3GPP TSG SA WG3 Security — S3#29 **S3-030436**
15 - 18 July 2003
San Francisco, USA

3GPP TSG SA WG3 #28 **S3-030251**
6-9 May 2003
Berlin, Germany

Agenda Item: 6.11 WLAN inter-working
Source: Ericsson
Title: SIM access via 'SIM Access Profile' and Bluetooth link
Document for: Discussion

1. Introduction

The user can get WLAN access with either a SIM card or UICC card. The protocols EAP-AKA and EAP-SIM will be used with a SIM or UICC card for mutual authentication in WLAN access.

According to the WLAN UE definitions in chapter 4.1.2 in TS 33.234, the UICC or SIM card may reside in a 3GPP UE and be accessed by a WLAN-UE through Bluetooth, IR or a serial cable interface. In this scenario it would be convenient for the user to get simultaneous WLAN and 3GPP access with the same UICC or SIM card.

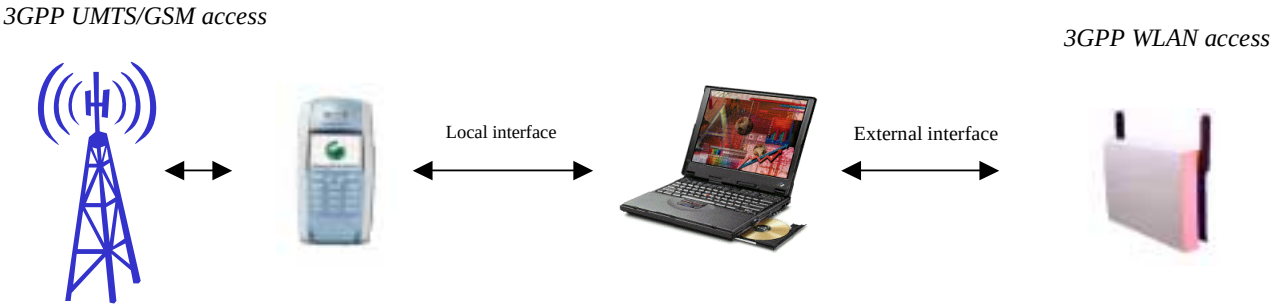

Figure 1 WLAN-UE Configuration

In order to allow a WLAN client running in a TE (e.g. laptop), accessing an application on a SIM/UICC, which resides in a 3GPP UE, a secured interface between the TE and MT is required in order to protect the signalling data (e.g. authentication challenges and responses). The TS 33.234 currently contains the following security requirements on the local interface between a TE and MT:

4.2.4 WLAN-UE Functional Split

The security functionality required on the terminal side for WLAN-3G inter-working may be split over several physical devices that communicate over local interfaces*. If this is the case, then the following requirements shall be satisfied:*

- *Any local interface shall be protected against eavesdropping, undetected modification attacks on security-relevant information. This protection may be provided by physical or cryptographic means.*
- *The endpoints of a local interface should be authenticated and authorised. The authorisation may be implicit in the security set-up.*

- *The involved devices shall be protected against eavesdropping, undetected modification attacks on security-relevant information. This protection may be provided by physical or cryptographic means.*

In the BLUETOOTH SIG group a 'SIM Access Profile' specification has been specified that could be used for this purposes, maybe with some potential modifications. The SIM Access Profile requires a secured Bluetooth link. The 'SIM Access Profile'-protocol and Bluetooth needs to be supported both in the TE and the 3GPP UE. This work could be used for other services as well as IMS, MBMS and so on.

Ericsson is in this paper promoting a new version of the SIM Access Profile specification, to better suite the 3GPP requirements on simultaneous WLAN and 3GPP access with the same SIM/UICC in the split WLAN-UE case. In addition, Ericsson proposes to remove requirement on integrity protection in TS 33.234 on the local interface between the TE and the MT.

Note that the solution discussed in this paper with 'SIM Access Profile' via Bluetooth, does not require any further standardisation on the UICC or GSM SIM cards.

2. Background

In the BLUETOOTH SIG group a 'SIM Access Profile' has been developed among other profiles, to be used via a Bluetooth link. The 'SIM Access Profile' specification was developed for car-embedded 2G/3G terminals, which does not support in-built SIM card readers.

2.1 'SIM access profile' in BLUETOOTH SIG

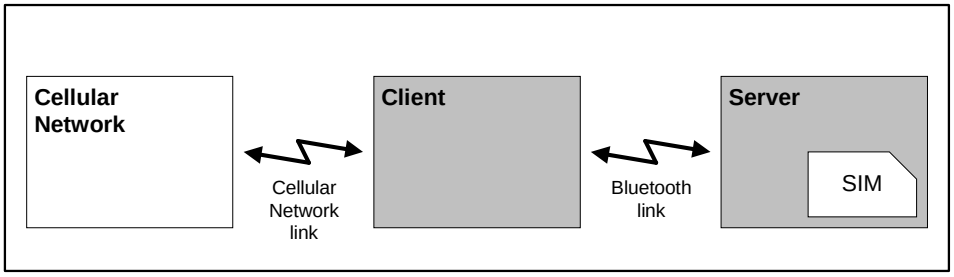

Figure 2 Basic System Configuration

With the current 'SIM Access Profile' specification, version 0.95VD d, the following use cases can be achieved with the SIM Access Profile:

- Register a client (e.g. car-embedded 2G or 3G UE) in a 2G or 3G cellular network using the subscription data stored in a SIM inserted into an external device (e.g. 2G or 3G UE, external SIM card reader).
- Make a call from a client (e.g. car-embedded 2G or 3G UE) using the subscription information stored in a SIM inserted into an external device (e.g. 2G or 3G UE, external SIM card reader).
- Use the client (e.g. car-embedded 2G or 3G UE) to access phonebook data stored in a SIM inserted into an external device (e.g. 2G or 3G UE, external SIM card reader).

In the figure above is should be emphasized, that the SIM Access Profile is implemented both in the client and the server and that:

- the server has no intelligence other than maintaining the physical contact to the SIM card;
- the server is not able to multiplex several SIM card sessions (e.g. one for GSM access and one for WLAN access);
- the server is only maintaining one single Bluetooth connection to the client.

It is expected that the 'SIM Access Profile' specification, version 095 VD d, shall be put into version 1.0 in September 2003.

2.2 Security requirements on the BLUETOOTH link set by 'SIM Access Profile'

The 'SIM Access Profile' specification sets the following security requirements on the BLUETOOTH link:

-Encryption is mandatory;

-Encryption key length shall be at least 128 bits;

-Server initiated authentication is mandated;

-Link keys- only combinations keys shall be used;

-Link keys may change each time a new SIM Access Profile connection is established.

It can be noticed that integrity protection is not supported in Bluetooth.

3. Discussions

This chapter discusses the scenario with a split WLAN –UE where a TE (e.g. laptop) in WLAN access gets SIM access from a UICC or GSM SIM card inserted in an external 2G/3G UE according to Figure 1. The following issues are covered:

-The potential information and data a WLAN client requires from a SIM/UICC;

- Two different potential signaling flows with EAP-AKA and EAP-SIM in a split WLAN-UE case with SIM Access Profile and Bluetooth;

- The promotion of a new version of the 'SIM Access Profile' specification to better suite 3GPP requirements on simultaneous WLAN and 3GPP access with the same SIM/UICC.

3.1 Split WLAN-UE

3.1.1 Information and data on a SIM/UICC required from a WLAN client

In the split WLAN-UE case, a WLAN client running in a TE (e.g. laptop) requires the following information and data from a UICC card or GSM SIM card inserted into a 3G/2G UE:

-The knowledge of whether a GSM SIM or UICC card is inserted.

-The knowledge of the residing applications on a UICC card.

-Read parameters as the IMSI from a GSM or USIM application;

-Send authentication challenge requests to the GSM and USIM application.

-Receive authentication challenge responses from the GSM and USIM application.

(-Access the phone book on a UICC or GSM SIM card.)

3.1.2 EAP-AKA utilizing 'SIM Access Profile' via a Bluetooth link

When a UICC is inserted into a 3G/2G UE, the network shall initiated EAP-AKA according to TS 33.234.

The following flow shows how the signalling between the network, TE, MT and a USIM application on a UICC could look like, when EAP-AKA is initiated by the network in WLAN access.

