# GSM TECHNICAL SPECIFICATION

**GSM 02.22**

**December 1996**

**Version 5.2.0**

Source: ETSI TC-SMG

Reference: TS/SMG-010222Q

ICS: 33.020

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

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

# Digital cellular telecommunications system (Phase 2+); Personalization of GSM Mobile Equipment (ME) Mobile functionality specification (GSM 02.22)

**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 4 92 94 42 00 - Fax: +33 4 93 65 47 16

# Contents

Foreword ..... 5

1 Scope ..... 7

2 Normative references ..... 7

3 Definitions and abbreviations ..... 8
3.1 Abbreviations ..... 8
3.2 Definitions ..... 8

4 General description ..... 9

5 Network personalization ..... 9
5.1 Network personalization ..... 9
5.1.1 Operation of network personalized ME ..... 10
5.1.2 Network personalization cycle ..... 10
5.1.2.1 Personalization cycle ..... 10
5.1.2.2 De-personalization cycle ..... 10
5.2 Network subset personalization ..... 11
5.2.1 Operation of Network subset personalized ME ..... 11
5.2.2 Network subset personalization cycle ..... 11
5.2.2.1 Personalization Cycle ..... 11
5.2.2.2 De-personalization cycle ..... 12

6 SP personalization ..... 12
6.1 Operation of SP personalized MEs ..... 13
6.2 SP personalization cycle ..... 13
6.2.1 Personalization cycle ..... 13
6.2.2 De-personalization cycle ..... 14

7 Corporate personalization ..... 14
7.1 Operation of corporate personalized MEs ..... 14
7.2 Corporate personalization cycle ..... 15
7.2.1 Personalization cycle ..... 15
7.2.2 De-personalization cycle ..... 16

8 SIM personalization ..... 16
8.1 Operation of SIM personalized ME ..... 16
8.2 SIM personalization cycle ..... 17
8.2.1 Personalization cycle ..... 17
8.2.2 De-personalization cycle ..... 17

9 Over the air de-personalization cycle ..... 17

10 Disable Personalization ..... 18

11 Manufacturer personalization and de-personalization ..... 19

12 Automatic personalization ..... 19

13 Personalization Cycle Restrictions ..... 19

14 Security ..... 19

Annex A (normative): Technical information ..... 21

A.1 GID1 and GID2 files ..... 21

A.2 Emergency calls only mode ..... 21

A.3 Co-operative Network List ..... 21

A.4 Over-the-air de-personalization ..... 21

History ..... 23

## Foreword

This Global System for Mobile communications Technical Specification (GTS) has been produced by the Special Mobile Group (SMG) Technical Committee (TC) of the European Telecommunications Standards Institute (ETSI).

This GTS provides functional specifications of five features to personalize GSM Mobile Equipment (ME) within the digital cellular telecommunications system.

The contents of this GTS are subject to continuing work within TC-SMG and may change following formal TC-SMG approval. Should TC-SMG modify the contents of this GTS it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version 5.x.y

where:

- y the third digit is incremented when editorial only changes have been incorporated in the specification;

- x the second digit is incremented for all other types of changes, i.e. technical enhancements, corrections, updates, etc.

Blank page

# 1 Scope

This Global System for Mobile communications Technical Specification (GTS) provides functional specifications of five features to personalize GSM Mobile Equipment (ME). These features are called:

- Network personalization;
- Network subset personalization;
- Service Provider (SP) personalization;
- Corporate personalization;
- Subscriber Identity Module (SIM) personalization.

This GTS specifies requirements for MEs which provide these personalization features.

These optional personalization features are stated in GSM 02.07 [2].

# 2 Normative references

This GTS incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this GTS only when incorporated in it by amendment or revision. For undated references, the latest edition of the publication referred to applies.

[1] GSM 01.04 (ETR 350): "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[2] GSM 02.07 (ETS 300 906): "Digital cellular telecommunications system (Phase 2+); Mobile Stations (MS) features".

[3] GSM 02.11 (ETS 300 921): "Digital cellular telecommunications system; Service accessibility".

[4] GSM 03.03 (ETS 300 927): "Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification".

[5] GSM 03.22 (ETS 300 930): "Digital cellular telecommunications system; Functions related to Mobile Station (MS) in idle mode and group receive mode".

[6] GSM 03.38 (ETS 300 900): "Digital cellular telecommunications system (Phase 2+); Alphabets and language-specific information".

[7] GSM 03.40 (ETS 300 901): "Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS) Point-to-Point (PP)".

[8] GSM 04.08 (ETS 300 940): "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification".

