



# **GSM** **T**ECHNICAL **S**PECIFICATION

**GSM 11.11**

July 1996

Version 5.3.0

Source: ETSI TC-SMG

Reference: TS/SMG-091111QR1

ICS: 33.060.50

**Key words:** Digital cellular telecommunications system, Global System for Mobile communications (GSM)



## **Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface; (GSM 11.11)**

**ETSI**

European Telecommunications Standards Institute

**ETSI Secretariat**

**Postal address:** F-06921 Sophia Antipolis CEDEX - FRANCE

**Office address:** 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE

**X.400:** c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 66 - Fax: +33 93 65 28 17

**Copyright Notification:** No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1996. All rights reserved.

|         |                                                                                |    |
|---------|--------------------------------------------------------------------------------|----|
| 10.1.1  | EF <sub>ICC</sub> ID (ICC Identification).....                                 | 51 |
| 10.2    | Contents of files at the GSM application level .....                           | 51 |
| 10.2.1  | EF <sub>LP</sub> (Language preference) .....                                   | 51 |
| 10.2.2  | EF <sub>IMSI</sub> (IMSI).....                                                 | 52 |
| 10.2.3  | EF <sub>Kc</sub> (Ciphering key Kc).....                                       | 53 |
| 10.2.4  | EF <sub>PLMNsel</sub> (PLMN selector).....                                     | 54 |
| 10.2.5  | EF <sub>HPLMN</sub> (HPLMN search period) .....                                | 54 |
| 10.2.6  | EF <sub>ACMmax</sub> (ACM maximum value).....                                  | 55 |
| 10.2.7  | EF <sub>SST</sub> (SIM service table).....                                     | 56 |
| 10.2.8  | EF <sub>ACM</sub> (Accumulated call meter) .....                               | 58 |
| 10.2.9  | EF <sub>GID1</sub> (Group Identifier Level 1) .....                            | 58 |
| 10.2.10 | EF <sub>GID2</sub> (Group Identifier Level 2) .....                            | 58 |
| 10.2.11 | EF <sub>SPN</sub> (Service Provider Name).....                                 | 59 |
| 10.2.12 | EF <sub>PUCT</sub> (Price per unit and currency table).....                    | 59 |
| 10.2.13 | EF <sub>CBMI</sub> (Cell broadcast message identifier selection).....          | 60 |
| 10.2.14 | EF <sub>BCCH</sub> (Broadcast control channels).....                           | 61 |
| 10.2.15 | EF <sub>ACC</sub> (Access control class).....                                  | 61 |
| 10.2.16 | EF <sub>FPLMN</sub> (Forbidden PLMNs) .....                                    | 62 |
| 10.2.17 | EF <sub>LOC</sub> i (Location information) .....                               | 62 |
| 10.2.18 | EF <sub>AD</sub> (Administrative data) .....                                   | 64 |
| 10.2.19 | EF <sub>Phase</sub> (Phase identification) .....                               | 65 |
| 10.2.20 | EF <sub>VGCS</sub> (Voice Group Call Service).....                             | 65 |
| 10.2.21 | EF <sub>VGCSS</sub> (Voice Group Call Service Status).....                     | 66 |
| 10.2.22 | EF <sub>VBS</sub> (Voice Broadcast Service).....                               | 67 |
| 10.2.23 | EF <sub>VBSS</sub> (Voice Broadcast Service Status).....                       | 67 |
| 10.2.24 | EF <sub>eMLPP</sub> (enhanced Multi Level Preemption and Priority).....        | 68 |
| 10.2.25 | EF <sub>AAeM</sub> (Automatic Answer for eMLPP Service) .....                  | 69 |
| 10.2.26 | EF <sub>CBMID</sub> (Cell Broadcast Message Identifier for Data Download)..... | 70 |
| 10.2.27 | EF <sub>ECC</sub> (Emergency Call Codes) .....                                 | 70 |
| 10.2.28 | EF <sub>CBMIR</sub> (Cell broadcast message identifier range selection).....   | 71 |
| 10.3    | Contents of files at the telecom level .....                                   | 72 |
| 10.3.1  | EF <sub>ADN</sub> (Abbreviated dialling numbers).....                          | 72 |
| 10.3.2  | EF <sub>FDN</sub> (Fixed dialling numbers).....                                | 75 |
| 10.3.3  | EF <sub>SMS</sub> (Short messages).....                                        | 75 |
| 10.3.4  | EF <sub>CCP</sub> (Capability configuration parameters) .....                  | 76 |
| 10.3.5  | EF <sub>MSISDN</sub> (MSISDN) .....                                            | 77 |
| 10.3.6  | EF <sub>SMSP</sub> (Short message service parameters).....                     | 78 |
| 10.3.7  | EF <sub>SMSS</sub> (SMS status) .....                                          | 79 |
| 10.3.8  | EF <sub>LND</sub> (Last number dialled).....                                   | 80 |
| 10.3.9  | EF <sub>SDN</sub> (Service Dialling Numbers).....                              | 80 |
| 10.3.10 | EF <sub>EXT1</sub> (Extension1).....                                           | 81 |
| 10.3.11 | EF <sub>EXT2</sub> (Extension2).....                                           | 82 |
| 10.3.12 | EF <sub>EXT3</sub> (Extension3).....                                           | 83 |
| 10.4    | Files of GSM (figure 8) .....                                                  | 83 |
| 11      | Application protocol .....                                                     | 85 |
| 11.1    | General procedures.....                                                        | 86 |
| 11.1.1  | Reading an EF .....                                                            | 86 |
| 11.1.2  | Updating an EF.....                                                            | 86 |
| 11.1.3  | Increasing an EF .....                                                         | 87 |
| 11.2    | SIM management procedures.....                                                 | 87 |
| 11.2.1  | SIM initialisation.....                                                        | 87 |
| 11.2.2  | GSM session termination .....                                                  | 88 |
| 11.2.3  | Emergency Call Codes.....                                                      | 88 |
| 11.2.4  | Language preference .....                                                      | 88 |
| 11.2.5  | Administrative information request;.....                                       | 89 |
| 11.2.6  | SIM service table request.....                                                 | 89 |
| 11.2.7  | SIM phase request .....                                                        | 89 |
| 11.2.8  | SIM Presence Detection and Proactive Polling .....                             | 89 |
| 11.3    | CHV related procedures.....                                                    | 89 |