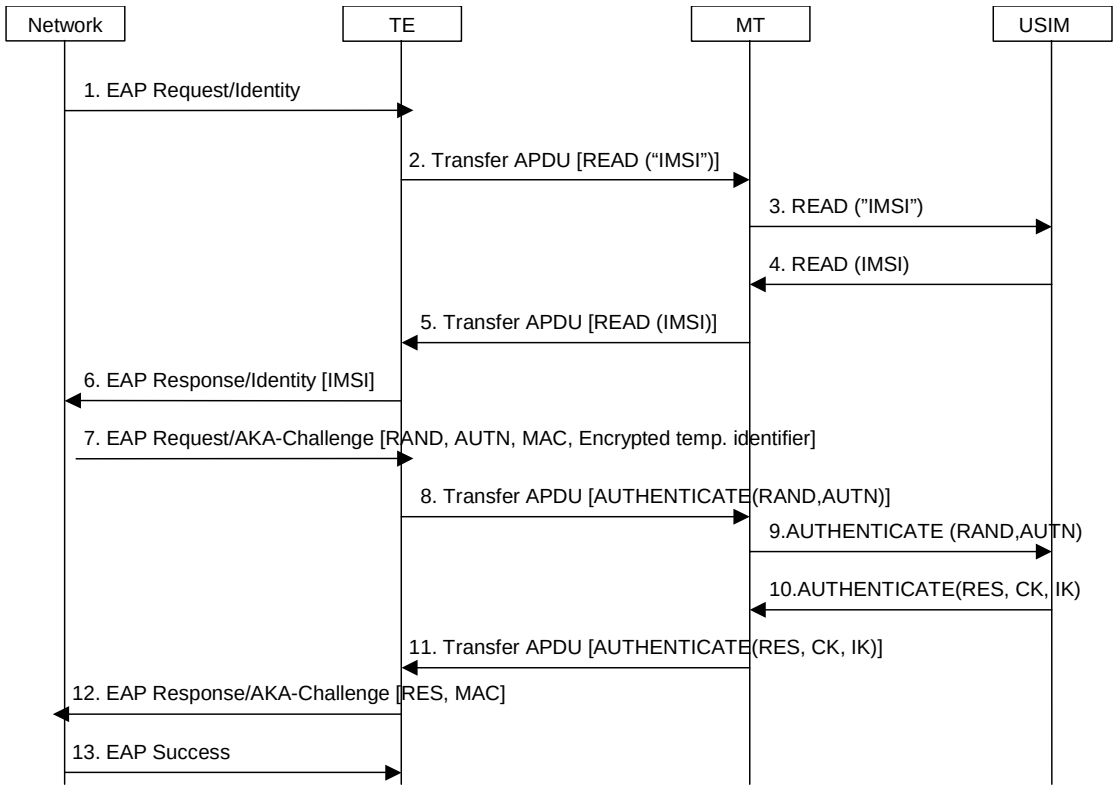

Figure 3 Flow with EAP-AKA

3.1.3 EAP-SIM utilizing ‘SIM Access Profile’ via a Bluetooth link

When a GSM SIM is inserted into a 3G/2G UE, the network shall initiate EAP-SIM according to TS 33.234.

The following flow shows how the signalling between the network, TE, MT and a GSM SIM application on a SIM could look like, when EAP-SIM is initiated by the network in WLAN access.

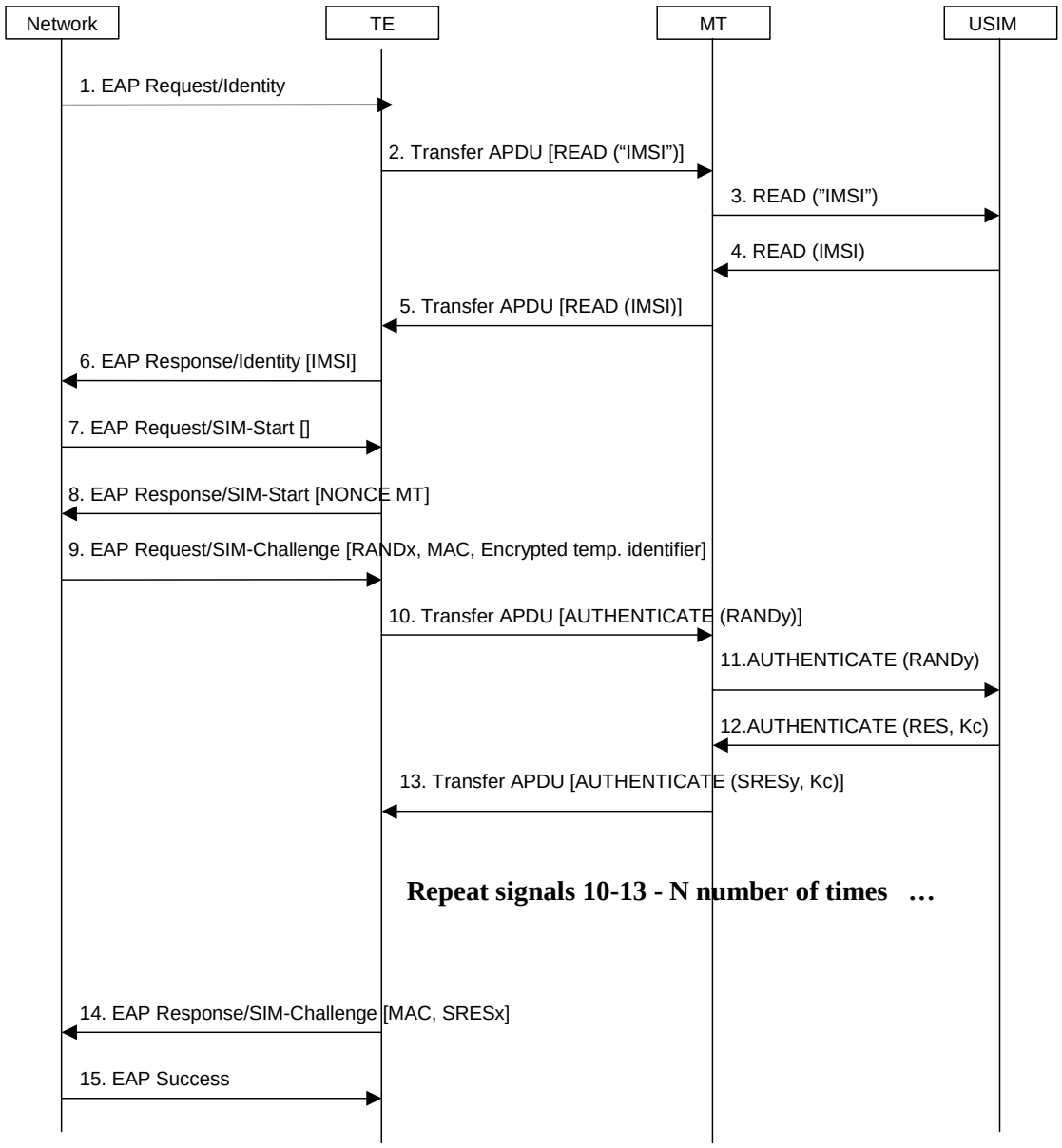

Figure 4 Flow with EAP-SIM

3.2 Promoting a new version of ‘SIM Access Profile’

Ericsson would like to promote a new version of the ‘SIM Access Profile’ in the Bluetooth SIG group to better suite the 3GPP requirements for 3GPP services as simultaneous WLAN and 3GPP access.

The 3GPP UE in Figure 1 should be allowed to use the same SIM card session to one and the same application on the SIM or UICC to be used for simultaneous GSM/UMTS access and WLAN access. Still only one single Bluetooth connection to a TE needs to be maintained in the 3GPP UE. In addition it should be an implementation issue in the 3GPP UE whether it only allows certain operations on the SIM or UICC card as reading parameters from the card and handle authentication challenges and responses on the card, when accessed from a TE via a SIM Access Profile and Bluetooth.

The following two sub-chapters contain proposals for new requirements on the ‘SIM Access Profile’ specification.

The third sub-chapter contains some open issues that we would like to discuss in this meeting.

3.2.1 New requirements on ‘SIM Access Profile’

A potential new version of SIM Access Profile could support the following:

3.2.1.1 ISIM support

The ‘SIM Access Profile’ specification should allow access to an ISIM application on a UICC. This could be used for services as IMS via 3GPP.

3.2.1.2 Simultaneous WLAN and 3GPP access with the same SIM or UICC

According to the ’SIM Access Profile’ specification in [1], a 2G/3G UE with a GSM SIM or UICC inserted is not allowed to access a 2G or 3G network and simultaneously have a SIM Access Profile connection established with a client (e.g. TE). This requirement was probably introduced in order to disallow that two terminals (e.g. client and server in figure 2) are accessing a GSM network with the same IMSI.

In order to allow simultaneous WLAN and 3GPP access with the same UICC or SIM card, it would be preferred if this requirement was changed to allow a 2G/3G UE to access a 2G or 3G network and simultaneously allow a SIM Access Profile connection to a TE via a BLUETOOTH link.

3.2.1.3 Features in ‘SIM Access Profile’

It is proposed that the following features in the SIM ACCESS PROFILE shall be supported in the new version of the specification:

- Connection Management;

- Transfer APDU;

- Transfer ATR;

- Report Status;

- Transfer card reader status;

- Error handling.

The 3G/2G UE shall be required to be switched on and a SIM/UICC card shall be powered on, in order to allow and accept a request from a TE to establish a SIM Access Profile connection. It shall not be possible from a TE (e.g. laptop) to reset, power on or off a SIM/UICC card inserted into a 3G/2G UE, as the SIM/UICC is already in use for GSM or UMTS access in the 2G/3G UE. Therefore it is proposed that the following features in the SIM ACCESS PROFILE shall NOT be supported in the new version of the specification:

- Reset SIM or USIM in the 2G/3G UE;

- Power on the SIM or USIM in the 2G/3G UE;

- Power off the SIM or USIM in the 2G/3G UE.

3.2.3 Open issues

3.2.3.1 Integrity protection on the local interface between a TE and MT

In chapter 4.2.4 in TS 33.234, we currently have a requirement on integrity protection on the local interface between a TE (e.g. laptop) and a MT:

4.2.4 WLAN-UE Functional Split

The security functionality required on the terminal side for WLAN-3G interworking may be split over several physical devices that communicate over local interfaces. If this is the case, then the following requirements shall be satisfied:

- ***Any local interface shall be protected against** eavesdropping**, undetected modification attacks on security-relevant information**. This protection may be provided by physical or cryptographic means.*

Considering the short communication distance in Bluetooth, Ericsson does not see any reasons for requiring integrity protection on the encrypted SIM access data. Therefore Ericsson proposes to delete such requirement from TS 33.234. If SA3 can't agree upon deleting this requirement, then SA3 should ask the BLUETOOTH SIG group, whether integrity protection can be supported and added to the 'SIM Access Profile' -specification.

3.2.3.2 PIN or password in Bluetooth

In BLUETOOTH a PIN or password of 16 characters is required today. This is not so user friendly. We encourage the usage of an improved pairing proposed by the BLUETOOTH SIG Security Expert Group to be used by the 'SIM Access Profile'. An improved pairing would allow a shorter PIN or password without providing less security.