[9] GSM 11.11 (ETS 300 977): "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[10] GSM 11.14: "Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

# 3 Definitions and abbreviations

## 3.1 Abbreviations

For the purposes of this GTS, the following abbreviations apply:

| | |
|---|---|
| CCK | Corporate Control Key |
| CNL | Co-operative Network List |
| GID1 | Group Identifier (level 1) |
| GID2 | Group Identifier (level 2) |
| EF | Elementary File |
| IMEI | International Mobile Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| MCC | Mobile Country Code |
| MNC | Mobile Network Code |
| NCK | Network Control Key |
| NSCK | Network Subset Control Key |
| PCK | Personalization Control Key |
| SIM | Subscriber Identity Module |
| SMS | Short Message Service |
| SP | Service Provider |
| SPCK | Service Provider Control Key |
| TMSI | Temporary Mobile Subscriber Identity |

Further GSM abbreviations are given in GSM 01.04 (ETR 350)[1].

## 3.2 Definitions

For the purposes of this GTS, the following definitions apply:

**corporate personalization**: Allows a corporate customer to personalize MEs that he provides for his employees or customers use so that they can only be used with the company's own SIMs.

**de-personalization**: Is the process of deactivating the personalization so that the ME ceases to carry out the verification checks.

**network personalization**: Allows the network operator to personalize a ME so that it can only be used with that particular network operator's SIMs

**network subset personalization:** A refinement of network personalization, which allows network operators to limit the usage of a ME to a subset of SIMs

**normal mode of operation:** Is the mode of operation into which the ME would have gone had no personalization checks been active.

**personalization**: Is the process of storing information in the ME and activating the procedures which verify this information against the corresponding information stored in the SIM whenever the ME is powered up or a SIM is inserted, in order to limit the SIMs with which the ME will operate.

**SIM personalization:** Enables a user to personalize a ME so that it may only be used with particular SIM(s).

**SP personalization:** Allows the service provider to personalize a ME so that it can only be used with that particular service provider's SIMs.

**user:** Normally refers to the person performing the personalization of de-personalization operations and may represent a network operator, service provider, manufacturer of the user/owner of the handset, depending on the context.

# 4 General description

The personalization features work by storing information in the ME which limits the SIMs with which it will operate, and by checking this information against the SIM whenever the ME is powered up or a SIM is inserted. If a check fails, the ME enters the "limited service state" in which only emergency calls can be attempted (see annex A.2).

There are five personalization categories of varying granularity; network, network subset, SP, corporate and SIM. The ME may be personalized to more than one network for each category (except SIM). The personalization categories are independent is so far as each category can be activated of de-activated regardless of the status of the others.

The checks carried out for each personalization category utilize codes for the network(s), network subset, SP, corporate and SIM as shown in table 1. The codes stored in the ME are common to all the personalization categories and are not replicated. However, each category has a separate personalization indicator to show whether it is active or not.

**Table 1: Codes used by each personalization category**

| Code | PLMN(s) (MCC, MNC) | IMSI digits 6 and 7 | SP | Corporate | IMSI digits 8 to 5 |
|---|---|---|---|---|---|
| Personalization category | | | | | |
| Network | ✓ | | | | |
| Network subset | ✓ | ✓ | | | |
| SP | ✓ | | ✓ | | |
| Corporate | ✓ | | ✓ | ✓ | |
| SIM | ✓ | ✓ | | | ✓ |

Precautions must be taken to ensure that when more than one personalization category is to be activated, the new codes are not in conflict with any existing valid codes. To avoid such conflicts, checks are carried out by the ME during the personalization cycle, as described in clause 13.

As an optional ME feature, the status (activated or not) of each personalization category and the values of the relevant codes may be read by the user.

If the ME is personalized to more than one network code, there is significant risk that the SP and corporate codes will loose their uniqueness. To avoid this, common network subset, SP and corporate coding schemes must be jointly administered by the relevant network operators to ensure the unambiguous identification of the relevant SPs and corporates.

# 5 Network personalization

## 5.1 Network personalization

Network personalization allows a ME to be personalized to a particular network, for example to prevent the use of stolen MEs on other networks. The ME may optionally be personalized to more than one network.

The ME is network personalized by storing the code (MCC+MNC) (see GSM 03.03 [4]) of the relevant network(s) in the ME and setting a network personalization indicator in the ME to "on". Whenever a SIM is inserted, or the MS is powered up with a SIM already in place, the International Mobile Subscriber Identity (IMSI) is read from the SIM and the embedded network code (MCC+MNC) checked against that stored in the ME. If the two values differ the MS shall go into emergency calls only mode as defined in annex A.2.

The network personalization feature is controlled by a Network Control Key, (NCK) which has to be entered into the ME in order to network de-personalize it.

In order to support the network personalization feature the ME shall have storage for the network personalization indicator, the network code and the NCK.

### 5.1.1 Operation of network personalized ME

The network personalization check described below is performed whenever a SIM is inserted or the ME is powered up with a SIM already in place.

The personalization check is as follows. When more than one personalization is active in the ME, normal mode of operation includes performing any outstanding personalization checks:

a) **check the ME is network personalized:** The ME checks its network personalization indicator, if it is set to "off" the personalization check shall be stopped and the MS goes into the normal mode of operation, omitting the remaining steps of the check;

b) **check the network code(s):** The ME reads the IMSI from the SIM, extracts the network code from it and checks it against the (list of) value(s) stored on the ME.

