



---

## LLD ACI CSIM

---

Project	G23-GSM Protocol Stack
Document Type	Technical Documentation
Title	LLD ACI CSIM
Author	Thomas Lüttig
Creation Date	28 July, 2003
Last Modified	28 July, 2003
ID and Version	8462.717.03.001
Status	Being Processed

Copyright © 2003 Texas Instruments, Inc. All rights reserved.

**Texas Instruments Proprietary Information – Strictly Private**

## **0 Document Control**

© Copyright Texas Instruments, Inc. 2003  
All rights reserved.

Every effort has been made to ensure that the information contained in this document is accurate at the time of printing. However, the software described in this document is subject to continuous development and improvement. Texas Instruments reserves the right to change the specification of the software. Information in this document is subject to change without notice and does not represent a commitment on the part of Texas Instruments. Texas Instruments accepts no liability for any loss or damage arising from the use of any information contained in this document.

The software described in this document is furnished under a license agreement and may be used or copied only in accordance with the terms of the agreement. It is an offence to copy the software in any way except as specifically set out in the agreement. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of Texas Instruments.

### **0.1 Document History**

ID	Author	Date	Status
----	--------	------	--------

### **0.2 References, Abbreviations, Terms**

[TI 7010.801] 7010.801, References and Vocabulary, Texas Instruments.

[1] ETSI Specification GSM 07.07

[2] ETSI Specification GSM 11.11

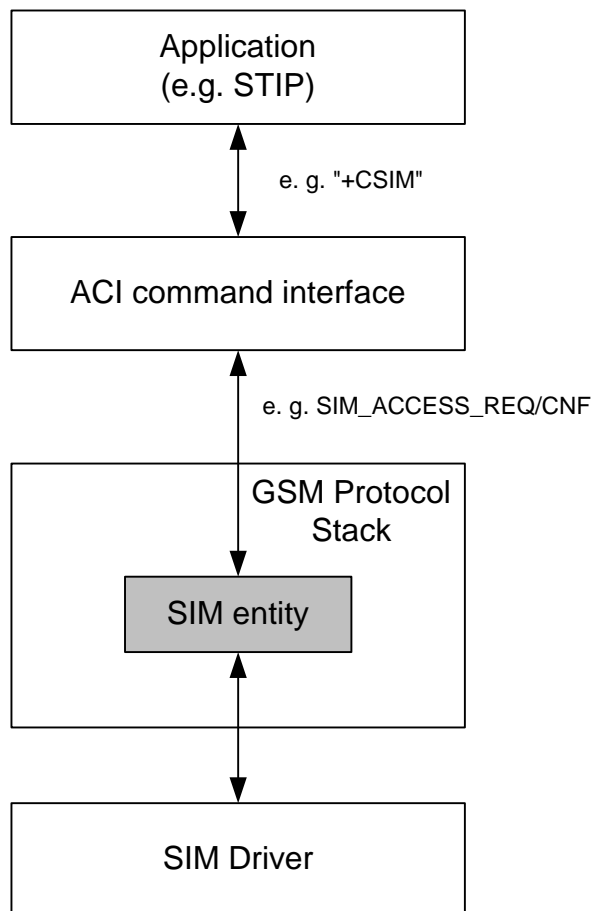
## Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>2</b>
<b>2</b>	<b>Overview .....</b>	<b>3</b>
<b>3</b>	<b>Interface description .....</b>	<b>4</b>
3.1	Generic SIM access .....	4
3.1.1	AT command .....	4
3.1.1.1	AT+CSIM .....	4
3.1.2	Data types.....	5
3.1.2.1	T_SIM_TRNS_ACC_PRM .....	5
3.1.2.2	T_SIM_TRNS_RSP_PRM .....	5
3.1.3	Functional interface .....	5
3.1.3.1	sAT_PlusCSIM .....	5
3.1.3.2	rAT_PlusCSIM .....	6
3.1.4	MSC .....	6
3.2	Answer to reset.....	7
3.2.1	AT command .....	7
3.2.1.1	AT%ATR.....	7
3.2.2	Functional interface .....	7
3.2.2.1	qAT_PercentATR.....	7

## **1 Introduction**

This document describes the modifications and implementation of CSIM/APDU feature in the ACI. Therefore two new AT commands will be introduced, AT%ATR (answer-to-reset) and AT+CSIM. AT%ATR is a proprietary command but AT+CSIM can be found in ETSI specification GSM 07.07 [1].

