. The Client uses this subscription module for connecting to the cellular network.

Furthermore, the proactive subscription module may request the Client to control the additional subscription module, which is located in the Server (see [4], [8] and [11]). For this purpose the SIM Access Profile provides the necessary means to perform all functions that are required by [4], [8] and [11]. For example, it is possible to

[1] While it is possible to access SIM-stored phonebook data using the SIM Access Profile, the Phone Book Access Profile (PBAP) is the preferred method.

- power the card in the Server on or off,
- reset the card in the Server or
- get the status of the card and the card reader (the Server).

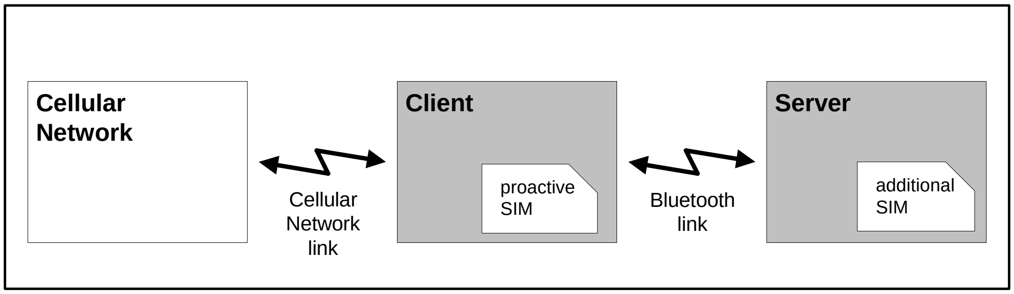

Figure 2.3: System Configuration with Proactive SIM in the Client

2.4 Profile Fundamentals

The SIM Access Profile describes the messages and procedures for accessing a subscription module over a Bluetooth link. It is especially designed for usage with:

- GSM SIM cards and provides a transport and remote control solution for GSM 11.11 [3] and GSM 11.14 [4].
- UICC cards and provides a transport and remote control solution for TS 102.221 [6], TS 31.102 [7] and TS 31.111 [8].
- R-UIM cards and provides a transport and remote control solution for TIA/EIA/IS-820 [9], TIA/EIA/IS-820-1 [10].

The SIM Access Server contains a subscription module and is responsible for establishing and maintaining the physical connection to the subscription module. The Server also acts as the mediator for all messages (APDUs) exchanged between the SIM Access Client and the subscription module. Furthermore, if the Client requests information from the Server about the subscription module or about the Server itself, the Server shall respond by sending the requested data over the Bluetooth link.

The Client is in most cases a phone, which behaves according to the relevant GSM, 3GPP or 3GPP2 specifications. This behavior is fully supported by the SIM Access Profile, by providing the necessary framework.

The Server might also be a phone, which apart from the SIM Access Profile functionality has the ability to use the subscription module for its own cellular network connection. According to the GSM, 3GPP and 3GPP2 specifications, this is only allowed, if the Server is outside of a SIM Access Profile connection (see Sections 4.1, 4.2 and 4.3 for details).

In general, the Server may establish a SIM Access Profile connection, even if there is no subscription module in the Server. Similarly, the Server may establish a connection, even if its subscription module is powered off. In order to handle these different situations, the Client shall be informed about the status of the subscription module during connection setup (see Sections 4.1 and 4.9).

The application of the profile is limited to one Server, which establishes a SIM Access Profile connection to one Client. Similarly, the Server shall only grant the Client access to a single GSM application, USIM application or an R-UIM application on a subscription module card in the context of this profile.

The Client initiates the connection to the Server and performs device discovery and paging. The Server therefore shall be discoverable and connectable according to the Generic Access Profile. See Section 8 for details.

2.5 Bluetooth Security

In order to ensure secure communication between Client and Server, several security measures from the Bluetooth specification are mandatory.

Bonding - Client and Server shall be bonded before setting up a SIM Access Profile connection. Security mode 2 or 3 is required for devices implementing the Bluetooth 2.0 + EDR, or earlier, specification. Security mode 4 is required for devices implementing the Bluetooth 2.1 + EDR, or later, specification. Details are given in Section 8.2.

Encryption - The link between Client and Server shall be encrypted using Bluetooth baseband encryption.

Server Initiated Authentication - The SIM Access Server shall always initiate the authentication procedure.

Link Keys – Only standard combination keys or authenticated combination keys shall be used for SIM Access Profile connections. This means that the ‘just works’ association model shall not be used with SAP as it results in an unauthenticated combination key and does not protect against man-in-the middle attacks. An implementation (client or server) shall support combination keys being changed at each new SIM Access Profile connection. An implementation should change the combination keys at each new SIM Access Profile connection. For increased security, this is encouraged.

Encryption Key Length - A SAP-enabled device shall support the maximum length encryption key as given in the Bluetooth specification. A connected pair of devices may use an encryption key smaller than the specification maximum when required by the laws of the country where the devices are being used, with the restriction that the length of the encryption key shall be at least 64 bits. For increased security, use of the maximum length is suggested.

PIN - When standard combination keys are used, the PIN shall have the length of 16 digits. Additionally, it is strongly recommended that the PIN satisfies the complexity requirements described in [12]. Fixed PINs shall not be used. When authenticated combination keys are used either a passkey or numerical comparison value shall be used depending on the I/O capabilities of the two devices. The length of this passkey or numerical comparison value shall be six digits. The Authentication_Requirements parameter shall be set to MITM Protection Required.

2.6 Conformance

If conformance to this profile is claimed, all capabilities indicated mandatory for this profile shall be supported in the specified manner (process mandatory). This also applies for all optional and conditional capabilities for which support is indicated. All mandatory capabilities, and optional and conditional capabilities for which support is indicated, are subject to verification as part of the Bluetooth qualification program.

3 Application Layer Features

Table 3.1 below shows the feature requirements made by this profile.

Item no.	Feature	Support in Client	Support in Server
1	Connection Management	M	M
2	Transfer APDU	M	M
3	Transfer ATR	M	M
4	Power SIM off	O	M
5	Power SIM on	M	M
6	Reset SIM	O	M
7	Report Status	M	M
8	Transfer Card Reader Status	O	M
9	Error Handling	M	M
10	Set Transport Protocol	O	O

Table 3.1: Application Layer Features

The features are defined in the following subclauses.

3.1 Feature Definitions

Connection Management—The ability to establish and terminate a SIM Access Profile connection between Client and Server.

An established SIM Access Profile connection is the prerequisite for all other features.

Transfer APDU—The ability to send APDUs (Application Protocol Data Units) over the Bluetooth link in both directions.

APDUs sent to the subscription module are called Command APDUs, while APDUs sent by the subscription module are called Response APDUs. Command APDUs and Response APDUs only occur as pairs, where each Command APDU is followed by a Response APDU. The APDU exchange shall always be initiated by the Client.

The format and content of the APDUs are defined in [3], [4] for CommandAPDU parameter, and in [12] for CommandAPDU7816 parameter (see Section 5.1.6).

Transfer ATR—The ability to send the content of the ATR (Answer to Reset) from the Server to the Client over the Bluetooth link.

The ATR shall be sent by the subscription module to the Server after the subscription module has been powered on or reset. It contains information about the interface provided by the subscription module and the services on the GSM SIM, the UICC or the R-UIM.

The format and content of the ATR are defined in [2].

Power SIM Off—The ability to power the subscription module off remotely.

This feature gives the Client a means to power the subscription module in Server off remotely. It is needed for the Application Toolkit[2] purposes as shown in Scenario 2 (Section 2.3.2).

Power SIM On—The ability to power the subscription module on remotely.

This feature gives the Client a means to power the subscription module in the Server on remotely. It is e.g. needed for Application Toolkit[2] purposes as shown in Scenario 2 (Section 2.3.2).

Reset SIM—The ability to reset the SIM remotely.

This feature gives the Client a means to reset the subscription module in the Server. It is e.g. needed for Application Toolkit[2], as shown in Scenario 2 (Section 2.3.2).

Report Status—The Server's ability to inform the Client about the status of the physical **connection** between the Server and the subscription module.

This feature enables the Client to react appropriately, if the subscription module is e.g. removed or inserted in the Server.

Transfer Card Reader Status—The ability to send the Card Reader Status from the Server to the Client over the Bluetooth link.

The card reader status contains some basic information about the Card Reader and the subscription module (for example, the size of the SIM or if the SIM is removable). This information is required for Application Toolkit[1] purposes as shown in Scenario 2 (Section 2.3.2) and specified in [4], [8] and [11].

Error Handling—The ability to handle invalid formatted messages.

If the Server receives an invalid formatted message from the Client, the Server shall send an appropriate error message (see Section 5.3).

Set Transport Protocol—The client's ability to request the use of another Transport Protocol than T=0 from the server.

The server shall reset the subscription module and switch to the desired protocol if supported by subscription module and Server.

The features "Power SIM off" and "Transfer Reader Status" are only applicable for Scenario 2 (Section 2.3.2). All other features are applicable for both Scenarios.

[2] Unless otherwise specified Application Toolkit shall refer to the SIM ATK as specified in [4], USAT as specified in [8] or CCAT as specified in [11] .

4 Procedures

This chapter describes the procedures for all features listed in the previous chapter. Each procedure consists of one or more messages that are exchanged between the SIM Access Client and Server.

Table 2 below maps each feature to the procedures used for that feature. It is mandatory to implement a procedure, if the respective feature is supported by the device.