A subscriber authentication key Ki is used in this procedure. This key Ki has a length of 128 bits and is stored within the SIM for use in the algorithms described below.

## 7.2 Algorithms and processes

The names and parameters of the algorithms supported by the SIM are defined in TS GSM 03.20 [11]. These are:

- Algorithm A3 to authenticate the MS to the network;
- Algorithm A8 to generate the encryption key.

These algorithms may exist either discretely or combined (into A38) within the SIM. In either case the output on the SIM/ME interface is 12 bytes. The inputs to both A3 and A8, or A38, are Ki (128 bits) internally derived in the SIM, and RAND (128 bits) across the SIM/ME interface. The output is SRES (32 bits)/Kc (64 bits) the coding of which is defined in the command RUN GSM ALGORITHM in clause 9.

## 7.3 File access conditions

Every file has its own specific access condition for each command. The relevant access condition of the last selected file shall be fulfilled before the requested action can take place.

For each file:

- the access conditions for the commands READ and SEEK are identical;
- the access conditions for the commands SELECT and STATUS are ALWays.

No file access conditions are currently assigned by GSM to the MF and the DFs.

The access condition levels are defined in the following table:

**Table 7: Access condition level coding**

| Level   | Access Condition            |
|---------|-----------------------------|
| 0       | ALWays                      |
| 1       | CHV1                        |
| 2       | CHV2                        |
| 3       | Reserved for GSM Future Use |
| 4 to 14 | ADM                         |
| 15      | NEVer                       |

The meaning of the file access conditions is as follows:

**ALWAYS:** the action can be performed without any restriction;

**CHV1** (card holder verification 1): the action shall only be possible if one of the following three conditions is fulfilled:

- a correct CHV1 value has already been presented to the SIM during the current session;
- the CHV1 enabled/disabled indicator is set to "disabled";
- UNBLOCK CHV1 has been successfully performed during the current session;

**CHV2:** the action shall only be possible if one of the following two conditions is fulfilled:

- a correct CHV2 value has already been presented to the SIM during the current session;
- UNBLOCK CHV2 has been successfully performed during the current session;

**ADM:** allocation of these levels and the respective requirements for their fulfilment are the responsibility of the appropriate administrative authority;