3.2.3.3 PIN to access the UICC or GSM SIM card with SIM Access Profile

In addition the user may be required to enter a PIN code in the **MT,** each time the MT receives a new request to establish a new SIM Access Profile connection from the TE, in order to allow access to the UICC or GSM SIM card . This could be required even though the user already has entered the PIN code once before when switching on the 3GPP UE. But this should be an implementation issue in the MT and could be configurable by the user in the MMI in the MT.

4. Conclusions

Ericsson proposes to send an LS to the Bluetooth Architecture Review Board (BARB) and the CAR groups, asking the groups to start the work on a new version of the SIM Access profile, and include a list of requirements presented in this paper.

In addition we propose to remove the requirement on integrity protection on a Bluetooth link in TS 33.234 on the local interface between the TE and the MT.

5. References

[1] SIM Access Profile, Interoperability Specification, version 0.95VD - d. Document no. CAR 020 SPEC/0.95cB.

[2] 3GPP TS 33.234 V0.4.0 "Wireless Local Area Network (WLAN) Interworking Security".

3GPP TSG-SA3 Meeting #28
Berlin, Germany, 6th-9th May, 2003

Tdoc ⌘DocNumber

CR-Form-v7

CHANGE REQUEST

⌘ **33.234** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **0.4.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Delete requirement on integrity protection on local interface
Source:	⌘	Ericsson
Work item code:	⌘	WLAN Interworking
Date:	⌘	01/05/2003
Category:	⌘	**C**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	A local Bluetooh link can be used between a TE and MT, in order to allow a WLAN client in a TE to access the UICC or SIM in a 3GPP UE. Bluetooth does not support integrity protection. In TS 33.234 we have currently a requirement on the local interface in the case of WLAN UE Functionality Split. Considering the short communication distance in Bluetooth, Ericsson does not see any reasons for requiring integrity protection on the encrypted SIM access data. Therefore Ericsson proposes to delete such requirement from TS 33.234.
Summary of change:	⌘	Delete requirement on integrity protection when a local Bluetooth link is used between a TE and MT.
Consequences if not approved:	⌘	Bluetooth does not support integrity protection. If we don't delete this requirement from TS 33.234, Bluetooth can not be used on the local interface between the TE and MT in this WLAN UE Functionality Split scenario, unless we require the Bluetooth forum where Bluetooth is developed, to add integrity protection.

Clauses affected:	⌘	4.2.4			
Other specs affected:	⌘	**Y**	**N**		
		☐	☐	Other core specifications	⌘
		☐	☐	Test specifications	
		☐	☐	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4.2.4 WLAN-UE Functional Split

The security functionality required on the terminal side for WLAN-3G interworking may be split over several physical devices that communicate over local interfaces. If this is the case, then the following requirements shall be satisfied:

- Any local interface shall be protected against eavesdropping, ~~undetected modification~~ attacks on security-relevant information. This protection may be provided by physical or cryptographic means.
- The endpoints of a local interface should be authenticated and authorised. The authorisation may be implicit in the security set-up.
- The involved devices shall be protected against eavesdropping, undetected modification attacks on security-relevant information. This protection may be provided by physical or cryptographic means.

[Editor's note: LS (S3-030145) sent to SA1 - SA3 would like to thank SA1 for the LS and attached documents on the proposal "Having a Single USIM to Authenticate Multiple Devices Simultaneously using local Wireless Link" (Tdoc S3-030006, S1-022388). It was noted at the meeting that there was interest in studying the security issues related to this proposal and also UE functionality split scenarios. It was also noted at the meeting that the TR 22.944 v5.1.0 doesn't address the User Equipment Functionality Split (UEFS) issues for Release 6, but only for Release 5. However there was concern among some members on enhancing the USIM as part of this proposal. SA3 wishes to inform SA1 that a decision on the feasibility of this proposal needs further evaluation.]

BLUETOOTH DOC	Date / Year-Month-Day 02-095-175	Approved Draft	Revision ~~0.95VD c~~ 0.95VD d	Document No CAR_020_SPEC/0.95cB 2
Prepared Holger Krummel	e-mail address Holger.Krummel@nokia.com			N.B. Confidential

SIM Access Profile

Interoperability Specification

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.

Special Interest Group (SIG)

The following companies are represented in the Bluetooth Special Interest Group:
3COM
Ericsson Mobile Communications AB
IBM Corp.
Intel Corp.
Agere Systems
Microsoft
Motorola
Nokia Corp.
Toshiba Corp.

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 w.r.t. 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	3rd-Oct-02	Updated to use generic term for all cards; Updated to allow access to R-UIM also
0.95VD f	13th-Nov-02	Changed generic term Identity Module to Subscriber Module

Contributors

Penny Breyer	Cambridge Silicon Radio Ltd.
Björn Bunte	Nokia Corp.
Lowell Campbell	Denso Corp.
Holger Krummel (owner)	Nokia Corp.
Holger Lenz	Berner & Mattner Systemtechnik GmbH
Tony Mansour	Motorola, Inc.
Jesus-Angel Gonzalez Pulido	Ericsson España, S.A.
Daniel S. Rokusek	Motorola, Inc.
Raghunandan Sanjeev	Motorola, Inc.

Kazu Suzuki	Denso Corp.
Michael Svob	Motorola, Inc.
Yoichiro Takeuchi	Toshiba Corp.
Kreg Ulery	Agere Systems
Christian Gehrmann	Ericsson Mobile Communications AB
Monica Wifvesson	Ericsson Mobile Communications AB
Ganesh Pattabiraman	Qualcomm Inc.

Disclaimer and copyright notice

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 and to adopt a process for adding new Bluetooth™ profiles after the release of the Specification.

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, ~~or~~ a UICC card or a R-UIM card via a Bluetooth link. Unless otherwise specified the term “Subscription ~~Identity~~ module” shall be used to refer to the GSM SIM card, a UICC card or a R-UIM card. The profile enables the usage model "Personalizing the Car and its Devices" (see [5]) and similar usage models, which involve a Bluetooth enabled SIM card holder and a cellular phone.

For example, with this profile, the user can personalize his/her car-embedded phone with ~~a~~an ~~GSM SIM or UICC~~identity subscription module ~~card~~ 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~~an ~~GSM SIM card or a UICC card Identity~~ subscription module (see [3] and [6]). It also enables multiple card operations as defined in [4], ~~and~~ [8] and [11].

1.2 Profile Dependencies

Figure 1-1 below 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.

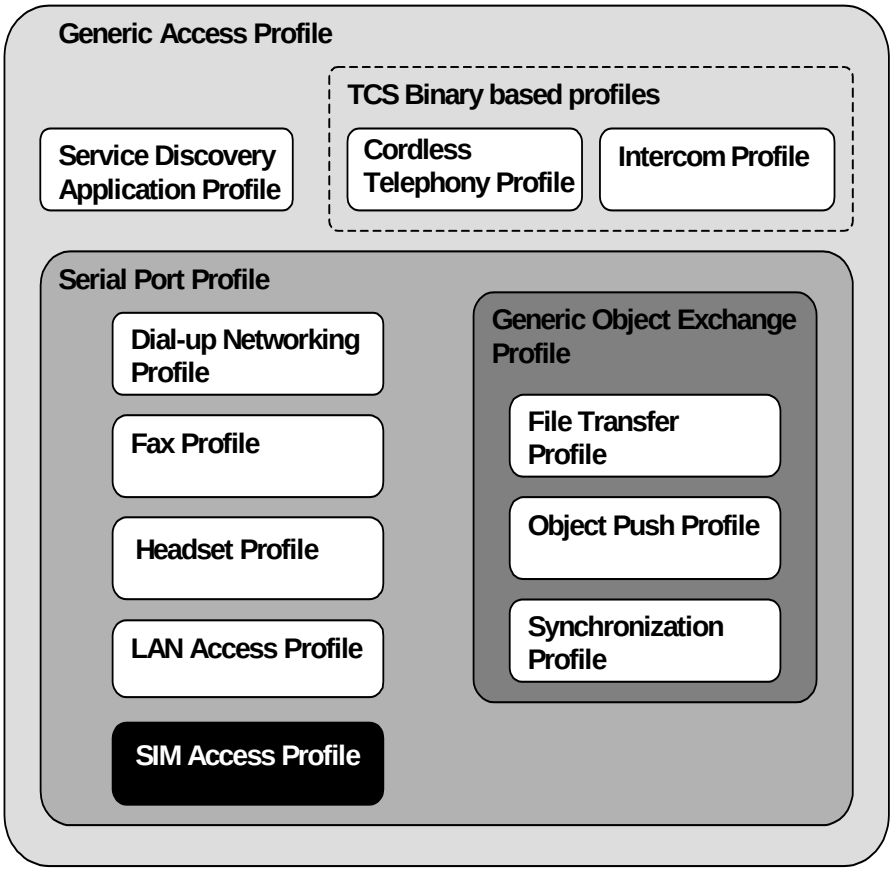

Figure 1-1 Profile Dependencies

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).

A blank entry in a table 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.