Item no.	Feature	Procedure	Ref.
1	Connection Management	Connect Report Status Transfer ATR Disconnect Initiated by the Client Disconnect Initiated by the Server	4.1 4.9 4.5 4.2 4.3
2	Transfer APDU	Transfer APDU	4.4
3	Transfer ATR	Transfer ATR	4.5
4	Power SIM off	Power SIM off	4.6
5	Power SIM on	Power SIM on Transfer ATR	4.7 4.5
6	Reset SIM	Reset SIM Transfer ATR	4.8 4.5
7	Report Status	Report Status	4.9
8	Transfer Card Reader Status	Transfer Card Reader Status	4.10
9	Error Handling	Error Response	4.11
10	Set Transport Protocol	Set Transport Protocol	1.12

Table 4.1: Application Layer Feature to Procedure Mapping

4.1 Connect

In order to start the SIM Access Profile connection and negotiate important parameters adherent to the connection, the messages CONNECT_REQ, CONNECT_RESP, STATUS_IND, TRANSFER_ATR_REQ and TRANSFER_ATR_RESP are used as described below.

Before the Client may send a SIM Access Profile message to the Server, the two devices must have established an L2CAP and RFCOMM connection (see also Section 7).

After the RFCOMM connection is established, the Client may issue a CONNECT_REQ message to the Server. The Server shall answer with the CONNECT_RESP message[3]. These two messages may be repeated as described in Section 4.1.1 in order to negotiate the maximum message size to be deployed in the SIM Access Profile connection.

If the Server contains a subscription module that is already powered on, the Server shall ensure that the subscription module is in a well-defined state. This shall be done without affecting ongoing phone calls on the server device. The transport protocol which shall be internally used by the server is T=0. To change the transport protocol, the feature 'Set Transport Protocol' shall be used.

After the Server has sent the CONNECT_RESP message with the parameter "ConnectionStatus" set to "OK, Server can fulfill requirements" (see Section 5.2.2), it shall inform the Client about the status of its subscription module connection by sending the STATUS_IND message (see Section 4.9 for details).

If the message size negotiation succeeds, but the server cannot reset the SIM due to an ongoing call, the server shall send the CONNECT_RESP with the parameter "OK", ongoing call. The server shall reset the SIM card and send the STATUS_IND ("Card reset") message as soon as the call has been released.

If a subscription module is inserted in the Server and powered on (i.e. STATUS_IND message contains the parameter "Card reset"), the Client shall request the ATR of the subscription module with the TRANSFER_ATR_REQ message. If the T=0 protocol is not supported (i.e. STATUS_IND message contains the parameter "Card_not_accessible"), the Client may request the ATR of the subscription module with the TRANSFER_ATR_REQ message to retrieve information about protocols supported by the subscription module and use the Set Transport Protocol feature subsequently. In both cases the Server shall answer with the TRANSFER_ATR_RESP message as described in Section 4.5.

Figure 4.1 illustrates how the Client and Server connect successfully:

[3] If the Server does not respond to the Client after a period of time defined by the Client, the latter shall either re-send the CONNECT_REQ message or abort the connection establishment procedure.

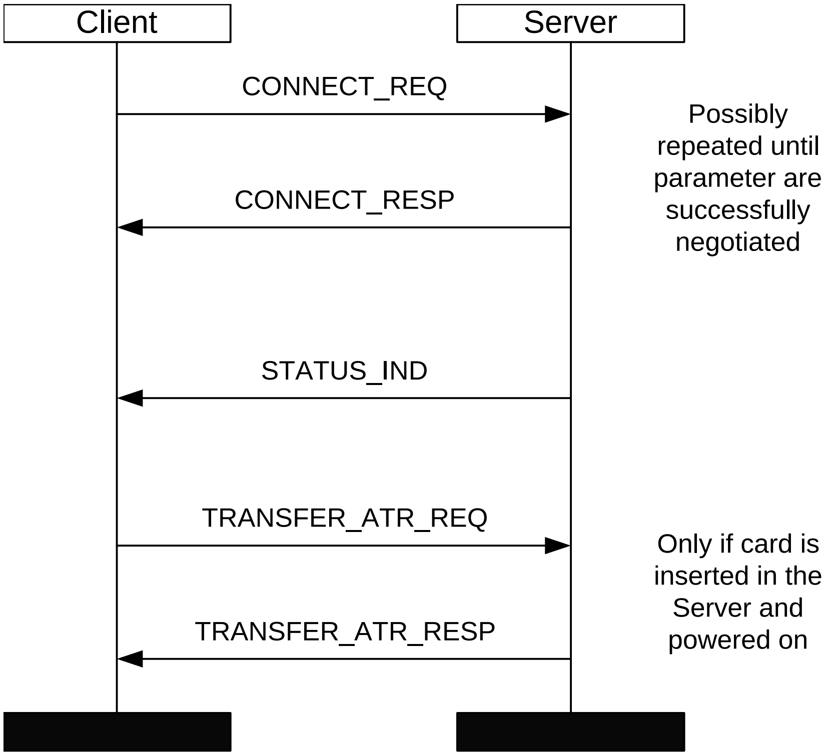
Client
Server
CONNECT_REQ
CONNECT_RESP
Possibly repeated until parameter are successfully negotiated
STATUS_IND
TRANSFER_ATR_REQ
TRANSFER_ATR_RESP
Only if card is inserted in the Server and powered on

Figure 4.1: Client Connecting to Server

The successful performance of the connection setup procedure is a precondition for all of the following procedures.

If the Server is unable to connect to the Client, it indicates this in the CONNECT_RESP message with the parameter "ConnectionStatus" set to "Error, Server unable to establish connection" (see Section 5.2.2). In this case, the SIM Access Profile connection between Client and Server is not established.

4.1.1 Negotiation of Profile Parameter

The CONNECT_REQ and CONNECT_RESP messages are also used to negotiate the maximum message size (parameter MaxMsgSize, see 5.2.1), that will be deployed in the SIM Access Profile connection.

First, the Client sends its MaxMsgSize value to the Server. If the Server supports this value, it shall set the parameter ConnectionStatus (see 5.2.2) in the CONNECT_RESP message to "OK, Server can fulfill requirements". If not, it shall set the ConnectionStatus to "Error, Server does not support message size" and includes its MaxMsgSize (i.e. a smaller value) in the CONNECT_RESP message.

In the latter case, it is up to the Client, if it sends another CONNECT_REQ message. This message shall then include the MaxMsgSize value proposed by the Server.

If the Client proposes a MaxMsgSize value, which the Server regards as too small, the Server shall set the "ConnectionStatus" parameter to "Error, maximum message size by Client is too small". In this case, the SIM Access Profile connection between the Client and the Server shall not be established.

4.2 Disconnect Initiated by the Client

If the Client wants to release the SIM Access Profile connection, it first shall terminate any existing GSM application session, USIM application session or R-UIM application session which involves the subscription module in the Server. The Client shall then send a DISCONNECT_REQ message to the Server.

The Server shall answer with a DISCONNECT_RESP message and the SIM Access Profile is successfully released.

After the disconnection of a SIM Access Profile connection, the Client shall immediately disconnect the corresponding RFCOMM data channel between the Client and the Server.

Note: After sending the DISCONNECT_RESP message, the Server may use the subscription module for another SIM Access Profile connection or for its own cellular network connection.

Figure 4.2 illustrates how the Client initiates a disconnect from the Server:

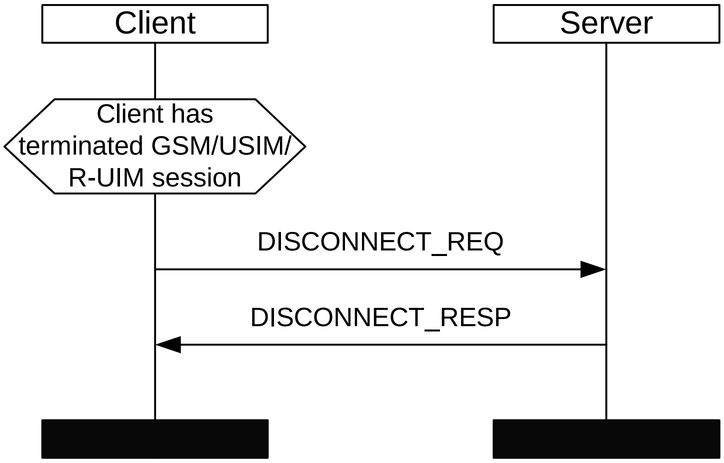

Figure 4.2: Client Disconnecting from Server (Initiated by the Client)

4.3 Disconnect Initiated by the Server

If the Server wants to release the SIM Access Profile connection, it shall send the DISCONNECT_IND message to the Client. Within this message the Server shall indicate if it wants to release the SIM Access Profile connection immediately or gracefully.

If the Server requests an immediate release, no more messages shall be exchanged and the SIM Access Profile connection shall be released directly after the

DISCONNECT_IND message. Furthermore, the Client immediately shall terminate any existing GSM application session, USIM application session or R-UIM application session in order to be compliant to the relevant GSM specifications, 3GPP specifications and 3GPP2 specifications. In this case the RFCOMM channel between the Client and the Server shall be immediately disconnected by the Server.