If no match is found in b), the ME may display an appropriate message, (e.g., "Incorrect SIM") and shall go into the emergency calls only mode as defined in annex A.2. If a match is found, the MS goes into the normal mode of operation.

### 5.1.2 Network personalization cycle

#### 5.1.2.1 Personalization cycle

The process of personalization can only be carried out on a currently unpersonalized ME, i.e., if the network personalization indicator is set to "off". Access to the personalization process shall be restricted in order to prevent unauthorized, accidental or unwanted personalization. Other restrictions are described in clause 13. In particular, multiple network personalization can only be carried out if no other personalization categories are active. The personalization process results in the NCK being set, the network personalization indicator being set to "on" and the storage in the ME of the network code(s) to which the ME is being personalized.

The network personalization process is as follows:

a) The network code(s) are entered into the ME. This may be accomplished by one of the following means:

- for the case of a single network code, the ME reads the IMSI from the SIM and extracts the network code;
- the ME reads the Co-operative Network List (CNL) from the SIM and extracts the list of network code(s) associated with network personalization;
- keypad entry;
- a manufacturer defined process.

b) The ME carries out the pre-personalization checks contained in clause 13. If they all pass, the network code(s) are stored in the ME. If any fail, the personalization process shall be terminated.

c) THE NCK is stored in the ME. This may be entered via the keypad by the user or by a manufacturer defined process.

d) The network personalization indicator is set to "on".

#### 5.1.2.2 De-personalization cycle

To de-personalize the ME, the correct NCK shall be entered. It is optional whether or not a SIM is inserted in the ME.

Network subset de-personalization shall be possible by keypad entry. If there is no keypad, then an alternative ME-based solution shall be provided. Other de-personalization methods may also be provided such as a network initiated process whereby the control key is sent to the MS over-the-air (see clause 9).

The network de-personalization process is as follows:

a) the NCK is entered into the ME;

b) if the entered NCK is the same as the one stored in the ME the network personalization indicator is set to "off".

If the entered and stored NCK values differ, the de-personalization process shall be stopped. The ME remains personalized and the stored network code(s) and NCK shall be left unchanged.

## 5.2 Network subset personalization

Network subset personalization is a refinement of network personalization, which allows network operators to limit the usage of a ME to a well defined subset of SIMs; e.g. where the ME is the property of a third party.

The ME is network subset personalized by storing the network code and the Network Subset Code (digits 6 and 7 of the IMSI) as an identification of the network subset and setting an network subset personalization indicator in the ME to "on". Whenever a SIM is inserted, or the MS is powered up with a SIM already in place, the network code and the network subset code are read from the SIM and checked against the stored values in the ME. If these values do not match, the ME shall go into emergency calls only mode, as defined in annex A.2.

The network subset personalization feature is controlled by a Network Subset Control Key (NSCK) which has to be entered into the ME in order to network subset de-personalize it.

In order to support the network subset personalization feature, the ME shall have storage for the network subset personalization indicator, the network and network subset codes and the NSCK.

### 5.2.1 Operation of Network subset personalized ME

The Network subset personalization check described below is performed whenever a SIM is inserted or the ME is powered up with a SIM already in place.

The personalization check is as follows. When more than one personalization is active in the ME, normal mode of operation includes performing any outstanding personalization checks.

**a)** **check the ME is network subset personalized:** The ME checks its network subset personalization indicator, if it is set to "off" the personalization check shall be stopped and the ME goes into the normal mode of operation, omitting the remaining steps of the check;

**b)** **check network subset code:** The ME reads the IMSI from the SIM, extracts the network subset code and checks it against the stored value;

**c)** **check the network code(s):** The ME checks the network code extracted from the IMSI against the (list of) stored value(s).

If no match is found in b) or c) the ME may display an appropriate message, (e.g. "Insert correct SIM") and shall go into emergency calls only mode, as defined in annex A.2. Otherwise the ME goes into the normal mode of operation.

### 5.2.2 Network subset personalization cycle

#### 5.2.2.1 Personalization Cycle

The process of personalization can only be carried out on a currently unpersonalized ME, i.e., if the network subset personalization indicator is set to "off". Access to the personalization process shall be restricted in order to prevent unauthorized, accidental or unwanted personalization. Other restrictions are described in clause 13. In particular, network subset personalization cannot be carried out if the ME is personalized to more than one network. The personalization process results in the NSCK being set, the network subset personalization indicator being set to "on" and the storage in the ME of the network and network subset codes which identify the specific network subset to which the ME is being personalized.