## 2 Overview



### 3 Interface description

#### 3.1 Generic SIM access

##### 3.1.1 AT command

##### 3.1.1.1 AT+CSIM

**Table 1: +CSIM parameter command syntax**

Command	Possible response(s)
+CSIM=<length>,<command>	+CSIM: <length>,<response> +CME ERROR: <err>
+CSIM=?	

##### **Description**

Set command transmits to the ME the <command> it then shall send as it is to the SIM. In the same manner the SIM <response> shall be sent back by the ME to the TA as it is.

This command allows a direct control of the SIM by an distant application on the TE. The TE shall then take care of processing SIM information within the frame specified by GSM.

NOTE: Compared to Restricted SIM Access command +CRSM, the definition of +CSIM allows TE to take more control over the SIM-ME interface. The locking and unlocking of the interface may be done by a special <command> value or automatically by TA/ME (by interpreting <command> parameter). In case that TE application does not use the unlock command (or does not send a <command> causing automatic unlock) in a certain timeout value, ME may release the locking.

##### **Defined values**

- <length> : integer type; length of the characters that are sent to TE in <command> or <response> (two times the actual length of the command or response)
- <command> : command passed on by the ME to the SIM in the format as described in GSM 11.11 [2] (hexadecimal character format; refer +CSCS)
- <response> : response to the command passed on by the SIM to the ME in the format as described in GSM 11.11 [2] (hexadecimal character format; refer +CSCS)

The description for this AT command is taken from ETSI specification GSM 07.07 [1].

### 3.1.2 Data types

#### 3.1.2.1 T\_SIM\_TRNS\_ACC\_PRM

typedef struct SIMTrnsAccPrm

```
{
    UBYTE      cmd;          /* access command */
    USHORT     reqDataFld;    /* requested datafield identifier */
    UBYTE      p1;           /* parameter 1 */
    UBYTE      p2;           /* parameter 2 */
    UBYTE      p3;           /* parameter 3 */
    USHORT     dataLen;       /* data length in bytes */
    UBYTE      *transData;    /* points to data buffer */
} T_SIM_TRNS_ACC_PRM;
```

For +CSIM the field *cmd* has the value SIM\_TRANSP\_CMD (taken from SIM SAP). The *transData* points to all transparent data that will be sent to the SIM entity. The data type of *dataLen* was changed from UBYTE to ULONG, because the *transData* can have a maximum length of 262 bytes (in SIM SAP: MAX\_SIM\_TRANSP). The fields *p1*, *p2*, *p3* and *reqDataFld* are not used in this case.

#### 3.1.2.2 T\_SIM\_TRNS\_RSP\_PRM

typedef struct

```
{
    UBYTE      sw1;          /* SIM result code 1 */
    UBYTE      sw2;          /* SIM result code 2 */
    USHORT     rspLen;       /* length of response data */
    UBYTE      *rsp;         /* pointer to response data */
} T_SIM_TRNS_RSP_PRM;
```

This data structure contains the response data that are received from the SIM entity. The data type of *rsp* was changed from UBYTE to USHORT because the maximum length of the response data can be 256 bytes (in SIM SAP: MAX\_SIM\_CMD).

### 3.1.3 Functional interface

#### 3.1.3.1 sAT\_PlusCSIM

Prototype:

```
T_ACI_RETURN sAT_PlusCSIM (T_ACI_CMD_SRC    srcId,
                           USHORT           dataLen,
                           UBYTE            *data);
```

Parameters:

<i>src_id</i>	source identifier
<i>dataLen</i>	length of data in <i>data</i>
<i>data</i>	data which are sent to the SIM (max. length: 262 bytes)

Return:

AT_EXCT	execution of command is in progress
AT_FAIL	execution of command failed
AT_BUSY	execution of command is rejected due to a busy command handler

**Description:**

This function allows sending data to the SIM. This data must be formatted as described in GSM 11.11. [2]