If the Server requests a graceful connection shutdown, a transfer of APDUs may occur before the Client terminates any existing GSM application session, USIM application session or R-UIM application session and sends the DISCONNECT_REQ message. Finally, the Server shall send a DISCONNECT_RESP message and the SIM Access Profile connection shall be released. Similar to the case of disconnect initiated by the Client, in case of graceful disconnection initiated by the Server the Client shall immediately disconnect the corresponding RFCOMM data channel between the Client and the Server.

If after graceful connection shutdown request from the Server certain amount of time (transmitted APDUs) elapsed and no DISCONNECT_REQ message was received from the Client, the Server may initiate an immediate disconnection by sending the DISCONNECT_IND message with DisconnectionType parameter set to immediate.

Figure 4.3 illustrates how the Server initiates a graceful disconnect from the Client. If an immediate disconnect is desired, the server shall send the DISCONNECT_IND message and end the connection.

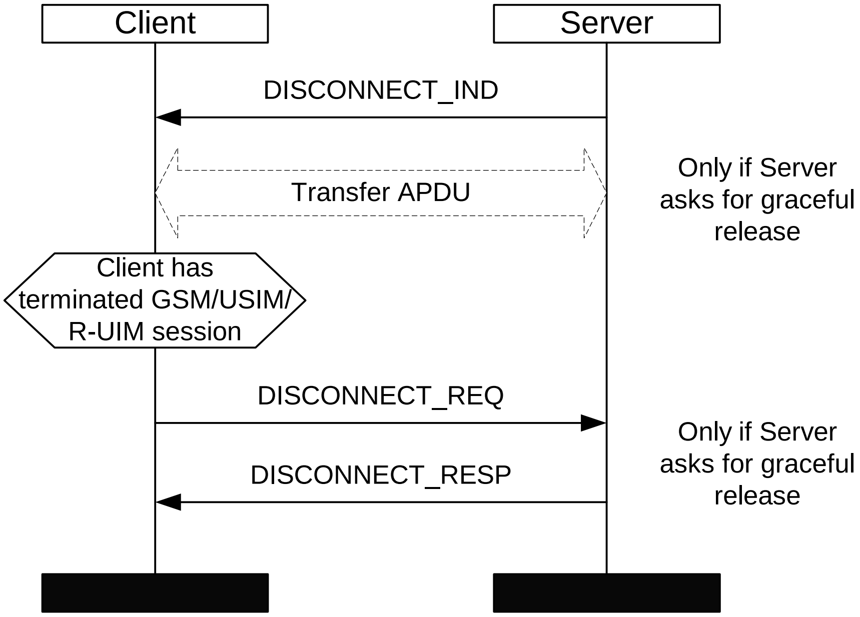
Client
Server
DISCONNECT_IND
Transfer APDU
Only if Server asks for graceful release
Client has terminated GSM/USIM/ R-UIM session
DISCONNECT_REQ
DISCONNECT_RESP
Only if Server asks for graceful release

Figure 4.3: Client Disconnecting Gracefully from Server (Initiated by the Server)

4.4 Transfer APDU

To transfer an APDU between the Client and the Server, the messages TRANSFER_APDU_ REQ and TRANSFER_APDU _RESP shall be used. ADPU transfers shall be initiated by the Client only.

Both messages contain an APDU (as defined for the GSM application in GSM 11.11 or GSM 11.14 and as defined in ISO/IEC 7816-4 for all other applications) in their payload. The message APDU_TRANSFER_REQ shall be used for Command-APDUs (from Client to the subscription module). The message TRANSFER_APDU_RESP shall be used for Response-APDUs (from the subscription module to the Client).

Figure 4.4 illustrates the successful exchange of APDUs between Client and Server:

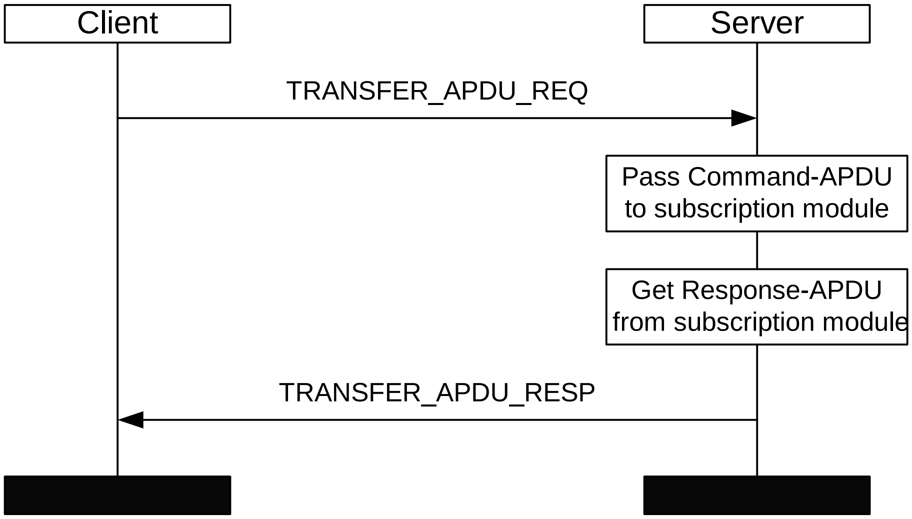
Client
Server
TRANSFER_APDU_REQ
Pass Command-APDU to subscription module
Get Response-APDU from subscription module
TRANSFER_APDU_RESP

Figure 4.4: APDU Transfer between Client and Server

If no error has occurred, the TRANSFER_APDU_RESP message shall contain the result code "OK, request processed correctly" (see Section 5.2.4). In case of an error, the TRANSFER_APDU_RESP message shall contain an appropriate result code (see also Section 5.2.4):

- If the card is removed from the Server, the result code "Error, card removed" shall be used.
- If the card is inserted in the Server but powered off, the result code "Error, card (already) powered off" shall be used.
- If the Server detects, that the card does not answer, the result code "Error, card not accessible" shall be used.

  NOTE: This is independent of the case in which the Client detects that the subscription module is not responding to; for example, Command APDUs.
- If an error has occurred that cannot adequately be described by any of the previous reasons, the result code "Error, no reason defined" shall be used.

4.5 Transfer ATR

The Client may request the Server to send the ATR from the subscription module. The TRANSFER_ATR_REQ message shall be used for this purpose. Following this request, the Server shall send the ATR to the Client in the payload of the TRANSFER_ATR_RESP message.

Figure 4.5 illustrates the successful ATR transfer:

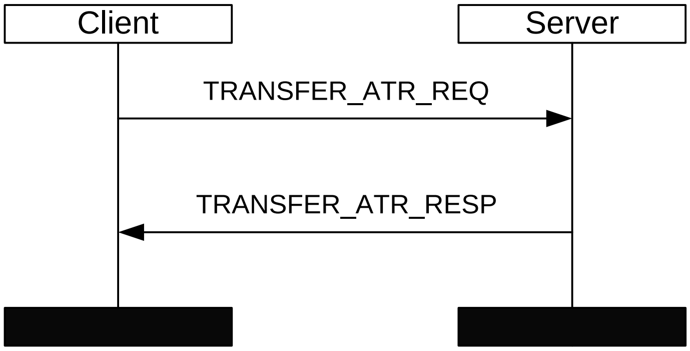

Figure 4.5: ATR Transfer between Client and Server

If no error has occurred, the TRANSFER_ATR_RESP message shall contain the result code "OK, request processed correctly." In case of an error, the TRANSFER_APDU_RESP message shall contain an appropriate result code (see Section 5.2.4):

- If the card is inserted in the Server but powered off, the result code "Error, card (already) powered off" shall be used.
- If the card is removed from the Server, the result code "Error, card removed" shall be used.
- If the Server cannot send the ATR for any other reason, the result code "Error, data not available" shall be used.

If an error has occurred, which cannot adequately be described by any of the previous reasons, the result code "Error, no reason defined" shall be used.

4.6 Power SIM Off

If the Client wants the Server to power off the subscription module, it first shall terminate any existing GSM application session, USIM application session, or R-UIM application session which involves the subscription module in the Server.

The Client may then send the POWER_SIM_OFF_REQ message to the Server. Upon receiving this message, the Server shall power off the subscription module; it removes the voltage from the card. Afterwards, the Server shall send the POWER_SIM_OFF_RESP message to the Client.

Figure 4.6 illustrates the successful case when the Client requests the Server to power off the subscription module:

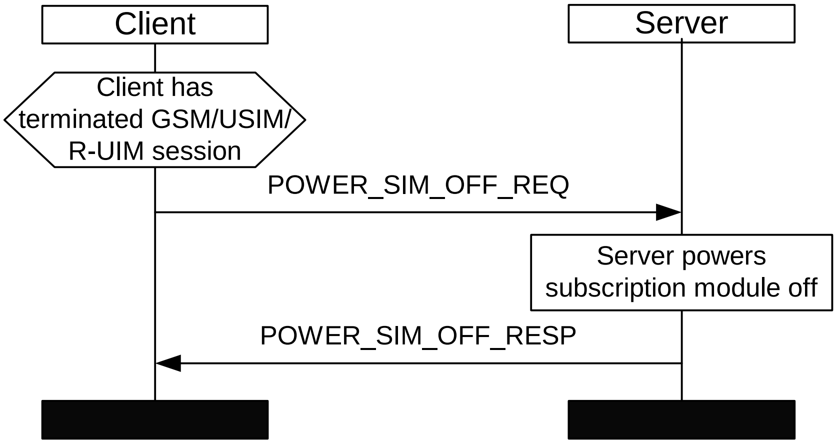
Client
Server
Client has terminated GSM/USIM/ R-UIM session
POWER_SIM_OFF_REQ
Server powers subscription module off
POWER_SIM_OFF_RESP

Figure 4.6: Client Requests Server to Power the SIM Off

If no error has occurred, the POWER_SIM_OFF_RESP message shall contain the result code "OK, request processed correctly" (see Section 5.2.4).