The network subset personalization process is as follows:

a) Network and network subset codes are entered into the ME. This may be accomplished by one of the following means:

   - for the case of a single network code, the ME reads the IMSI from the SIM and extracts the network and network subset codes;

   - the ME reads the Co-operative Network List (CNL) from the SIM and extracts the list of network code(s) and the network subset code associated with network subset personalization;

   - keypad entry;

   - a manufacturer defined process.

b) The ME carries out the pre-personalization checks contained in clause 13. If they all pass, the network and network subset codes are stored in the ME. If any fail, the personalization process shall be terminated.

c) The NSCK is stored in the ME. This may be entered via the keypad by the user or by a manufacturer defined process.

d) The network subset personalization indicator is set to "on".

#### 5.2.2.2 De-personalization cycle

To de-personalize the ME the correct NSCK shall be entered. It is optional whether or not a SIM is inserted.

Network subset de-personalization shall be possible by keypad entry. If there is no keypad, then an alternative ME-based solution shall be provided. Other de-personalization methods may also be provided such as a network initiated process whereby the control key is sent to the MS over-the-air (see clause 9).

The network subset de-personalization process is as follows:

a) the NSCK is entered into the ME;

b) if the entered NSCK is the same as the one stored in the ME the network subset personalization indicator is set to "off".

If the entered and stored NSCK values differ, the de-personalization process shall be stopped and the ME remain personalized. The stored network and network subset codes and the NSCK are left unchanged.

## 6 SP personalization

Service provider or SP personalization is a feature which allows a service provider to associate a ME with the SP. This feature only works with SIMs which support the GID1 file. For the purpose of SP personalization the GID1 file is programmed with an SP code that identifies the service provider.

The ME is SP personalized by storing the network SP codes and setting an SP personalization indicator in the ME to "on". Whenever a SIM is inserted, or the ME is powered up with a SIM already in place, the network and SP codes are read and checked against those stored in the ME. If the pairs of values differ the ME shall go into emergency calls only mode as defined in annex A.2.

The SP personalization feature is controlled by a Service Provider Control Key, (SPCK) which has to be entered into the ME in order to SP de-personalize it.

In order to support the SP personalization feature the ME shall have storage for the SP personalization indicator, the network and SP codes and SPCK.

### 6.1 Operation of SP personalized MEs

The personalization check described below is performed whenever a SIM is inserted or the ME is powered up with a SIM already in place.

The personalization check is as follows. When more than one personalization is active in the ME, normal mode of operation includes performing any outstanding personalization checks:

a) **check the ME is SP personalized:** The ME checks the SP personalization indicator, if it is set to "off" the personalization check shall be stopped and the ME goes into its normal mode of operation;

b) **check the SIM supports GID1:** The ME checks that the SIM supports the GID1 file;

c) **check the SP code:** The ME reads the SP code from GID1 file as defined in annex A.1. and checks it against the stored value;

d) **check the network code(s):** The ME reads the IMSI from the SIM, extracts the network code from it and checks it against the (list of) stored value(s).

If b) fails or no match is found in c) or d), the ME may display an appropriate message (e.g. "insert correct SIM") and shall go into emergency calls only mode, as defined in annex A.2. Otherwise, the ME goes into the normal mode of operation.

### 6.2 SP personalization cycle

#### 6.2.1 Personalization cycle

The process of personalization can only be carried out on a currently unpersonalized ME, i.e., if the SP personalization indicator is set to "off". Access to the personalization process shall be restricted in order to prevent unauthorized, accidental or unwanted personalization. Other restrictions are described in clause 13. In particular, SP personalization cannot be carried out if the ME is personalized to more than one network. The personalization process results in the SPCK being set, the SP personalization indicator being set to "on" and the storage in the ME of the network and SP codes to which the ME is being personalized.

The SP personalization process is as follows:

a) The SP code is entered into the ME. This may be accomplished by one of the following means:

- the ME checks that the SIM supports the GID1 file, if not the SP personalization process is aborted with an appropriate error message. The ME reads the SP code from the SIM. If the SP code is set to the default value (see annex A.1) then the personalization process shall be aborted with an appropriate error message. Otherwise the SP code is entered into the ME.

- the ME reads the Co-operative Network List (CNL) from the SIM and extracts the SP code associated with SP personalization;

- keypad entry;

- a manufacturer defined process.

b) The network code is entered into the ME. This may be accomplished by one or the following means:

- for the case of a single network code, the ME reads the IMSI from the SIM and extracts the network code;

- the ME reads the Co-operative Network List (CNL) from the SIM and stores the list of network code(s) associated with SP personalization;

- keypad entry;

- manufacturer defined process.

c) The ME carries out the pre-personalization checks contained in clause 13 on the new codes entered into the ME. If they all pass, the network and SP codes are stored in the ME. If any fail, the personalization process shall be terminated.

d) The SPCK is stored in the ME. This may be entered via the keypad by the user or by a manufacturer defined process.

e) The SP personalization indicator is set to "on".

### 6.2.2 De-personalization cycle

To de-personalize the ME, the correct SPCK shall be entered. It is optional whether or not a SIM is inserted in the ME.