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 shall never 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):

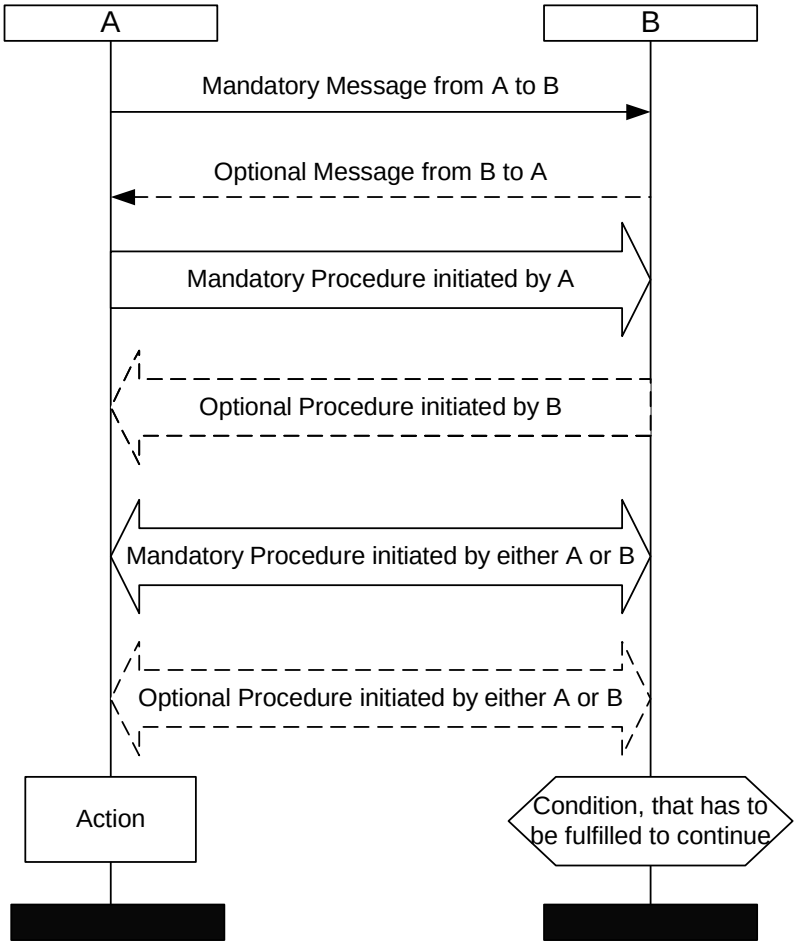

Figure 1-2 Arrows used in signaling diagrams

1.3.3 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 below shows the protocols and entities used in this profile.

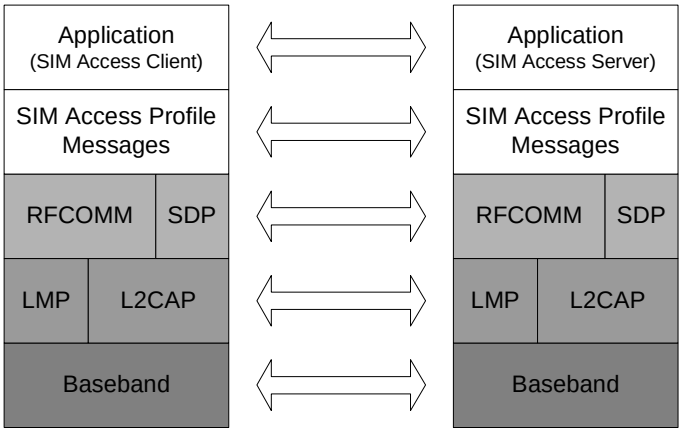

Figure 2-1 Protocol Stack

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

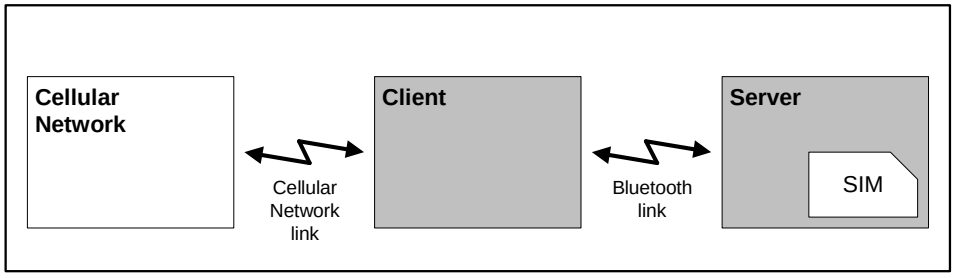

Figure 2-2 Basic System Configuration

The following two roles are defined for this profile:

Server - The SIM Access Server has direct (galvanic) access to ~~a~~an ~~GSM SIM or UICC card~~ ~~Identity~~ subscription module. It acts as a SIM card reader, which assists the Client in accessing and controlling the ~~GSM SIM or UICC card~~ ~~identity~~ 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 ~~GSM SIM or UICC card~~ ~~identity~~ 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~~an ~~GSM SIM or UICC card~~ ~~identity~~ subscription module in the Server for a connection to the cellular network.

Both the ~~GSM SIM/UICC card~~ ~~identity~~ 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: ~~GSM SIM or UICC~~~~Identity~~ subscription Module in the Server

As shown in Figure 2-2, the Server contains ~~a~~an ~~GSM SIM or a UICC~~~~Identity~~ subscription Module, which is used by the Client. The Client accesses the files and services of the ~~GSM SIM or the UICC~~ card ~~Identity~~ subscription module as if the ~~GSM SIM or UICC~~ ~~Identity~~ 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 ~~GSM SIM or the UICC~~~~Identity~~ subscription module.
- make a call from the Client using the subscription information stored in the ~~GSM SIM or the UICC~~~~Identity~~ subscription module.
- use the Client to access phonebook data stored in the ~~GSM SIM or the UICC~~~~Identity~~ subscription module.

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 ~~GSM SIM or UICC~~~~Identity~~ subscription module. The Client uses this ~~GSM SIM or UICC~~~~Identity~~ subscription module for connecting to the cellular network.

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

- 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 (i.e. the Server).

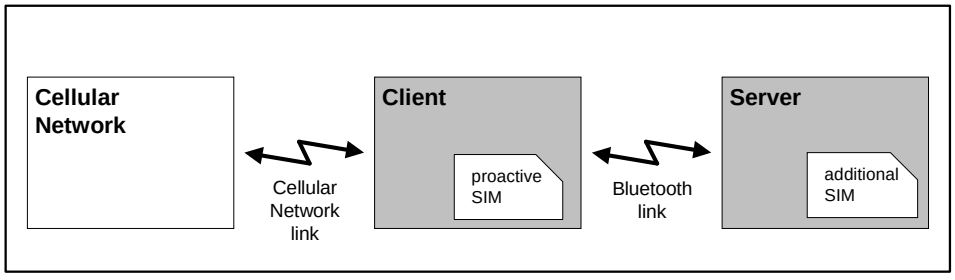

Figure 2-3 System Configuration with proactive SIM in the Client

2.4 Profile Fundamentals

The SIM Access Profile describes the messages and procedures for accessing an ~~Identity~~ subscription module ~~GSM SIM card or a UICC card~~ over a Bluetooth link. It is especially designed for usage with:

- GSM SIM cards[1] and provides a transport and remote control solution for GSM 11.11 [3] and GSM 11.14 [4].

[1] It is intended to extend the profile for usage with future cellular systems (e. g. 3rd generation systems' USIM or R-UIM) in upcoming profile revisions.

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

The Client is in most cases a phone, which has to behave according to the relevant GSM,~~and~~ 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 ~~GSM SIM or UICC~~~~Identity~~ subscription module for its own cellular network connection. According to the ~~GSM~~ GSM, ~~and~~ 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 ~~GSM SIM or UICC~~~~Identity~~ subscription module in the Server. Similarly, the Server may establish a connection, even if its ~~GSM SIM or UICC~~~~Identity~~ subscription module is powered off. In order to handle these different situations, the Client shall be informed about the status of the ~~GSM SIM or UICC~~~~Identity~~ 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, ~~or~~ USIM application or a R-UIM application on ~~a~~an ~~GSM SIM or UICC~~~~Identity~~ subscription module card in the context of this profile.

It is assumed, that the Client is initiating 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. Either security mode 2 or 3 shall be used for the SIM Access Profile connection. 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 combination keys shall be used for SIM Access Profile connections. An implementation shall support combination keys being changed at each new SIM Access Profile connection. An implementation may change the combination keys at each new SIM Access Profile connection. For increased security, this is encouraged.

Encryption key length - The encryption key deployed in the system shall ~~support the~~support the maximum length as given in the Bluetooth specification. An implementation may use a length at this maximum. The length of the encryption key shall be at least 64 bits. For increased security, use of the maximum length is encouraged.

Passkey - The length of the passkey shall be 16 digits (decimal) at least. Fixed passkeys shall not be used.[2]

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.

[2] In an implementation specfic example, the SIM Access Server can generate the passkey using the Bluetooth PRNG and display it. This passkey is then entered into the SIM Access Client. The SIM Access Server can be designed such, that it does not accept any other passkey than the one it has generated.

3 Application Layer Features

Table 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	M	M
7	Report Status	M	M
8	Transfer Card Reader Status	O	M
9	Error Handling	M	M

Table 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 ~~GSM SIM or the UICC~~Identity subscription module are called Command APDUs, while APDUs sent by the ~~GSM SIM or the UICC~~Identity 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 is always initiated by the Client.

The format and content of the APDUs are defined in [3], ~~and~~ [4], [6], [7], ~~and~~ [8], [9], [10] and [11].

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 is sent by the ~~GSM SIM or the UICC~~Identity subscription module to the Server after the ~~GSM SIM or the UICC~~Identity subscription module has been powered on or reset. It contains information about the

interface provided by the ~~GSM SIM or the UICC~~Identity subscription module and the services on the GSM SIM~~, and~~ 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 ~~GSM SIM or UICC~~Identity subscription module off remotely.

This feature gives the Client a means to power the ~~GSM SIM or UICC~~Identity subscription module in Server off remotely. It is needed for the Application Toolkit[3] ~~SIM ATK (Application Toolkit) [4] and USAT (USIM Application Toolkit) [8]~~ purposes as shown in Scenario 2 (Section 2.3.2).

Power SIM on - The ability to power the ~~GSM SIM or UICC~~Identity subscription module on remotely.

This feature gives the Client a means to power the ~~GSM SIM or the UICC~~Identity subscription module in the Server on remotely. It is e~~. g~~.g. needed for Application Toolkit[3] ~~SIM ATK (Application Toolkit) [4] and USAT (USIM Application Toolkit) [8]~~ 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 ~~GSM SIM or the UICC~~Identity subscription module in the Server. It is e~~. g~~.g. needed for Application Toolkit[3] ~~SIM ATK purposes [4], and USAT (USIM Application Toolkit) [8]~~ 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 ~~GSM SIM and the UICC Identity~~ subscription module.