In case of an error, the POWER_SIM_OFF_RESP message shall contain an appropriate result code (see also Section 5.2.4):

- If the card is already powered off, the result code "Error, card (already) powered off" shall be used.
- If the card is removed from the Server, the result code "Error, card removed" shall be used.

If an error has occurred, which cannot adequately be described by any of the previous reasons, the result code "Error, no reason defined" shall be used.

4.7 Power SIM On

If a subscription module is powered off, the Client may request the Server to power it on again; to apply the supply voltage and clock signal to the subscription module. The POWER_SIM_ON_REQ message shall be used for this purpose.

Upon receiving this message, the Server powers the subscription module on. The transport protocol which shall be internally used by the server is T=0. To change the transport protocol, the feature ‘Set Transport Protocol’ shall be used. After this has been completed, the Server shall send the POWER_SIM_ON_RESP message to the Client.

If the POWER_SIM_ON_RESP message indicates that the subscription module was powered on successfully (see below), the Client shall request the ATR of the subscription module with the TRANSFER_ATR_REQ message. If the POWER_SIM_ON_RESP message indicates that the SIM doesn’t support the T=0 protocol (see below), the Client may request the ATR of the subscription module with the TRANSFER_ATR_REQ message to retrieve information about the subscription module. In both cases the Server shall answer with the TRANSFER_ATR_RESP message as described in Section 4.5.

Figure 4.7 illustrates the successful case when the Client requests the Server to power on the subscription module:

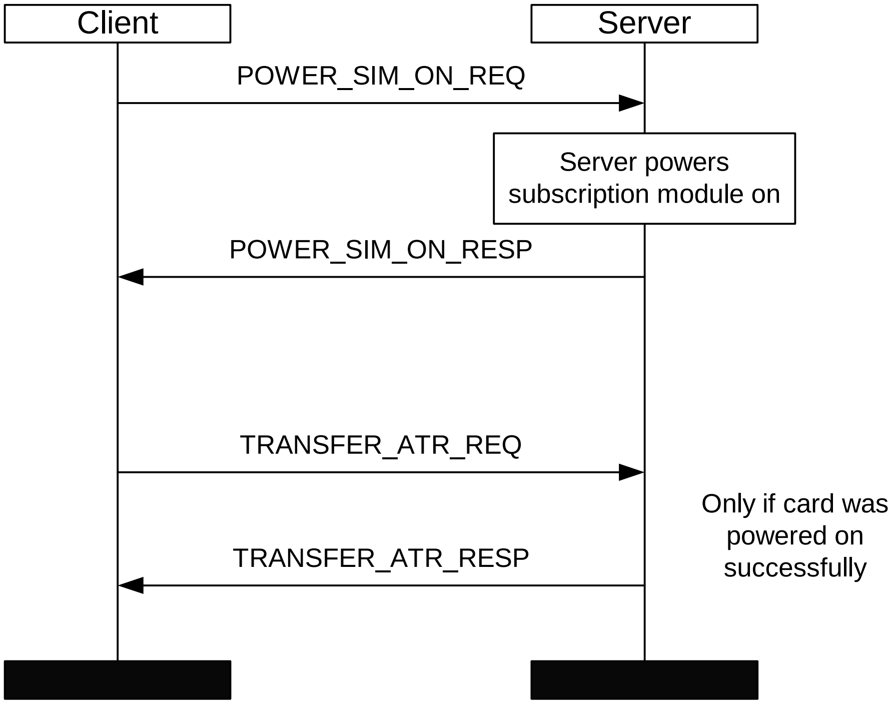

Figure 4.7: Client Requests Server to Power the SIM On

If no error has occurred, the POWER_SIM_ON_RESP message shall contain the result code "OK, request processed correctly" (see Section 5.2.4).

In case of an error, the POWER_SIM_ON_RESP message shall contain an appropriate result code (see also Section 5.2.4):

- If the card is removed from the Server, the result code "Error, card removed" shall be used.
- If the card is inserted in the Server but either cannot be powered on or the T=0 protocol is not supported, the result code "Error, card not accessible" shall be used.
- If the card is inserted in the Server but already powered on, the result code "Error, card (already) powered on" shall be used. In this case, the Server shall neither reset nor power on the card again.
- If an error has occurred, which cannot adequately be described by any of the previous reasons, the result code "Error, no reason defined" shall be used.

4.8 Reset SIM

If the Client wants the Server to reset the subscription module, it first shall terminate any existing GSM application session, USIM application session or R-UIM application session, which involves the subscription module in the Server.

The Client may then send the RESET_SIM_REQ message to the Server. Upon receiving this message, the Server shall reset the subscription module. The transport protocol which shall be internally used by the server is T=0. To change the transport protocol, the feature ‘Set Transport Protocol’ shall be used. After this has been completed, the Server shall send the RESET_SIM_RESP message to the Client.

If the RESET_SIM_RESP message indicates that the subscription module was reset successfully (see below), the Client shall request the ATR of the subscription module with the TRANSFER_ATR_REQ message. If the RESET_SIM_RESP message indicates that the subscription module doesn’t support the T=0 protocol (see below), the Client may request the ATR of the subscription module with the TRANSFER_ATR_REQ message to retrieve information about the subscription module. In both cases the Server shall answer with the TRANSFER_ATR_RESP message as described in Section 4.5.

Figure 4.8 illustrates the successful case when the Client requests the Server to reset the subscription module:

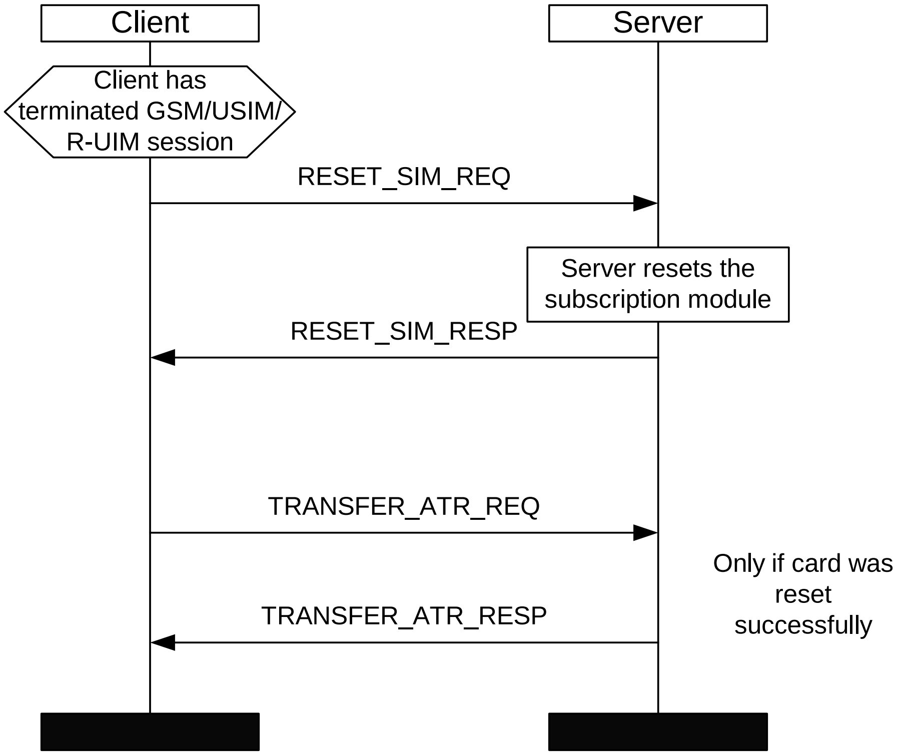
Client
Server
Client has terminated GSM/USIM/ R-UIM session
RESET_SIM_REQ
Server resets the subscription module
RESET_SIM_RESP
TRANSFER_ATR_REQ
Only if card was reset successfully
TRANSFER_ATR_RESP

Figure 4.8: Client Requests the Server to Reset the SIM

If no error has occurred, the RESET_SIM_RESP message shall contain the result code "OK, request processed correctly" (see Section 5.2.4).

In case of an error, the RESET_SIM_RESP message shall contain an appropriate result code (see also Section 5.2.4):

- If the card is removed from the Server, the result code "Error, card removed" shall be used.
- If the card is inserted in the Server but either cannot be reset or the T=0 protocol is not supported, the result code "Error, card not accessible" shall be used.
- If the card is inserted in the Server and powered off, the result code "Error, card (already) powered off" shall be used. In this case, the Server shall not perform any actions, such as powering on the card.

If an error has occurred, which cannot adequately be described by any of the previous reasons, the result code "Error, no reason defined" shall be used.

4.9 Report Status

This procedure is deployed during the connection setup phase (see Section 4.1) or whenever a change in the physical connection between Server and SIM occurs. The STATUS_IND message is used to inform the Client about the status or the status change.