**3.1.3.2 rAT\_PlusCSIM**

**Prototype:**

```
void rAT_PlusCSIM (SHORT      rspLen,
                   UBYTE      *rsp );
```

**Parameters:**

<i>rspLen</i>	length of response data in bytes
<i>rsp</i>	response data including sw1 and sw2 (max. length: 258 bytes)

**Return:**

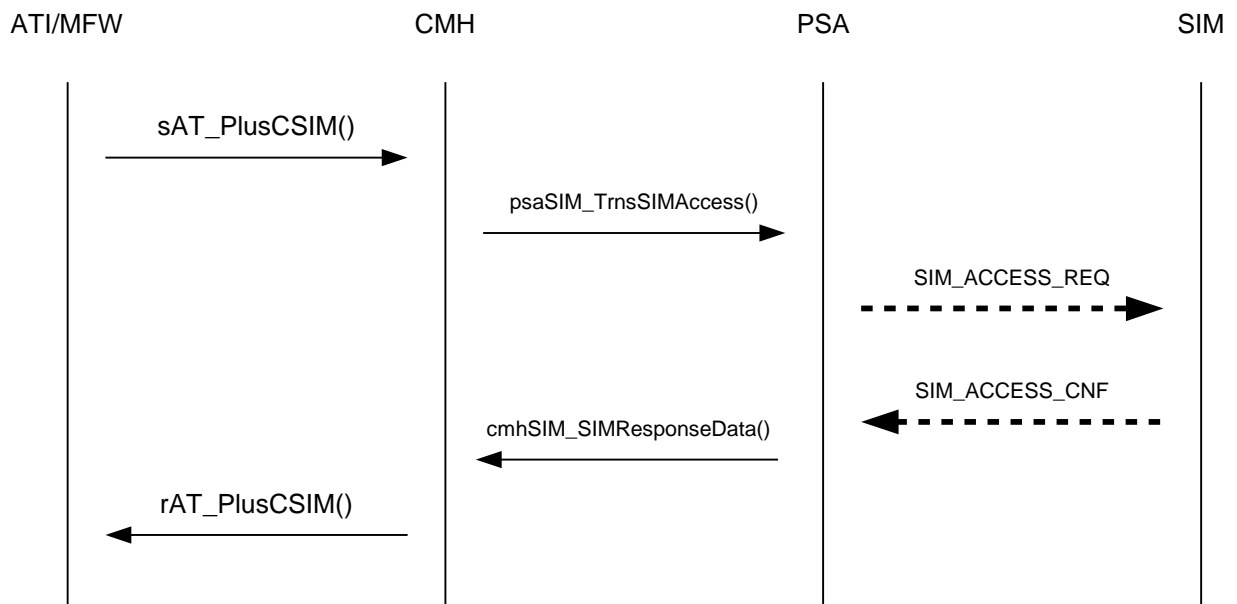
**void**

**Description:**

Informs MFW/ATI about the response data that received from the SIM.

**3.1.4 MSC**

```
[Generic SIM Access, set command]
AT+CSIM= 18,81A400000200053100
+CSIM: 12,800200509000
OK
```





## 3.2 Answer to reset

### 3.2.1 AT command

#### 3.2.1.1 AT%ATR

**Table 2: %ATR parameter command syntax**

Command	Possible response(s)
%ATR?	%ATR: <phase>, <atr> +CME ERROR: <err>
%ATR=?	

#### Description

The query command can be used by an application to obtain information about the phase, status and answer to reset (ATR) of the SIM.

#### Defined values

<phase> : integer type; phase of the SIM that is stored in the EF Phase (GSM 11.11 [2])

<atr> : answer to reset (hexadecimal character format), described in GSM 11.11 [2]

### 3.2.2 Functional interface

#### 3.2.2.1 qAT\_PercentATR

##### Prototype:

```
T_ACL_RETURN qAT_PercentATR (T_ACL_CMD_SRC srcId,
                               UBYTE *phase,
                               UBYTE *atr_info);
```

##### Parameters:

*src\_id* source identifier

*phase* phase of the SIM card

*atr\_info* atr (answer to reset) according to GSM 11.11 [2] (max. length: 33 bytes)

##### Return:

**AT\_FAIL** execution of command failed

**AT\_CMPL** execution of command completed

##### Description:

Queries the phase and atr info. The atr is received when switching the mobile on. The phase is received after PIN1 is entered.