This feature enables the Client to react appropriately, if the ~~GSM SIM or the UICC~~Identity 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 ~~GSM SIM or the UICC~~Identity subscription module ~~card~~ (e.g. the size of the SIM or if the SIM is removable). This information is

[3] 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].

required for~~-~~ Application Toolkit ~~SIM ATK and USAT~~ purposes as shown in Scenario 2 (Section 2.3.2) and specified in [4]~~, and~~ [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 will send an appropriate error message.

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.

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	4.1
		Report Status	4.9
		Transfer ATR	4.5
		Disconnect Initiated by the Client	4.2
		Disconnect Initiated by the Server	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	4.7
		Transfer ATR	4.5
6	Reset SIM	Reset SIM	4.8
		Transfer ATR	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

Table 2: 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.

Before the Client can send a SIM Access Profile message to the Server, the two devices shall establish 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 then answers with the CONNECT_RESP message[4]. These two messages may be repeated as

[4] If the Server does not respond to the Client after a period of time defined by the Client, the latter decides how to proceed. It can either re-send the CONNECT_REQ message or abort the connection establishment procedure.

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~~an ~~GSM SIM or a UICC~~Identity subscription module, which is already powered on, the Server shall reset the ~~GSM SIM or the UICC~~Identity subscription module (latest) before sending the CONNECT_RESP message. This ensures that the ~~GSM SIM or the UICC~~Identity subscription module is in a well-defined state, when accessed by the Client.

After the Server has send the CONNECT_RESP message with the parameter "ConnectionStatus" set to "OK, Server can fulfill requirements" (see Section 5.3.2), it informs the Client about the status of its ~~GSM SIM or UICC~~Identity subscription module connection with the STATUS_IND message (see Section 4.9 for details).

If ~~a~~an ~~GSM SIM or UICC~~Identity 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 ~~GSM SIM or the UICC~~Identity subscription module with the TRANSFER_ATR_REQ message. The Server will then answer with the TRANSFER_ATR_RESP message as described in Section 4.5.

Figure 4-1 illustrates how the Client and Server connect successfully:

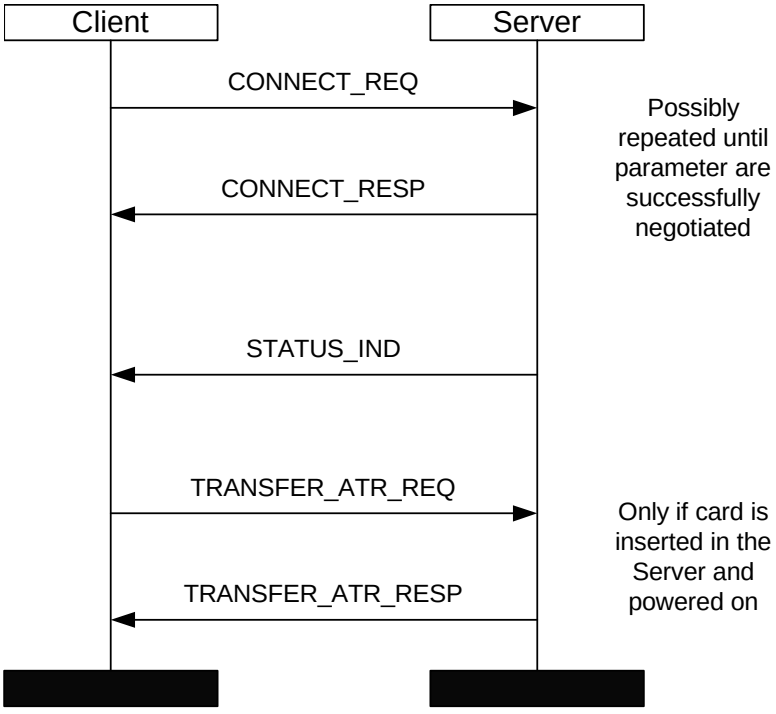

Figure 4-1 Client connecting to Server

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 5.3.2). 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 5.3.1), 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 sets the parameter ConnectionStatus (see 5.3.2) in the CONNECT_RESP message to "OK, Server can fulfill requirements". If not, it sets 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 ~~, or~~ USIM application session or R-UIM application session which involves the ~~GSM SIM or the UICC~~Identity subscription module in the Server. The Client can then send a DISCONNECT_REQ message to the Server.

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

Note: After sending the DISCONNECT_RESP message, the Server may use the ~~GSM SIM or the USIM~~ ~~Identity~~ 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:

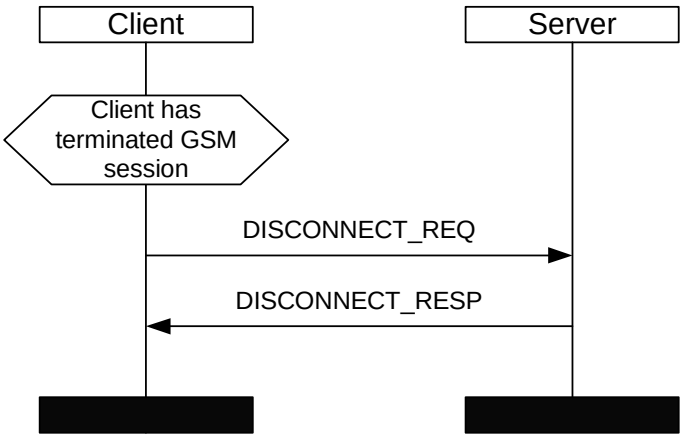

Figure 4-2 Client disconnecting from Server (initiated by the Client)

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 can indicate, if it wants to release the SIM Access Profile connection immediately or gracefully.

If the Server asks for an immediate release, no more messages will be exchanged and the SIM Access Profile connection is released directly after the DISCONNECT_IND message. Furthermore, the Client immediately shall terminate any existing GSM application session, ~~or~~ USIM application session or R-UIM application session in order to be inline with the relevant GSM specifications, ~~and~~ 3GPP specifications and 3GPP2 specifications.

If the Server asks for a graceful connection shutdown, the transfer of APDUs is still allowed before the Client terminates any existing GSM application session, ~~or~~ USIM application session or R-UIM application session and sends the DISCONNECT_REQ message. Finally, the Server sends a DISCONNECT_RESP message and the SIM Access Profile connection is released.

Figure 4-3 illustrates how the Server initiates a graceful disconnect from the Client. If an immediate disconnect is desired, the MSC will only contain the DISCONNECT_IND message.

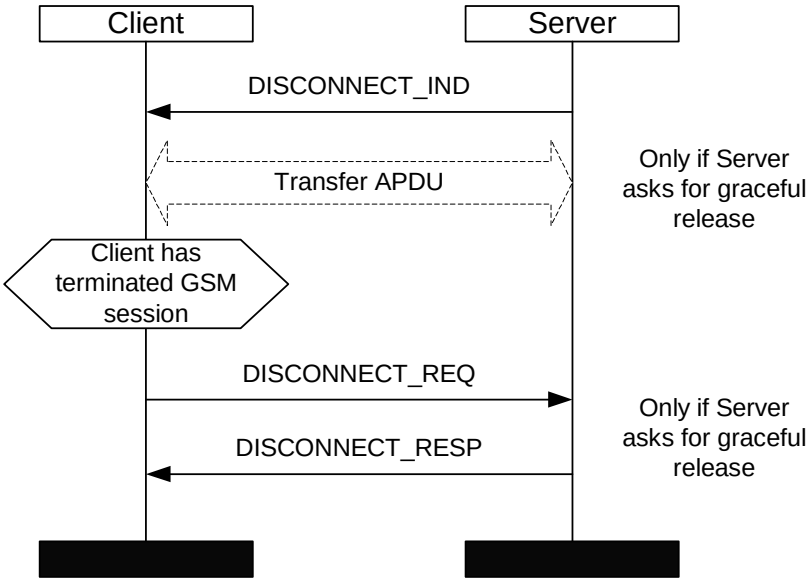

Figure 4-3 Client disconnecting gracefully from Server (initiated by the Server)

4.4 Transfer APDU

For transferring an APDU between the Client and the Server, the messages TRANSFER_APDU_ REQ and TRANSFER_APDU _RESP are used. ADPU transfers are always initiated by the Client.

Both messages contain an APDU (as defined for the GSM application in GSM 11.11 or GSM 11.14, ~~and~~ as defined for the USIM application in TS 31.102 and TS 31.111 or as defined for the R-UIM application in TIA/EIA/IS-820 and TIA/EIA/IS-820-1) in their payload. The message APDU_TRANSFER_REQ is used for Command-APDUs (from Client to the ~~GSM SIM or the UICC~~Identity subscription module). The message TRANSFER_APDU_RESP is used for Response-APDUs (from the ~~GSM SIM or the UICC~~Identity subscription module to the Client).