During the connection setup phase (see Section 4.1) three alternatives are possible:

- A subscription module is inserted in the Server and has been powered on or reset prior to the SIM Access Profile connection or after releasing an ongoing phone call. In this case, the STATUS_IND message has the parameter "Card_reset."
- A subscription module is inserted in the Server, but cannot be powered on, is not accessible, or doesn’t support the default T=0 protocol. In this case, the STATUS_IND message has the parameter "Card_not_accessible."
- No subscription module is inserted in the Server. In this case, the STATUS_IND message has the parameter "Card_removed."

During an ongoing connection, the following changes in the subscription module status can occur:

- The subscription module is removed from the Server. In this case, the STATUS_IND message with the parameter "Card_removed" shall be sent.
- A subscription module is inserted in the Server. In this case, the STATUS_IND message with the parameter "Card_inserted" shall be sent. If the Client wants to take the subscription module into use, it has to power it on.
- While the subscription module remains inserted in the Server, the physical contact between Server and the subscription module can be lost. In this case, the message STATUS_IND with the parameter "Card_not_accessible" shall be sent.
- If a non-accessible card can be made accessible again, the Server shall power the card on. After that, the Server shall send the STATUS_IND message with the parameter “Card_recovered.”

All of the above cases are independent from those cases, in which the Client detects, that the subscription module is not responding to e. g. Command APDUs. In any case, the behavior of the Client shall be in line with the GSM specifications 3GPP specifications and 3GPP2 specifications [3], [4], [6], [7], [8], [9], [10], and [11].

Figure 4.9 illustrates the case when the Server detects a change in the physical connection to the card:

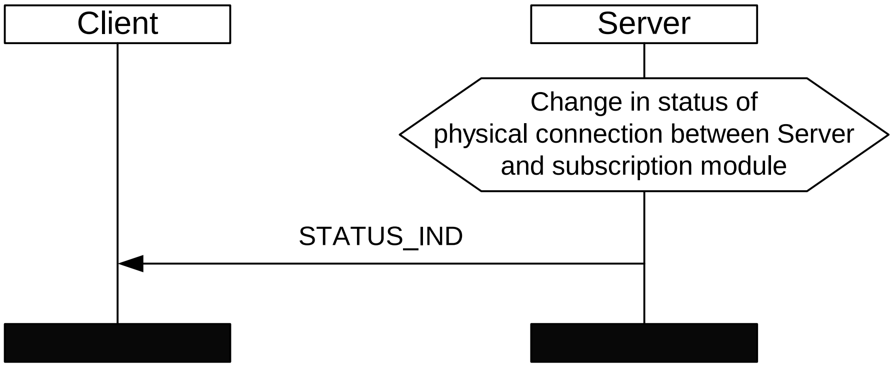
Client
Server
Change in status of physical connection between Server and subscription module
STATUS_IND

Figure 4.9: Server Reports Status Change to the Client

Please note, that the STATUS_IND message shall not be used in conjunction with a status change due to a POWER_SIM_OFF_REQ, POWER_SIM_ON_REQ or RESET_SIM_REQ message.

4.10 Transfer Card Reader Status

The Client may ask the Server to return the Card Reader Status using the TRANSFER_CARD_READER_STATUS_REQ message. Following this request, the Server shall send the Client the Card Reader Status in the TRANSFER_CARD_READER_STATUS_RESP message.

Figure 4.10 shows the allowed signaling flow when the Client requests the Card Reader Status from the Server:

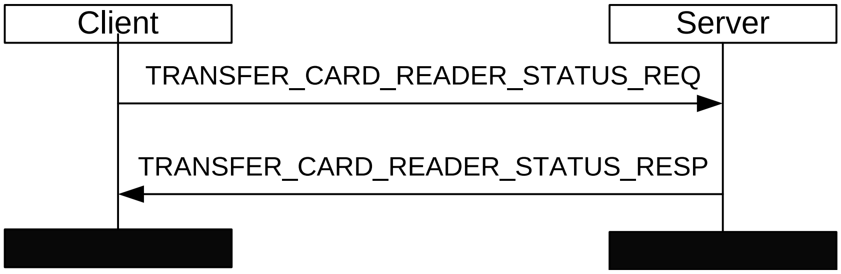
Client
Server
TRANSFER_CARD_READER_STATUS_REQ
TRANSFER_CARD_READER_STATUS_RESP

Figure 4.10: Request Card Reader Status

If no error has occurred, the TRANSFER_CARD_READER_STATUS_RESP message shall contain the result code "OK, request processed correctly" (see Section 5.2.4). In case of an error, the TRANSFER_CARD_READER_STATUS_RESP message shall contain an appropriate result code (see also Section 5.2.4):

If the Server cannot send the Card Reader Status for any other reason, the result code "Error, data not available" shall be used.

If any other error has occurred, the result code "Error, no reason defined" shall be used.

4.11 Error Response

The Server shall send an Error Response message ERROR_RESP to the Client whenever it has received a request message from the Client, which was invalid or improperly formatted (see Figure 4.11).

The Client may close the SIM Access Profile Connection after it has received an ERROR_RESP message from the Server.

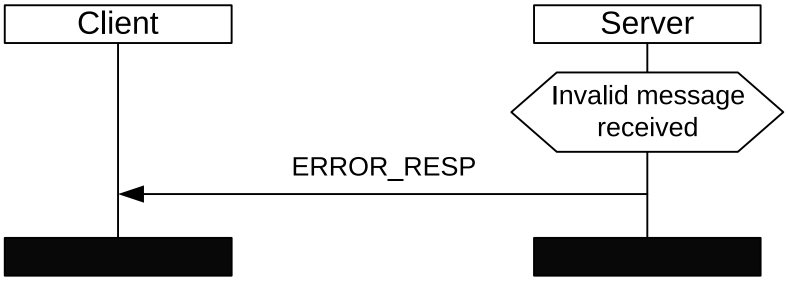

Figure 4.11: Error Response Message

In all cases, where an error occurred while processing a valid and properly formatted request, the error shall be indicated in the respective response message (for example, TRANSFER_APDU_RESP).

1.12 Set Transport Protocol

If the server supports the T=0 protocol, it shall be used as a default protocol (see sections 4.1, 4.7, 4.8). If the server or the subscription module do not support T=0, then the initial STATUS_IND after the CONNECT_RESP shall contain the status “Card not accessible”. The mechanisms described in this chapter shall then be used to select an appropriate protocol.

The client may change the transport protocol, by first terminating any existing GSM application session, USIM application session or R-UIM application session, which involves the subscription module in the Server.

The client shall then send the SET_TRANSPORT_PROTOCOL_REQ with a parameter that specifies the transport protocol which the client wants to use.

If the command is supported by the server, the server shall respond with SET_TRANSPORT_PROTOCOL_RESP and status “OK, request processed correctly”. The server shall then internally perform a reset of the subscription module and issue a STATUS_IND with the status “Card reset”. The client shall then continue with TRANSFER_ATR_REQ.

If the command is supported by the server, but the subscription module does not support the selected transport protocol, the status of the STATUS_IND shall be “Card not accessible”. The client may then send the TRANSFER_ATR_REQ to retrieve information about the subscription module.

If the command is supported by the server, but the required transport protocol is not supported by the server, the server shall respond with the error code “Error, not supported” in the SET_TRANSPORT_PROTOCOL_RESP. Before the subscription module can be accessed again, another SET_TRANSPORT_PROTOCOL_REQ is needed.

If the server does not support the command, it shall respond with ERROR_RESP as described in Section 4.11.

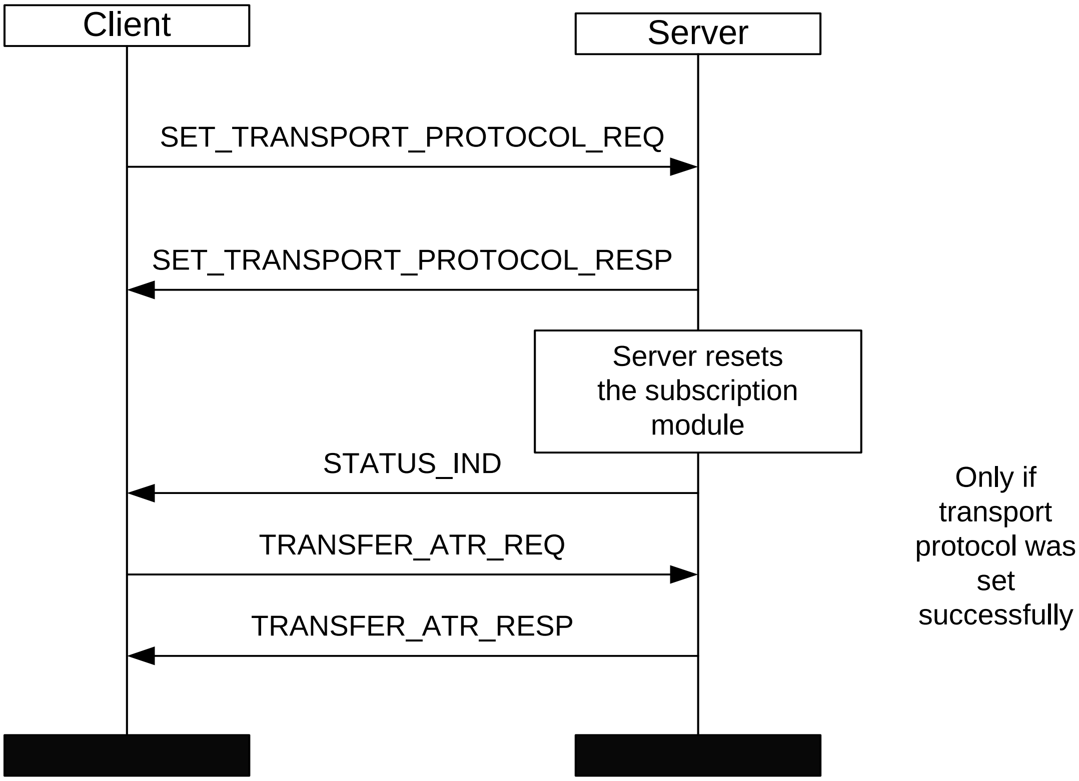
Client
Server
SET_TRANSPORT_PROTOCOL_REQ
SET_TRANSPORT_PROTOCOL_RESP
Server resets the subscription module
STATUS_IND
TRANSFER_ATR_REQ
TRANSFER_ATR_RESP
Only if transport protocol was set successfully

Figure 4.12: Set transport protocol

4.12 State Machine

Figure 4.13 shows the simplified state machine underlying the SIM Access Profile. The three main states are "Not connected", "Connection under negotiation" and "Connected". Within the "Connected" state, several sub-states exist.