SP de-personalization shall be possible by keypad entry. If there is no keypad, then an alternative ME-based solution shall be provided. Other de-personalization methods may also be provided such as a network initiated process whereby the control key is sent to the MS over-the-air (see clause 9).

The SP de-personalization process is as follows:

a) the SPCK is entered into the ME;

b) if the entered SPCK is the same as the one stored in the ME, the SP personalization indicator is set to "off".

If the entered and stored SPCK values differ, the de-personalization process shall be stopped and the ME remains SP personalized. The stored network and SP codes and SPCK shall be left unchanged.

## 7 Corporate personalization

Corporate personalization is a refinement of SP personalization which allows companies to prevent the use of MEs they provide for their employees or customers with other SIMs without that corporate personalization.

This feature only works with SIMs which support both the GID1 and GID2 files. For the purpose of corporate personalization the GID1 file is programmed at pre-personalization with an SP code that identifies the service provider and the GID2 file is programmed by the service provider or corporate customer with a code that identifies the corporate customer.

The ME is corporate personalized by storing the network operator, SP and corporate codes and setting a corporate personalization indicator in the ME to "on". Whenever a SIM is inserted, or the ME is powered up with a SIM already in place, the network operator, SP and corporate codes are read and checked against those stored in the ME. If the sets of values differ the ME shall go into emergency calls only mode, as defined in annex A.2.

The corporate personalization feature is controlled by a Corporate Control Key (CCK), which has to be entered into the ME in order to de-personalize it.

In order to support the corporate personalization feature the ME shall have storage for the corporate personalization indicator, the network operator, SP and corporate codes and the corporate control key, CCK.

### 7.1 Operation of corporate personalized MEs

The personalization check described below is performed whenever a SIM is inserted or the ME is powered up with a SIM already in place.

The personalization check is as follows. When more than more personalization is active in the ME, normal mode of operation includes performing any outstanding personalization checks:

a) **check the ME is corporate personalized:** The ME checks the corporate personalization indicator, if it is set to "off" the personalization check shall be stopped and the ME goes into its normal mode of operation;

b) **check the SIM supports GID1 and GID2:** The ME checks that the SIM supports the GID1 and GID2 files;

c) **check the corporate code:** The ME reads the corporate code from the GID2 file as defined in annex A.1. and checks it against the stored value;

d) **check the SP code:** The ME reads the SP code from the GID1 file as defined in annex A.1. and checks it against the stored value;

e) **check the network code(s):** The ME reads the IMSI from the SIM, extracts the network code from it and checks it against the (list of) stored value(s).

If b) fails, or no match is found in c), d) or e), the ME may display an appropriate message (e.g. "Insert correct SIM") and shall go into emergency calls only mode, as defined in annex A.2. Otherwise, the ME goes into the normal mode of operation.

## 7.2 Corporate personalization cycle

### 7.2.1 Personalization cycle

The process of personalization can only be carried out on a currently unpersonalized ME, i.e., if the corporate personalization indicator is set to "off". Access to the personalization process shall be restricted in order to prevent unauthorized, accidental or unwanted personalization. Other restrictions are described in clause 13. In particular, corporate personalization cannot be carried out if the ME is personalized to more than one network. The personalization process results in the CCK being set, the corporate personalization indicator being set to "on" and the storage in the ME of the network, SP and corporate codes to which the ME is being personalized.

The corporate personalization process is as follows:

a) The SP and corporate codes are entered into the ME. This may be accomplished by one of the following means:

- the ME checks that the SIM supports the GID1 and GID2 files, if not the corporate personalization process shall be aborted with an appropriate error message;

  the ME reads the corporate and SP codes from the SIM from the GID2 and GID1 files respectively. If either of them is set to the default value, then the corporate personalization process shall be aborted with an appropriate error message. Otherwise the corporate and SP codes are entered into the ME;

- keypad entry;

- a manufacturer defined process.

b) The network code is entered into the ME. This may be accomplished by one of the following means:

- for the case of a single network code, the ME reads the IMSI from the SIM and extracts the network code;

- keypad entry;

- a manufacturer defined process.

c) The ME carries out the pre-personalization checks contained in clause 13 on the new codes entered into the ME. If they all pass, the network, SP and corporate codes are stored in the ME. If any fail, the personalization process shall be terminated.

d) The CCK is stored in the ME. This may be entered via the keypad by the user or by a manufacturer defined process;

e) The corporate personalization indicator is set to "on".

### 7.2.2 De-personalization cycle

To de-personalize the ME the correct CCK shall be entered. It is optional whether or not a SIM is inserted in the ME.

The corporate de-personalization shall be possible by keypad entry. If there is no keypad, then an alternative ME-based solution shall be provided. Other de-personalization methods may also be provided such as a network initiated process whereby the control key is sent to the MS over-the-air (see clause 9).