Figure 4-4 illustrates the successful exchange of APDUs between Client and Server:

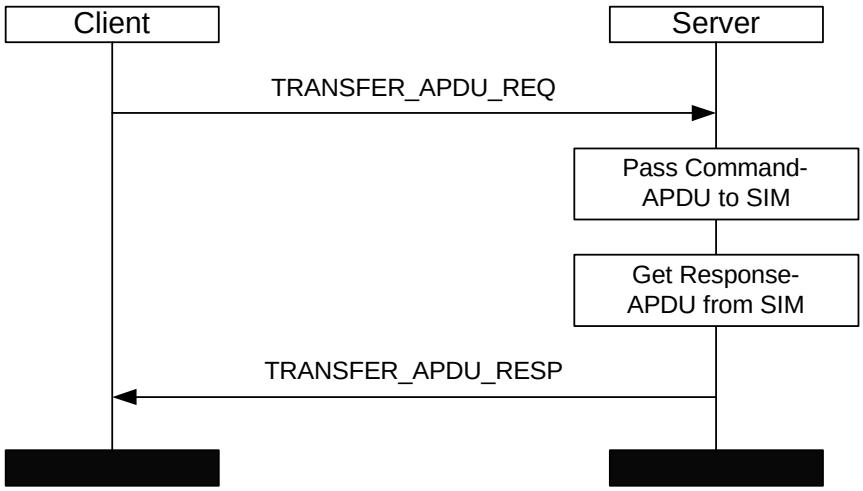

Figure 4-4 APDU Transfer between Client and Server

If no error has occurred, the TRANSFER_APDU_RESP message will also contain the result code "OK, request processed correctly" (see Section 5.3.4). In case of an error, the TRANSFER_APDU_RESP message will only contain an appropriate result code (see also Section 5.3.4):

- If the card is removed from the Server, the result code "Error, card removed" is used.
- If the card is inserted in the Server but powered off, the result code "Error, card (already) powered off" is used.
- If the Server detects, that the card does not answer, the result code "Error, card not accessible" is used.
  Please note, that this is independent of the case, in which the Client detects, that the ~~GSM SIM or the UICC~~~~Identity~~ subscription module is not responding to e. g. Command APDUs.
- If an error has occurred, which cannot adequately be described by any of the previous reasons, the result code "Error, no reason defined" is used.

4.5 Transfer ATR

The Client may ask the Server to send the ATR from the ~~GSM SIM or the UICC~~~~Identity~~ subscription module. The TRANSFER_ATR_REQ message is used for this purpose. Following this request, the Server sends the ATR to the Client in the payload of the TRANSFER_ATR_RESP message.

Figure 4-5 illustrates the successful ATR transfer:

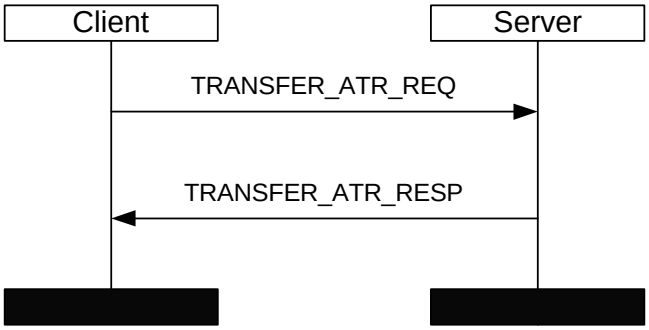

Figure 4-5 ATR Transfer between Client and Server

If no error has occurred, the TRANSFER_ATR_RESP message will also contain the result code "OK, request processed correctly" (see Section 5.3.4). In case of an error, the TRANSFER_APDU_RESP message will only contain an appropriate result code (see also Section 5.3.4):

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

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

4.6 Power SIM off

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

The Client can then send the POWER_SIM_OFF_REQ message to the Server. Upon receiving this message, the Server powers off the ~~GSM SIM or the UICC~~Identity subscription module, i. e. it removes the voltage from the card. Afterwards, the Server sends 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 ~~GSM SIM or the UICC~~Identity subscription module ~~card~~:

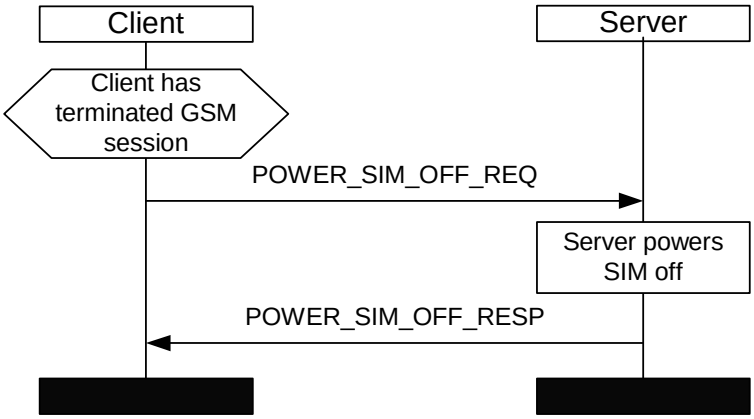

Figure 4-6 Client requests Server to power the SIM off

If no error has occurred, the POWER_SIM_OFF_RESP message will contain the result code "OK, request processed correctly" (see Section 5.3.4).

In case of an error, the POWER_SIM_OFF_RESP message will contain an appropriate result code (see also Section 5.3.4):

- If the card is already powered off, the result code "Error, card (already) powered off" is used.

- If the card is removed from the Server, the result code "Error, card removed" is used.

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

4.7 Power SIM on

If ~~a~~an ~~GSM SIM or a UICC~~Identity ~~subscription~~ module is powered off, the Client may request the Server to power it on again, i. e. to apply the supply voltage and clock signal to the ~~GSM SIM or the UICC~~Identity ~~subscription~~ module. The POWER_SIM_ON_REQ message is used for this purpose.

Upon receiving this message, the Server powers the ~~GSM SIM or the UICC~~Identity ~~subscription~~ module on and eventually performs a PPS procedure. After this has been completed, the Server sends the POWER_SIM_ON_RESP message to the Client.

If the POWER_SIM_ON_RESP message indicates that the ~~GSM SIM or the UICC~~Identity ~~subscription~~ module was powered on successfully (see below), the Client shall request the ATR of the ~~GSM SIM or the UICC~~Identity

subscription module with the TRANSFER_ATR_REQ message. The Server will then 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 ~~GSM SIM or the UICC~~~~Identity~~ subscription module ~~card~~:

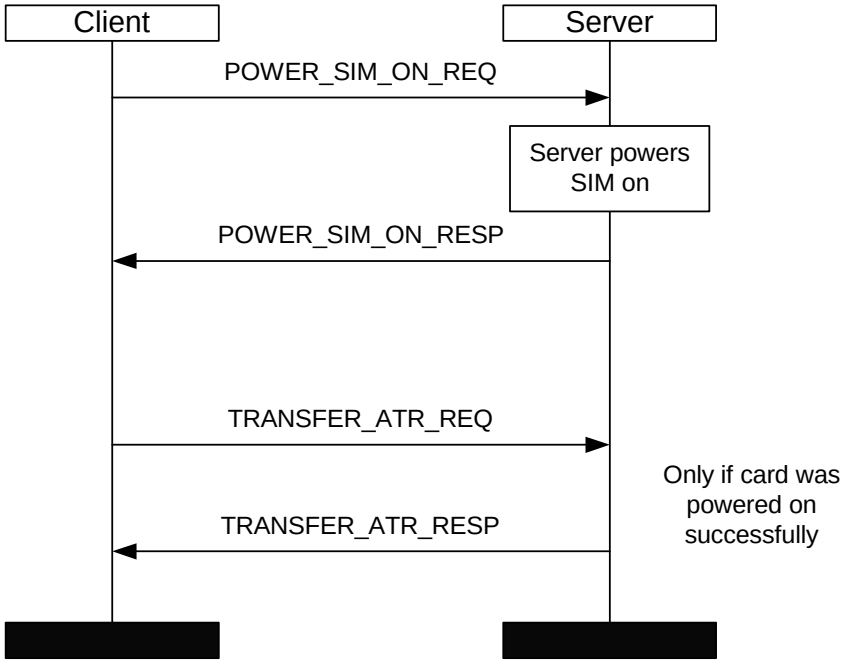

Figure 4-7 Client requests Server to power the SIM on

If no error has occurred, the POWER_SIM_ON_RESP message will contain the result code "OK, request processed correctly" (see Section 5.3.4).

In case of an error, the POWER_SIM_ON_RESP message will contain an appropriate result code (see also Section 5.3.4):

- If the card is removed from the Server, the result code "Error, card removed" is used.
- If the card is inserted in the Server but cannot be powered on, the result code "Error, card not accessible" is used.
- If the card is inserted in the Server but already powered on, the result code "Error, card (already) powered on" is 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" is used.

4.8 Reset SIM

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

The Client can then send the RESET_SIM_REQ message to the Server. Upon receiving this message, the Server resets the ~~GSM SIM or the UICC~~~~Identity~~ subscription module and eventually performs a PPS procedure. After this has been completed, the Server sends the RESET_SIM_RESP message to the Client.

If the RESET_SIM_RESP message indicates that the ~~GSM SIM or the UICC~~~~Identity~~ subscription module was reset on successfully (see below), the Client shall request the ATR of the ~~GSM SIM or the UICC~~~~Identity~~ subscription module with the TRANSFER_ATR_REQ message. The Server will then 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 ~~GSM SIM or the UICC~~~~Identity~~ subscription module card:

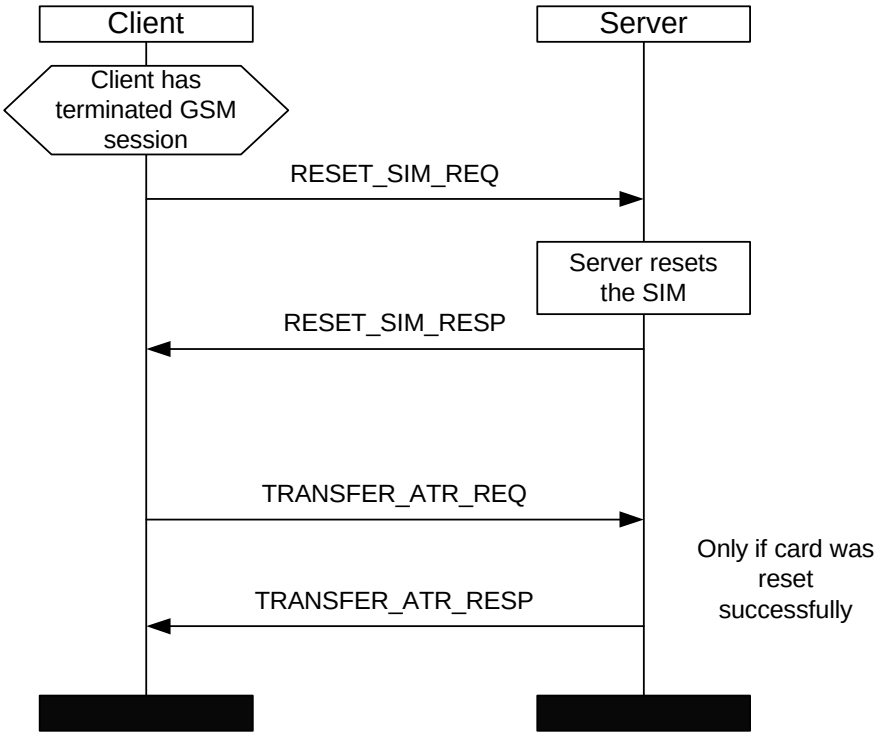

Figure 4-8 Client requests the Server to reset the SIM

If no error has occurred, the RESET_SIM_RESP message will contain the result code "OK, request processed correctly" (see Section 5.3.4).