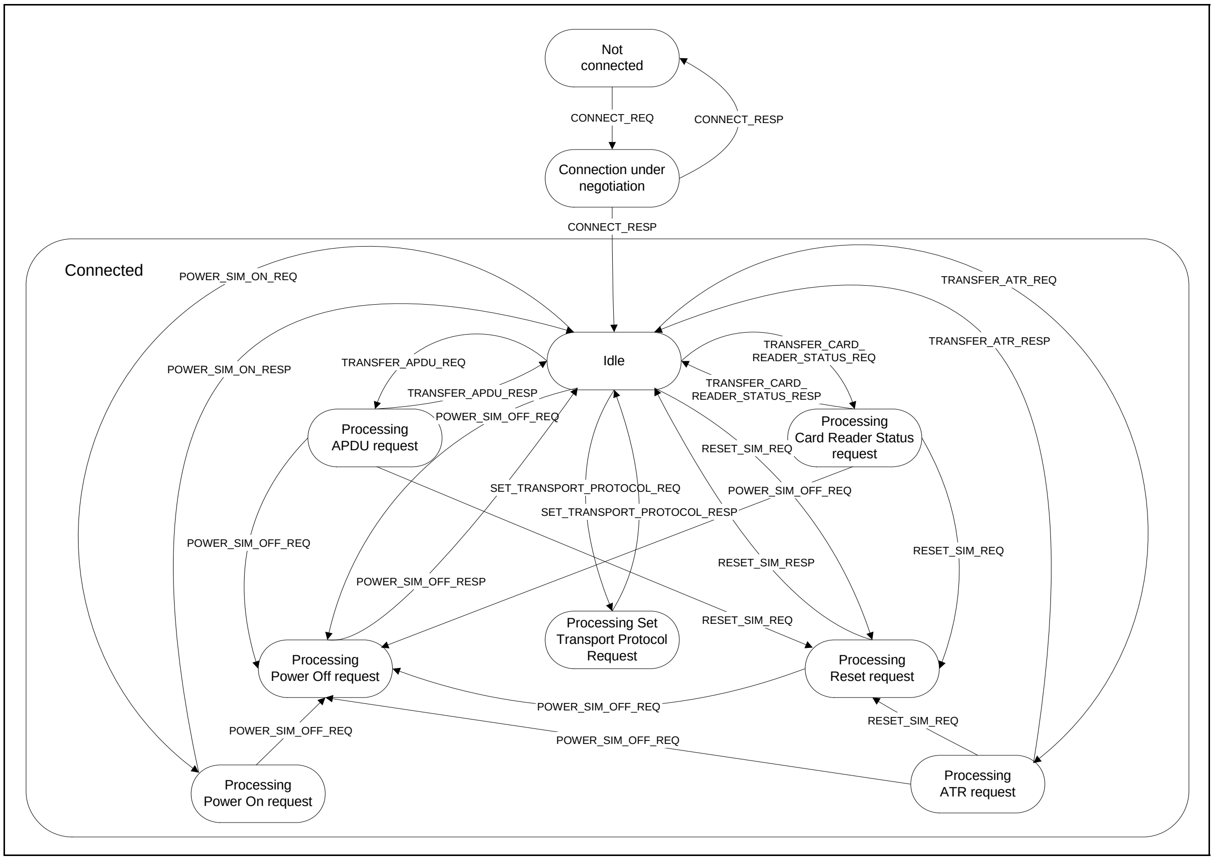

Figure 4.13: Simplified State Machine

As it can be seen from the state machine, each request message (e. g. TRANSFER_APDU_REQ) can in general only be followed by the corresponding response message (TRANSFER_APDU_RESP). However, there are two exceptions. The POWER_SIM_OFF_REQ and RESET_SIM_REQ can be sent in nearly any state, in order to allow the Client to reactivate a not accessible subscription module card.

For simplicity reasons, the messages DISCONNECT_REQ, DISCONNECT_IND, DISCONNECT_RESP, STATUS_IND and ERROR_RESP are not included in the figure. The usage of these messages is as follows:

- The DISCONNECT_REQ, DISCONNECT_IND (and DISCONNECT_RESP) messages may be sent in any of the sub-states of the "Connected" state. After Client and Server have disconnected as described in Sections 4.2 and 4.3, the new state is "Not connected."
- The STATUS_IND message may be sent in any of the sub-states of the "Connected" state. After that, the new state is "Idle."
- The ERROR_RESP message replaces - when necessary - any other response message. If the previous state was "Connection under negotiation", the new state is "Not connected". In all other cases, the new state is "Idle."

4.13 Bluetooth Link Loss

The Server or the Client can detect a Bluetooth link loss. Whenever either device detects a Bluetooth link loss, the SIM Access Profile connection shall be terminated by that device.

5 Message and Parameters

This chapter describes the coding and formats of the messages and parameters of the SIM Access Profile. The SIM Access Profile messages are transported on an RFCOMM link.

5.1 Message Formats

Messages are formatted as shown in Figure 5.1 (length of each field is given in bytes):

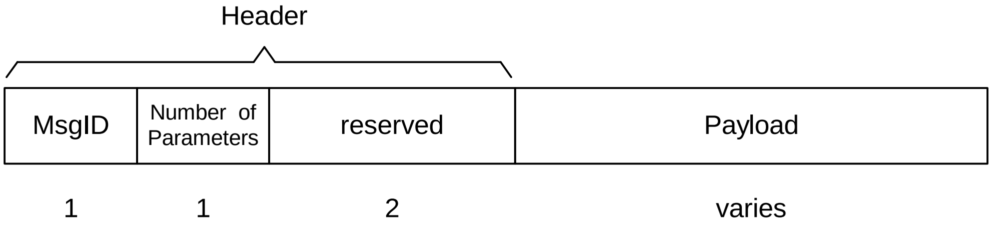

Figure 5.1: Message Format

The message header consists of three fields. The field "MsgID" contains the message ID as given in Section 1.13. The field "Number of Parameters" gives the number of parameters in the payload of the message.

Two bytes are reserved for future use and shall be set to 0x0000 until otherwise specified in future revisions of the SIM Access Profile.

The payload itself contains the parameters as listed in the following Sections. Each Parameter is formatted as shown in

Figure 5.2 using three fields:

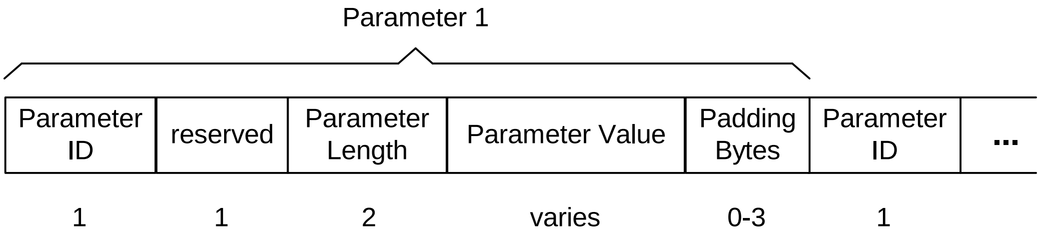

Figure 5.2: Payload Coding

The fields "Parameter ID", "Parameter Length", "Parameter Value", the reserved field and the "Padding Bytes" are repeated for each parameter. The ordering of the parameters shall be as listed in the tables in Section 1.13.

The reserved field and the padding bytes shall be set to 0x00 until otherwise specified in future revisions of the SIM Access Profile.

The "Parameter ID" shall contain the ID of the parameter as listed in Section 5.2. The "Parameter Length" field gives the length of the "Parameter Value" (see Section 5.2).

The length of each Parameter shall be a multiple of four bytes. Therefore, one to three additional bytes have to be added directly after the "Parameter Value".

1.13 Message Coding

This section defines the allowed messages in the SIM Access Profile. It is mandatory to implement a message, if the respective procedure is supported by the device.