The corporate de-personalization process is as follows:

a) the CCK is entered into the ME;

b) if the entered CCK is the same as the one stored in the ME, the corporate personalization indicator is set to "off".

If the entered and stored CCK values differ the de-personalization process shall be stopped and the ME remains corporate personalized. The stored network operator, SP and corporate codes and CCK are left unchanged

## 8 SIM personalization

SIM personalization is an anti-theft feature. When a ME is SIM personalized to a particular SIM it will refuse to operate with any other SIM. Hence, if the ME is stolen the thief will not be able to use it with another SIM (see note). While this does not stop the ME being stolen it should make it less attractive to the thief.

NOTE: If the ME and the SIM to which it has been personalized are stolen together the ME would become unusable once the SIM is reported stolen and is disconnected.

The ME is SIM personalized by storing the IMSI of the relevant SIM in the ME and setting a SIM personalization indicator in the ME to "on". Whenever a SIM is inserted, or the ME is powered up with a SIM already in place, the IMSI is read from the SIM and checked against that stored in the ME. If the two values differ the ME shall go into emergency calls only mode as described in annex A.2.

The SIM personalization feature is controlled by a Personalization Control Key (PCK). This key is selected by the user at SIM personalization and shall be entered into the ME to SIM de-personalize the ME.

In order to support the SIM personalization feature the ME should have storage for the SIM personalization indicator, an IMSI and the PCK.

Multiple instances of SIM personalization can be supported, i.e. whenever a SIM is inserted, or the ME is powered up with a SIM already in place, the IMSI is read from the SIM and checked against a list of IMSIs stored in the ME.

### 8.1 Operation of SIM personalized ME

The SIM personalization check described below is performed whenever a SIM is inserted or the ME is powered up with a SIM already in place.

The personalization check is as follows. When more than one personalization is active in the ME, normal mode of operation includes performing any outstanding personalization checks:

a) **check the ME is SIM personalized:** The ME checks its SIM personalization indicator, if it is set to "off" the personalization check shall be stopped and the ME goes into the normal mode of operation, omitting the remaining steps of the check;

b) **read IMSI:** The ME reads the IMSI from the SIM;

c) **SIM personalization check:** The ME checks the read IMSI against that stored in the ME. If they differ the ME shall display an appropriate message (e.g. "Insert correct SIM") and shall go into emergency calls only mode as described in annex A.2. If the IMSIs agree the ME goes into the normal mode of operation.

### 8.2 SIM personalization cycle

#### 8.2.1 Personalization cycle

The process of personalization can only be carried out on a currently unpersonalized ME, i.e., if the SIM personalization indicator is set to "off". It results in the PCK being set, the SIM personalization indicator being set to "on" and the storage in the ME of the IMSI(s) of the SIM(s) to which the ME is being SIM personalized. Before personalization can proceed, all active personalization categories shall be checked; if any fail, the process shall be terminated.

The SIM personalization process is as follows:

a) to personalize the ME to a SIM, the IMSI is read from the SIM and entered into the ME;

b) the ME carries out the pre-personalization checks contained in clause 13. If they all pass, the IMSI value is stored in the ME. If any fail, the personalization process shall be terminated;

c) to personalize the ME to more than one SIM, the procedures given in a) and b) shall be repeated;

d) the PCK is then stored in the ME. A single value of PCK shall be used for both single and multiple SIM personalization;

e) the SIM personalization indicator is set to "on".

#### 8.2.2 De-personalization cycle

To de-personalize the ME, the correct PCK shall be entered. This SIM shall be inserted in the ME, and the personalization check shall have been passed.

SIM de-personalization shall be provided by keypad entry. Other de-personalization methods may also be provided.

The SIM de-personalization process is as follows:

a) the user enters the PCK in the ME;

b) if the entered PCK is the same as the one stored in the ME, the SIM personalization indicator is set to "off".

If the entered and stored PCK values differ, the de-personalization process shall be stopped and the ME remain personalized. The stored IMSI and PCK are left unchanged.

## 9 Over the air de-personalization cycle

As an optional ME feature, the ME may be de-personalized over-the-air (OTA) by the network. The network, network subset, SP and corporate categories may be de-personalized in this way. More than one category may be de-personalized at the same time. The process results in the relevant personalization indicator(s) being set to "off". The ME must be registered on a network.

Two OTA methods are defined both of which use MT SMS-PP messages. With the first method, the IMEI of the ME to be de-personalized and the Control Key(s) of the personalization categories to be de-personalized are sent directly to the ME. The ME performs checks on both the IMEI and the key values and the outcome of the attempted de-personalization(s) is acknowledged to the network.

With the second method, the keys of the personalization categories to be de-personalized are sent to the ME via the SIM. The IMEI is not included and the de-personalization process only checks the keys. The outcome of the attempted de-personalization(s) is acknowledged to the network.