In case of an error, the RESET_SIM_RESP message will contain an appropriate result code (see also Section 5.3.4):

- If the card is removed from the Server, the result code "Error, card removed" is used.
- If the card is inserted in the Server but cannot be reset, the result code "Error, card not accessible" is used.
- If the card is inserted in the Server and powered off, the result code "Error, card (already) powered off" is used. In this case, the Server shall not perform any actions, e. g. 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" is 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:

- AAn GSM SIM or a UICCIdentity subscription module is inserted in the Server and has been powered on or reset prior to the SIM Access Profile connection. In this case, the STATUS_IND message has the parameter "Card_reset".
- AAn GSM SIM or a UICCIdentity subscription module is inserted in the Server, but cannot be powered on or is not accessible. In this case, the STATUS_IND message has the parameter "Card_not_accessible".
- No GSM SIM or UICCIdentity 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 GSM SIM or the UICCIdentity subscription module status can occur:

- The GSM SIM or the UICCIdentity subscription module is removed from the Server. In this case, the STATUS_IND message with the parameter "Card_removed" shall be sent.
- AAn GSM SIM or a UICCIdentity 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 GSM SIM or the UICCIdentity subscription module into use, it has to power it on.
- While the GSM SIM or the UICCIdentity subscription module remains inserted in the Server, the physical contact between Server and the GSM SIM or the UICCIdentity 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 ~~GSM SIM or UICC~~~~Identity~~ subscription module is not responding to e. g. Command APDUs. In any case, the behavior of the Client shall be inline with the GSM specifications ~~and~~ 3GPP specifications and 3GPP2 specifications
[3], ~~and~~ [4], [6], [7] ~~and~~ [8], [9], [10], [11].

Figure 4-9 illustrates the case when the Server detects a change in the physical connection to the card:

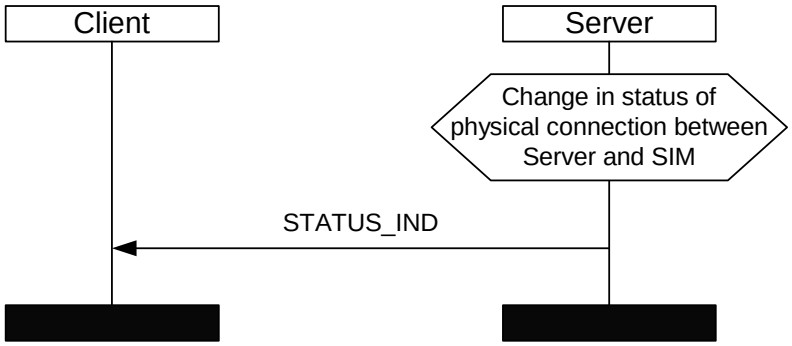

Figure 4-9 Server reports status change to the Client

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 sends 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:

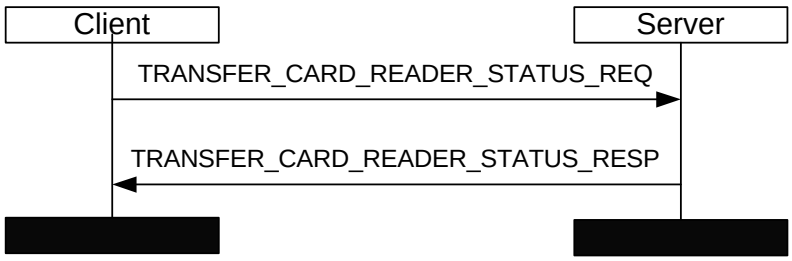

Figure 4-10 Request Card Reader Status

If no error has occurred, the TRANSFER_CARD_READER_STATUS_RESP message will also contain the result code "OK, request processed correctly" (see Section 5.3.4). In case of an error, the TRANSFER_CARD_READER_STATUS_RESP message will only contain an appropriate result code (see also Section 5.3.4):

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

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

4.11 Error Response

The Server sends 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).

It is up to the Client, if it wants to close the SIM Access Profile Connection after it has received an ERROR_RESP message from the Server.

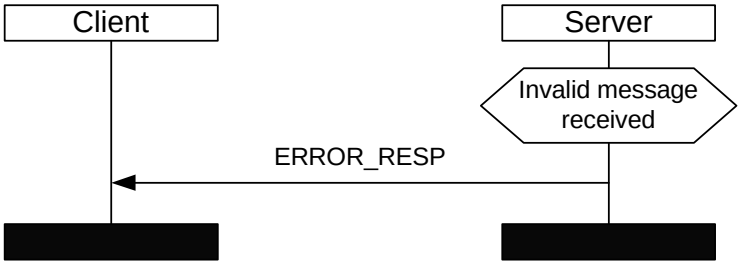

Figure 4-11 Error Response message

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 (e.g. TRANSFER_APDU_RESP).

4.12 State Machine

Figure 4-12 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.

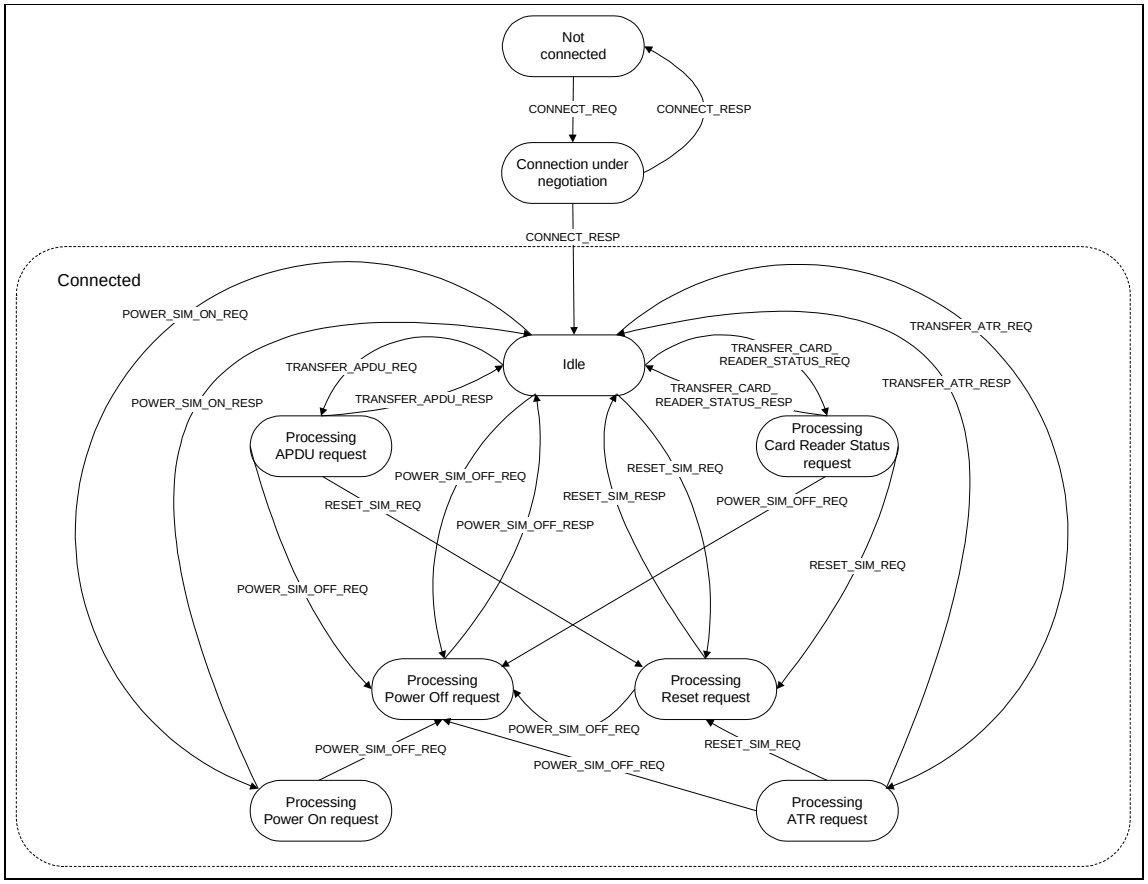

Figure 4-12 Simplified state machine

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 ~~GSM SIM or UICC~~~~Identity~~ 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 can 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 can 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

A Bluetooth link loss can be detected by the Server or the Client. Whenever either device detects a Bluetooth link loss, the SIM Access Profile connection is automatically terminated.