Message	Direction	Msg ID
CONNECT_REQ	Client -> Server	0x00
CONNECT_RESP	Server -> Client	0x01
DISCONNECT_REQ	Client -> Server	0x02
DISCONNECT_RESP	Server -> Client	0x03
DISCONNECT_IND	Server -> Client	0x04
TRANSFER_APDU_REQ	Client -> Server	0x05
TRANSFER_APDU_RESP	Server -> Client	0x06
TRANSFER_ATR_REQ	Client -> Server	0x07
TRANSFER_ATR_RESP	Server -> Client	0x08
POWER_SIM_OFF_REQ	Client -> Server	0x09
POWER_SIM_OFF_RESP	Server -> Client	0x0A
POWER_SIM_ON_REQ	Client -> Server	0x0B
POWER_SIM_ON_RESP	Server -> Client	0x0C
RESET_SIM_REQ	Client -> Server	0x0D
RESET_SIM_RESP	Server -> Client	0x0E
TRANSFER_CARD_READER_STATUS_REQ	Client -> Server	0x0F
TRANSFER_CARD_READER_STATUS_RESP	Server -> Client	0x10
STATUS_IND	Server -> Client	0x11
ERROR_RESP	Server -> Client	0x12
SET_TRANSPORT_PROTOCOL_REQ	Client -> Server	0x13
SET_TRANSPORT_PROTOCOL_RESP	Server -> Client	0x14

Table 5.1: Message Overview

5.1.1 CONNECT_REQ

The CONNECT_REQ message contains the following parameter:

Parameter	Ref.	Status
MaxMsgSize	5.2.1	M

Table 5.2: Parameter of the CONNECT_REQ Message

The parameter MaxMsgSize shall be used by the Client and Server to negotiate the value that is to be used for the SIM Access Profile connection (see Section 4.1.1).

5.1.2 CONNECT_RESP

The CONNECT_RESP message contains the following parameters:

Parameter	Ref.	Status
ConnectionStatus	5.2.2	M
MaxMsgSize	5.2.1	C (ConnectionStatus)

Table 5.3: Parameters of the CONNECT_RESP Message

The parameter ConnectionStatus shall indicate, if the Server can fulfill the capability proposed by the Client. It shall also indicate if the Server is unable to connect to the Client.

If the Server cannot fulfill the requested capability, the parameter MaxMsgSize shall contain the value that is supported by the Server. Details are described in Section 4.1.1.

5.1.3 DISCONNECT_REQ

The DISCONNECT_REQ message contains no parameter.

5.1.4 DISCONNECT_RESP

The DISCONNECT_RESP message contains no parameter.

5.1.5 DISCONNECT_IND

The DISCONNECT_IND message contains the following parameter:

Parameter	Ref.	Status
DisconnectionType	5.2.3	M

Table 5.4: Parameter of the DISCONNECT_IND Message

The Disconnect Type shall indicate if the Server wants to shutdown the SIM Access Profile connection gracefully or immediately.

5.1.6 TRANSFER_APDU_REQ

The TRANSFER_APDU_REQ message contains the following parameters:

Parameter	Ref.	Status
CommandAPDU	5.3.5	C1
CommandAPDU7816	5.3.5	C1

Table 5.5: Parameter of the TRANSFER_APDU_REQ Message

C1: The TRANSFER_APDU_REQ message shall always contain exactly one of the CommandAPDU or the CommandAPDU7816 parameters.

If the device implementing the SAP server is GSM-capable, the support of the CommandAPDU parameter is mandatory for the server, otherwise optional. If the client implements the GSM application, the support of the CommandAPDU parameter is mandatory for the client, otherwise optional.

The support of the CommandAPDU7816 parameter is optional for the client[4] and is mandatory for the server.

5.1.7 TRANSFER_APDU_RESP

The TRANSFER_APDU_RESP message contains the following parameters:

Parameter	Ref.	Status
ResultCode	5.2.4	M
ResponseAPDU	5.2.5	C (ResultCode)

Table 5.6: Parameter of the TRANSFER_APDU_RESP Message

The parameter ResultCode shall indicate if the Command APDU was processed correctly. Any error response from the subscription module interface to the Server is mapped onto this field.

The parameter ResponseAPDU shall be included only if the Command APDU was processed correctly and no other error occurred.

5.1.8 TRANSFER_ATR_REQ

The TRANSFER_ATR_REQ message contains no parameter.

5.1.9 TRANSFER_ATR_RESP

The TRANSFER_ATR_RESP message contains the following parameters:

Parameter	Ref.	Status
ResultCode	5.2.4	M
ATR	5.2.6	C (ResultCode)

Table 5.7: Parameters of the TRANSFER_ATR_RESP Message

The parameter ResultCode includes possible error codes.

The parameter ATR includes the Answer to Reset from the subscription module. It shall be included only if no error has occurred.

5.1.10 POWER_SIM_OFF_REQ

The POWER_SIM_OFF_REQ message contains no parameter.

[4] It is recommended for the SIM Access Profile 1.x compliant client implementations to support the CommandAPDU7816 parameter.

5.1.11 POWER_SIM_OFF_RESP

The POWER_SIM_OFF_RESP message contains the following parameter:

Parameter	Ref.	Status
ResultCode	5.2.4	M

Table 5.8: Parameter of the POWER_SIM_OFF_RESP Message

The parameter ResultCode includes possible error codes.

5.1.12 POWER_SIM_ON_REQ

The POWER_SIM_ON_REQ message contains no parameter.

5.1.13 POWER_SIM_ON_RESP

The POWER_SIM_ON_RESP message contains the following parameter:

Parameter	Ref.	Status
ResultCode	5.2.4	M

Table 5.9: Parameter of the POWER_SIM_ON_RESP Message

The parameter ResultCode includes possible error codes and shall indicate, if the subscription module was powered on successfully.

5.1.14 RESET_SIM_REQ

The RESET_SIM_REQ message contains no parameter.

5.1.15 RESET_SIM_RESP

The RESET_SIM_RESP message contains the following parameter:

Parameter	Ref.	Status
ResultCode	5.2.4	M

Table 5.10: Parameter of the RESET_SIM_RESP Message

The parameter ResultCode includes possible error codes and shall indicate, if the subscription module was successfully reset.

5.1.16 STATUS_IND

The message STATUS_IND shall be used to indicate (a change in) the availability of the subscription module. The STATUS_IND message contains the following parameter:

Parameter	Ref.	Status
StatusChange	5.2.8	M

Table 5.11: Parameter of the STATUS_IND Message

The parameter StatusChange shall include the reason for the status change.

5.1.17 TRANSFER_CARD_READER_STATUS_REQ

The TRANSFER_CARD_READER_STATUS_REQ message contains no parameter.

5.1.18 TRANSFER_CARD_READER_STATUS_RESP

The TRANSFER_CARD_READER_STATUS_RESP message contains the following parameters:

Parameter	Ref.	Status
ResultCode	5.2.4	M
CardReaderStatus	5.2.7	C (ResultCode)

Table 5.12: Parameters of the TRANSFER_CARD_READER_STATUS_RESP Message

The parameter ResultCode includes possible error codes.

The parameter CardReaderStatus includes the Card Reader Status as described in GSM 11.14, Section 12.33 and TS 31.111, Section 8.33. It shall be included only if no error has occurred.

5.1.19 ERROR_RESP

The ERROR_RESP message contains no parameter.

5.2.20 SET_TRANSPORT_PROTOCOL_REQ

The SET_TRANSPORT_PROTOCOL_REQ message contains the following parameter:

Parameter	Ref.	Status
Transport Protocol	5.2.9	M

Table 5.13: Parameter of the SET_TRANSPORT_PROTOCOL_REQ Message

5.2.21 SET_TRANSPORT_PROTOCOL_RESP

The SET_TRANSPORT_PROTOCOL_RESP message contains the following parameter:

Parameter	Ref.	Status
ResultCode	5.2.4	M

Table 5.14: Parameter of the SET_TRANSPORT_PROTOCOL_RESP Message

5.2 Parameter IDs and Coding

The following table lists all parameters used in the messages of the SIM Access Profile, their length (in Bytes) and Parameter ID.

Parameter	Length	Parameter ID
MaxMsgSize	2	0x00
ConnectionStatus	1	0x01
ResultCode	1	0x02
DisconnectionType	1	0x03
CommandAPDU	Varies	0x04
CommandAPDU7816	Varies	0x10
ResponseAPDU	Varies	0x05
ATR	Varies	0x06
CardReaderStatus	1	0x07
StatusChange	1	0x08
Transport Protocol	1	0x09

Table 5.15: List of Parameter IDs

5.2.1 MaxMsgSize

The parameter MaxMsgSize consists of two bytes and is coded as an unsigned integer.

5.2.2 ConnectionStatus

The parameter ConnectionStatus is a one byte field. The values are as given in the following table:

Possible values for ConnectionStatus	**Value**
OK, Server can fulfill requirements	0x00
Error, Server unable to establish connection	0x01
Error, Server does not support maximum message size	0x02
Error, maximum message size by Client is too small	0x03
OK, ongoing call	0x04
Reserved	All others

Table 5.16: Possible Values for ConnectionStatus

5.2.3 DisconnectionType

The parameter DisconnectionType is a one byte field. The values are as given in Table 5.17.

Possible values for **DisconnectionType**	**Value**
Graceful	0x00

Immediate	0x01
Reserved	All others

Table 5.17: Possible Values for DisconnectType

"Graceful" shall be used if a graceful disconnect shall be performed while "Immediate" shall be used in case of an immediate disconnect.