The network de-personalizes the ME by one of the following methods:

(i) SMS-PP, ME-specific:

a) A point-to-point SMS message is sent by the network to the MS, the message being marked as being destined for the ME only and for the purposes of ME de-personalization (see GSM 03.40 [7]). The User Data of the SMS contains the de-personalization key(s) and the IMEI (see annex A.4). If the ME supports the feature, then it shall not display the data on the ME.

b) The ME compares the values of the IMEI and the key(s) sent by the network with the corresponding values stored in the ME. If they are the same, the relevant personalization indicator(s) is (are) set to "off".

If the IMEI values differ, the personalization status of all categories shall be left unchanged.

If any key values differ, the corresponding personalization status shall be left unchanged.

c) The MS sends a SMS acknowledgement to the network indicating the result of the attempted de-personalization process (see annex A.4).

(ii) SMS-PP SIM Data Download:

a) A SMS message is sent by the network to the SIM updating the $EF_{DCK}$ using the SMS-PP SIM Data Download of the SIM Tool Kit (see GSM 11.14 [10]).

b) The SIM causes the ME to send an SMS acknowledgement to the network, as a result of the terminal response to the ENVELOPE command.

c) The SIM shall issue a REFRESH command to instruct the ME to perform an initialization procedure. During the initialization procedure the ME reads the de-personalization key field(s) from $EF_{DCK}$ stored in the SIM after performing all personalization checks.

d) For each control key in $EF_{DCK}$ which is empty (set to default), the corresponding personalization status shall be left unchanged.

e) For each control key in the $EF_{DCK}$ which is not the same as the corresponding stored key, the personalization status shall be left unchanged.

f) For each control key in $EF_{DCK}$ which is the same as the one stored in the ME, the corresponding personalization indicator is set to "off".

g) All the keys in the $EF_{DCK}$ are reset to the default value by the ME.

## 10 Disable Personalization

There shall be a means to disable the personalization at each level individually such that the ME shall operate with any (i.e. all) SIM at that level.

The process of disable-personalization can only be carried out on a currently unpersonalized ME, i.e., if the personalization indicator for that level is set to "off". It results in the personalization indicator remaining set to "off". When a particular level is disabled in this manner there shall be a means to make it impossible to change this status i.e. the disable becomes irreversible thus eliminating the need for key-administration.

## 11 Manufacturer personalization and de-personalization

Manufacturers may enter into private arrangements to personalize MEs before delivery or at other times. They may also have the capability to de-personalize/reset MEs for example, when a ME needs repairing, when the relevant control key has been forgotten or lost or if the ME has been blocked as a result of excessive failed attempts at de-personalization.

In all cases, secure arrangements shall be followed with the transfer and handling of the critical data such as the IMSI and the associated control keys.

In common with the normal de-personalization processes, the manufacturer controlled processes should be secure and be key or password controlled.

## 12 Automatic personalization

ME manufacturers may offer alternative means of personalizing the ME such as adding functionality to the ME so that it automatically personalizes itself to the first SIM inserted in it, using one or more of the five personalization levels described in clauses 5 to 8. In the case of SP and corporate personalization, this is subject to the SIM supporting GID1 and GID2 (as required) and the contents of those files being non-default.

## 13 Personalization Cycle Restrictions

The following checks shall be carried out by the ME during the personalization cycle.

Before any new codes are stored in the ME, the ME shall check them against any corresponding existing valid codes stored in the ME. An existing code is deemed to be valid only when another personalization category is active (i.e. the personalization indicator is on) and when that category utilizes the codes(s) as shown in table 1. For each personalization process the ME shall compare the new code values with any existing valid values for all the following case:

- if there is no existing, valid, code the personalization process shall continue;

- if the new code value is the same as an existing, valid, code the personalization process shall continue otherwise, the personalization process shall be terminated;

- If the new list of network codes (including the case of a single code) has the same length and the same values as an existing valid list, the personalization process shall continue, otherwise the personalization process shall be terminated.

## 14 Security

This clause lists a number of security requirements which should be satisfied if the personalization features are to be effective. The requirements are not arranged in any particular order.

a) The control keys shall be decimal strings with an appropriate number of digits for the level of personalization. PCK should be at least 6 digits, and the remaining control keys at least 8 digits in length. The maximum length for any control key is 16 digits.

b) Where more than one of the personalization features are in use, distinct control keys should be used for the different features.

c) The NCK, NSCK, SPCK and CCK should be randomly selected or pseudo-randomly generated and differ from ME to ME.

d) The PCK should be randomly selected for each ME. In particular, subscribers should be strongly encouraged not to use obvious values such as part of the dialling number.

e) It should be impractical to read or recover any of the control keys from the ME.

f) It should be impractical to alter or delete the values of the personalization indicators, the control keys, the stored IMSI or the stored network operator, SP and corporate codes, other than by the defined personalization and de-personalization processes, without completely disabling the ME from working with any SIM. (Possible methods that might be used by criminals to alter or delete the values include freezing, baking, exposure to magnetic fields or UV light.)