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

Message are formatted as shown in Figure 5-1 (length of each field is given in bytes):

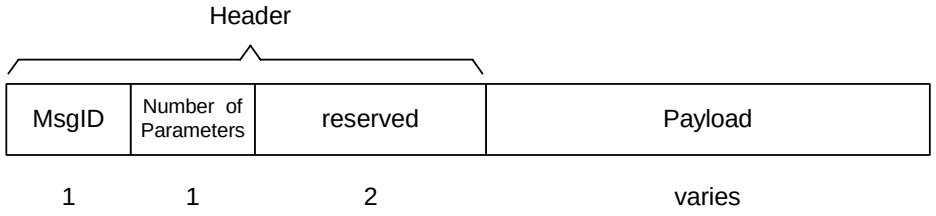

Figure 5-1 Message Format

The message header consists of three fields. The field "MsgID" contains the message ID as given in Section 5.2. 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:

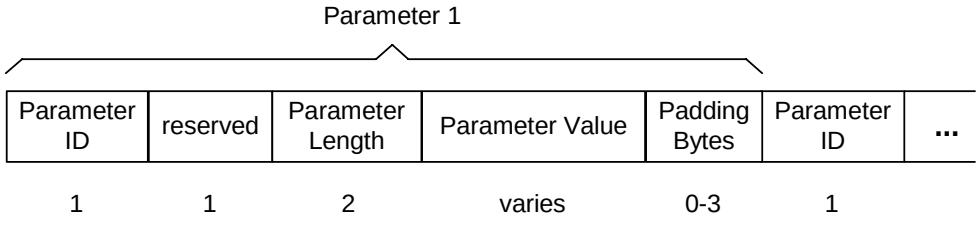

Figure 5-2 Payload Coding

The fields "Parameter ID", "Parameter Length", "Parameter Value", the reserved field and the "Padding Bytes" are repeated for each parameter. The ordering of the parameter is as listed in the tables in Section 5.2.

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" contains the ID of the parameter as listed in Section 5.3. The "Parameter Length" field gives the length of the "Parameter Value" (see Section 5.3).

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".

5.2 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

Table 3 Message Overview

5.2.1 CONNECT_REQ

The CONNECT_REQ message contains the following parameter:

Parameter	Ref.	Status
MaxMsgSize	5.3.1	M

Table 4: Parameter of the CONNECT_REQ message

The parameter MaxMsgSize is 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).

5.2.2 CONNECT_RESP

The CONNECT_RESP message contains the following parameters:

Parameter	Ref.	Status
ConnectionStatus	5.3.2	M
MaxMsgSize	5.3.1	C (ConnectionStatus)

Table 5: Parameters of the CONNECT_RESP message

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

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

5.2.3 DISCONNECT_REQ

The DISCONNECT_REQ message contains no parameter.

5.2.4 DISCONNECT_RESP

The DISCONNECT_RESP message contains no parameter.

5.2.5 DISCONNECT_IND

The DISCONNECT_IND message contains the following parameter:

Parameter	Ref.	Status
DisconnectionType	5.3.3	M

Table 6: Parameter of the DISCONNECT_IND message

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

5.2.6 TRANSFER_APDU_REQ

The TRANSFER_APDU_REQ message contains the following parameter:

Parameter	Ref.	Status
CommandAPDU	5.3.5	M

Table 7: Parameter of the TRANSFER_APDU_REQ message

5.2.7 TRANSFER_APDU_RESP

The TRANSFER_APDU_RESP message contains the following parameters:

Parameter	Ref.	Status
ResultCode	5.3.4	M
ResponseAPDU	5.3.5	C (ResultCode)

Table 8: Parameter of the TRANSFER_APDU_RESP message

The parameter ResultCode indicates, if the Command APDU was processed correctly. Any error response from the ~~GSM SIM card or the UICC card Identity~~ subscription module interface to the Server is mapped onto this field.

The parameter ResponseAPDU is only included, if the Command APDU was processed correctly and no other error occured.

5.2.8 TRANSFER_ATR_REQ

The TRANSFER_ATR_REQ message contains no parameter.

5.2.9 TRANSFER_ATR_RESP

The TRANSFER_ATR_RESP message contains the following parameters:

Parameter	Ref.	Status
ResultCode	5.3.4	M
ATR	5.3.6	C (ResultCode)

Table 9: Parameters of the TRANSFER_ATR_RESP message

The parameter ResultCode includes possible error codes.

The parameter ATR includes the Answer to Reset from the ~~GSM SIM or the UICCIdentity~~ subscription module. It is only included if no error has occurred.

5.2.10 POWER_SIM_OFF_REQ

The POWER_SIM_OFF_REQ message contains no parameter.

5.2.11 POWER_SIM_OFF_RESP

The POWER_SIM_OFF_RESP message contains the following parameter:

Parameter	Ref.	Status
ResultCode	5.3.4	M

Table 10: Parameter of the POWER_SIM_OFF_RESP message

The parameter ResultCode includes possible error codes.

5.2.12 POWER_SIM_ON_REQ

The POWER_SIM_ON_REQ message contains no parameter.

5.2.13 POWER_SIM_ON_RESP

The POWER_SIM_ON_RESP message contains the following parameter:

Parameter	Ref.	Status
ResultCode	5.3.4	M

Table 11: Parameter of the POWER_SIM_ON_RESP message

The parameter ResultCode includes possible error codes and indicates, if the ~~GSM SIM or the UICC~~~~Identity~~ subscription module was powered on successfully.

5.2.14 RESET_SIM_REQ

The RESET_SIM_REQ message contains no parameter.

5.2.15 RESET_SIM_RESP

The RESET_SIM_RESP message contains the following parameter:

Parameter	Ref.	Status
ResultCode	5.3.4	M

Table 12: Parameter of the RESET_SIM_RESP message

The parameter ResultCode includes possible error codes and indicates, if the ~~GSM SIM or the UICC~~~~Identity~~ subscription module was successfully reset.

5.2.16 STATUS_IND

The message STATUS_IND is used to indicate (a change in) the availability of the SIM. The STATUS_IND message contains the following parameter:

Parameter	Ref.	Status
StatusChange	5.3.8	M

Table 13: Parameter of the STATUS_IND message

The parameter StatusChange includes the reason for the status change.

5.2.17 TRANSFER_CARD_READER_STATUS_REQ

The TRANSFER_CARD_READER_STATUS_REQ message contains no parameter.

5.2.18 TRANSFER_CARD_READER_STATUS_RESP

The TRANSFER_CARD_READER_STATUS_RESP message contains the following parameters:

Parameter	Ref.	Status
ResultCode	5.3.4	M
CardReaderStatus	5.3.7	C (ResultCode)

Table 14: 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 is only included if no error has occurred.

5.2.19 ERROR_RESP

The ERROR_RESP message contains no parameter.

5.3 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
Command APDU	Varies	0x04
Response APDU	Varies	0x05
ATR	Varies	0x06
CardReaderStatus	1	0x07
StatusChange	1	0x08

Table 15 List of Parameter IDs

5.3.1 MaxMsgSize

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

5.3.2 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
Reserved	All others

Table 16 Possible values for ConnectionStatus

5.3.3 DisconnectionType

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

Possible values for **DisconnectionType**	**Value**
Graceful	0x00
Immediate	0x01
Reserved	All others

Table 17 Possible values for DisconnectType

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

5.3.4 ResultCode

The parameter ResultCode is a one byte field. The values are as given in the following table, 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**
OK, request processed correctly	0x00	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
Reserved	All others						

Table 18 Possible values for ResultCode

5.3.5 CommandAPDU and ResponseAPDU

The parameter CommandAPDU and ResponseAPDU contain an APDU that is coded in accordance with:

- the GSM 11.11 specification for the GSM application; ~~and~~
- the TS 102.221 specification for the USIM application.
- The TIA/EIA/IS-820 and TIA/EIA/IS-820-1 specification for the R-UIM application

5.3.6 ATR

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

5.3.7 CardReaderStatus

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

5.3.8 StatusChange

The parameter StatusChange includes the reason for the change in the Status of the ~~GSM SIM or the UICC~~Identity subscription module ~~card~~. The possible values are given in the following table:

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 19 Possible values for StatusChange

5.4 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 Chapter 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 20 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	GenericTelephony		M	
ServiceClass1		UUID	SIM Access		M	
Protocol Descriptor List					M	
Protocol #0		UUID	L2CAP		M	
Protocol #1		UUID	RFCOMM		M	
ProtocolSpecificParameter0	ServerChannel	Uint8	N=server channel #		M	
BluetoothProfileDescriptorList					M	
Profile0	SupportedProfile	UUID	SIM Access		M	
Parameter for Profile #0	Version	Uint16	0x0100[5]		M	
Service Name	Displayable Text name	String	Service-provider defined		O	"SIM Access"

Table 20 SDP entry for SIM Access Server

[5] Indicating version 1.0

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 text together with the associated subclauses 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.

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 can 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

The table 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 21 Generic Access Profile modes

8.2 Security Aspects

The table shows the support status for Security aspects within the SIM Access Profile. Either Security Mode 2 or 3 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
3	Encryption	M	M
C1: Support for at least one of the security modes 2 and 3 is mandatory. 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 22 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 23 Idle mode procedures

9 References

[1] Specification of the Bluetooth System 1.1

[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 Identity Module - Mobile Equipment (SIM-ME) Interface

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

[5] CAR_010_MRD/1.0, “Bluetooth SIG Car Profile Working Group MRD”

[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 Identity Module (R-UIM) for TIA/EIA Spread Spectrum Standards

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

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

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)
GSM	Global System for Mobile Communications
GSM SIM	GSM Subscriber Identity Module
L2CAP	Logical Link Control and Adaptation Protocol
LC	Link Controller
LM	Link Manager
LMP	Link Manager Protocol
ME	Mobile Equipment
PIN	Personal Identification Number
PPS	Parameter and Protocol Selection
PRNG	Pseudo Random Number Generator
SIM	Subscriber Identity Module
UICC	UMTS term for the physical card
USIM	Universal Subscriber Identity Module
R-UIM	Removable User Identity Module

11 List of Figures

12 List of Tables