5.2.4 ResultCode

The parameter ResultCode is a one byte field. The values are as given in Table 5.18, which also lists the messages, for that a ResultCode value is applicable:

Possible values for **ResultCode**	**Value**	**Used in**						
		TRANSFER_APDU_RESP	**TRANSFER_ATR_RESP**	**POWER_SIM_OFF_RESP**	**POWER_SIM_ON_RESP**	**RESET_SIM_RESP**	**TRANSFER_CARD_ READER_STATUS_RESP**	**SET_TRANSPORT_ PROTOCOL_RESP**
OK, request processed correctly	0x00	M	M	M	M	M	M	M
Error, no reason defined	0x01	M	M	M	M	M	M	
Error, card not accessible	0x02	M			M	M		
Error, card (already) powered off	0x03	M	M	M		M		
Error, card removed	0x04	M	M	M	M	M		
Error, card already powered on	0x05				M			
Error, data not available	0x06		M				M	
Error, not supported	0x07							M
Reserved	All others							

Table 5.18: Possible values for ResultCode

5.2.5 CommandAPDU, CommandAPDU7816 and ResponseAPDU

The parameter CommandAPDU contains a C-APDU that shall be coded in accordance with the GSM 11.11 specification. The parameter CommandAPDU7816 contains a C-APDU that shall be coded in accordance with ISO/IEC 7816-4 specification.

The parameter ResponseAPDU contains an R-APDU that shall be coded in accordance with either the GSM 11.11 or the ISO/IEC 7816-4 specifications, depending on whether it is contained in the TRANSFER_APDU_RESP message responding to the TRANSFER_APDU_REQ message containing the CommandAPDU or the CommandAPDU7816 parameter.

5.2.6 ATR

The parameter ATR shall contain an ATR that is coded as described in the ISO/IEC 7816-3 specification.

5.2.7 CardReaderStatus

The parameter CardReaderStatus shall contain the Card Reader Status and is coded as described in the GSM 11.14 specification and TS 31.111 specification.

5.2.8 StatusChange

The parameter StatusChange shall include the reason for the change in the Status of the subscription module. The possible values are given in Table 5.19.

Possible values for **StatusChange**	**ID**
Unknown Error	0x00
Card reset	0x01
Card not accessible	0x02
Card removed	0x03
Card inserted	0x04
Card recovered	0x05
Reserved	All other

Table 5.19: Possible Values for StatusChange

5.2.9 TransportProtocol

The parameter TransportProtocol shall contain the identifier for the protocol which is used between Client and Server as described in the ISO 7816-4 specification.

Possible values for **TransportProtocol**	**Value**
T=0	0x00
T=1	0x01
Reserved	All others

Table 5.20: Possible Values for TransportProtocol

5.3 Example

Figure 5.3 gives an example of a SIM Access Profile message. It shows the CONNECT_REQ message with the parameter MaxMsgSize=280 (decimal). The values for MsgID and ParameterID are as given in Section 5.

Meaning	MsgID	Number of para-meters	Reserved		Para-meter ID	Reserved	Parameter Length		Parameter Value		Padding Bytes	
Value (Hex)	0x00	0x01	0x00	0x00	0x00	0x00	0x00	0x02	0x01	0x18	0x00	0x00
Length (Bytes)	1	1	2		1	1	2		2		2	

Figure 5.3: Message Example

6 Service Discovery Procedures

Table 6.1 below lists all entries in the SDP database of the SIM Access Server. In the "status" column it is indicated whether the presence of this field is mandatory or optional.

Item	Definition:	Type:	Value:	AttrID	Status	Default
ServiceClassIDList					M	
ServiceClass0		UUID	SIM Access		M	
ServiceClass1		UUID	GenericTelephony		M	
Protocol Descriptor List					M	
Protocol #0		UUID	L2CAP		M	
Protocol #1		UUID	RFCOMM		M	
ProtocolSpecificParameter0	Server Channel	Uint8	N=server channel #		M	
BluetoothProfileDescriptor List					M	
Profile0	Supported Profile	UUID	SIM Access		M	
Parameter for Profile #0	Version	Uint16	0x0102[5]		M	
Service Name	Displayable Text name	String	Service-provider defined		O	"SIM Access"

Table 6.1: SDP Entry for SIM Access Server

[5] Indicating version 1.02

7 Serial Port Profile Interoperability Requirements

The SIM Access Profile requires compliance to the Serial Port Profile. For the purpose of reading the Serial Port Profile, the SIM Access Client shall always be considered to be Device A (the "initiator") and the SIM Access Server shall always be considered to be Device B (the "acceptor").

The following texts, together with the associated sub-clauses, define the requirements with regard to this profile in addition to the requirements defined in the Serial Port Profile.

7.1 RFCOMM Interoperability Requirements

For RFCOMM, no additions to the requirements stated in the Serial Port Profile apply.

7.2 L2CAP Interoperability Requirements

For the L2CAP layer, no additions to the requirements stated in the Serial Port Profile apply.

7.3 Link Manager (LM) Interoperability Requirements

In addition to the LM Interoperability Requirements stated in the Serial Port Profile, this profile mandates the use of link encryption using a standard combination key or an authenticated combination key.

7.4 Link Control (LC) Interoperability Requirements

For the Link Controller, no additions to the requirements stated in the Serial Port Profile apply.

7.4.1 Class of Device Usage

A device, which is active in the Server role of the SIM Access Profile, shall set the "Telephony" bit in the Service Class field.

It furthermore may use the following setting in the Class of Device field:

1. Indicate "Peripheral" as Major Device class
2. Indicate "SIM Card Reader" as Minor Device Class

The inquiring Client may use this information to filter the inquiry responses.

8 Generic Access Profile Interoperability Requirements

The SIM Access Profile requires compliance to the Generic Access Profile. This section defines the support requirements with regards to procedures and capabilities defined in Generic Access Profile.

8.1 Modes

Table 8.1 shows the support status for Modes within the SIM Access Profile.

	Procedure	Support in the Client	Support in the Server
1	Discoverability modes		
	Non-discoverable mode		
	Limited discoverable mode		O
	General discoverable mode		M
2	Connectability modes		
	Non-connectable mode		
	Connectable mode		M
3	Pairing modes		
	Non-pairable mode		
	Pairable mode	M	M
A blank entry designates, that the device may support the respective procedure, but it is not required to do so during the operation of the SIM Access Profile.			

Table 8.1: Generic Access Profile Modes

8.2 Security Aspects

The table shows the support status for Security aspects within the SIM Access Profile. Security Mode 2, or 3 or 4 shall be used for a SIM Access Profile connection.

	Procedure	Support in the Client	Support in the Server
1	Authentication	M	M
2	Security modes		
	Security mode 1		
	Security mode 2	C1	C1
	Security mode 3	C1	C1
	Security mode 4	C1/C2	C1/C2
3	Encryption	M	M
C1: Support for at least one of the security modes 2, 3, or 4 is mandatory. C2: Support for security mode 4 is mandatory in devices supporting the Bluetooth 2.1 + EDR, or later, core specification.			

Table 8.2: Security Aspects

8.3 Idle Mode Procedures

The table shows the support status for Idle mode procedures within the SIM Access Profile (see Section 6 of the Generic Access Profile [1]).

	Procedure	Support in the Client	Support in the Server
1	General inquiry	M	
2	Limited inquiry	O	
3	Name discovery	O	
4	Device discovery	O	
5	Bonding	M	M
A blank entry designates, that the device may support the respective procedure, but it is not required to do so during the operation of the SIM Access Profile.			

Table 8.3: Idle Mode Procedures

9 References

[1] Specification of the Bluetooth System v1.2 or later

[2] ISO/IEC 7816-3 Information technology - Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic Signals and transmission protocols

[3] GSM 11.11 Specification of the Subscriber Module - Mobile Equipment (SIM-ME) Interface

[4] GSM 11.14 Specification of the SIM Application Toolkit for the Subscriber Module - Mobile Equipment (SIM - ME) Interface

[5] <Reference removed>

[6] TS 102.221 UICC-Terminal Interface; Physical and Logical Characteristics

[7] TS 31.102 Characteristics of the USIM Application

[8] TS 31.111 USIM Application Toolkit (USAT)

[9] TIA/EIA/IS-820 Removable User Module (R-UIM) for TIA/EIA Spread Spectrum Standards

[10] TIA/EIA/IS-820-1 Removable User Subscription Module (R-UIM) for TIA/EIA Spread Spectrum Standards Addendum 1

[11] TIA/EIA/915 CDMA Card Application Toolkit

[12] ISO/IEC 7816-4 Information technology - Identification cards - Integrated circuit(s) cards with contacts, Part 4: Inter-industry command for interchange

10 List of Acronyms and Abbreviations

Abbreviation or Acronym	**Meaning**
APDU	Application Protocol Data Unit
ATK	Application Toolkit
ATR	Answer To Reset
CHV	Card Holder Verification (the PIN of the SIM)
GAP	Generic Access Profile
GSM	Global System for Mobile Communications
GSM SIM	GSM Subscriber Module
L2CAP	Logical Link Control and Adaptation Protocol
LC	Link Controller
LM	Link Manager
LMP	Link Manager Protocol
ME	Mobile Equipment
MITM	Man In The Middle (a type of security attack)
PIN	Personal Identification Number
PPS	Parameter and Protocol Selection
PRNG	Pseudo Random Number Generator
SIM	Subscriber Module
SSP	Secure Simple Pairing
UICC	UMTS term for the physical card
USIM	Universal Subscriber Module
UUID	Universally Unique IDentifier
R-UIM	Removable User Module

11 List of Figures

12 List of Tables