g) For each de-personalization procedure, there shall be a mechanism to prevent unauthorized attempts to de-personalize the ME. These may include blocking the ME if the number of failed attempts to de-personalize the ME exceeds a certain limit, or alternatively introducing an increasing delay after each successive failed de-personalization attempt. Other mechanisms may be also be used.

h) The SIM personalization feature will only succeed in discouraging thieves if they know or suspect that the ME is SIM personalized. Therefore, unless and until SIM personalized MEs become the norm, it is desirable that the ME should advertise the fact that it is SIM personalized.

i) Manufacturers should not de-personalize a ME for a user unless they have obtained the appropriate level of approval, e.g., from the network operator for network personalization, from the service provider for service provider personalization, etc.

j) ME manufacturers should ensure that the personalization processes (except for SIM personalization) are protected against unauthorized, accidental or malicious operation.

# Annex A (normative): Technical information

## A.1 GID1 and GID2 files

The GID1 and GID2 elementary files on the SIM are specified in GSM 11.11 (ETS 300 977) [9].

For the purposes of this GTS, a SIM is said to support one of these two files if it is marked as both allocated and activated in the SIM service table.

The SP and corporate codes are stored in byte 1 of the appropriate files.

If byte 1 contains a hexadecimal value between "00" and "FE" inclusive, then this represents the SP/corporate code in the GID1/GID2 files respectively. For the purpose of these personalization features, the ME shall ignore the contents of any other bytes of the file.

The value "FF" is the default value to be used in byte 1 when no meaningful SP/corporate code is represented in the GID1/GID2 files respectively. This value shall not be allocated as an SP/corporate code.

Note that network operators would normally allocate SP codes for its service providers and SPs would normally allocate corporate codes for its corporate customers.

## A.2 Emergency calls only mode

The expression "emergency calls only mode" is used in this GTS to describe the state the MS (combined ME and SIM) enters when a personalization check fails. In this mode, the state of the MS is equivalent to the "limited service state" (see GSM 03.22) [5]. Although the personalization has failed, the ME will be able to access the TMSI and IMSI from the SIM, and therefore any emergency call request shall use these as the MS identity, as defined in GSM 04.08 [8].

Set up of emergency calls remains as usual dependent on the status of Access Class 10 being broadcast in the cell (see GSM 02.11) [3].

## A.3 Co-operative Network List

The Co-operative Network List is specified in GSM 11.11 (ETS 300 977) [9].

For the purposes of this GTS, a SIM is said to support this feature if it is marked as both allocated and activated in the SIM service table.

The value "FF" is the default value to be used when no meaningful code is represented. This value shall not be allocated as a code value.

## A.4 Over-the-air de-personalization

a) The ME-specific de-personalization SMS messages sent by the network to de-personalize the ME shall be coded according to GSM 03.40 [7] with the TP-UD field coded as follows:

| **Character** | **Description** |
|---|---|
| 1 - 40 | Operator specific text padded with spaces to character 40. |
| 41 - 48 | Network control key |
| 49 - 56 | Network subset control key |
| 57 - 64 | SP control key |
| 65 - 72 | Corporate control key |
| 73 - 88 | IMEI |

For the IMEI and each control key, the most significant digit is coded first in the string, e.g. character 41 is the most significant digit of NCK.

All characters are coded according to the default alphabet described in GSM 03.38 [6].

The string "FFFFFFFF" shall be used in place of a key to indicate that de-personalization of that category is not required.

b) The acknowledgement to the ME De-personalization Short Message shall be a SMS-DELIVER-REPORT for RP-ACK as described in GSM 03.40 with the TP-User-Data coded according to the default alphabet described in GSM 03.38 [6] as below:

| **Character** | **Description** |
|---|---|
| 1-16 | IMEI of ME |
| 17 | Network personalization status |
| 18 | Network subset personalization status |
| 19 | SP personalization status |
| 20 | Corporate personalization status |

Status codes shall indicate the resulting status of each personalization category as below.

| **Status code** | **Description** |
|---|---|
| 0 | Currently not personalized |
| 1 | Permanently not personalized |
| 2 | Personalized |
| 3 | IMEI mismatch |
| Other | RFU |

If the IMEI of the ME does not match the IMEI included in the De-personalization Short Message, then the status of all the personalization categories shall be coded "IMEI mismatch".c) The format for the control keys stored on the SIM is specified in GSM 11.11 [9].

For the purposes of this GTS, a SIM is said to support this feature if it is marked as both allocated and activated in the SIM service table.

The value "FF" is the default value to be used when no meaningful value for a key is represented. This value shall not be allocated as a key value.

## History

| Document history | |
|---|---|
| December 1996 | Publication of GSM 02.22 Version 5.2.0 |
| | |
| | |
| | |
| | |

ISBN 2-7437-1185-X
Dépôt légal : Décembre 1996