3GPP TSG SA WG3 Security — S3#10 **S3-000032**

19-21 January, 2000

Antwerpen, Belgium

Source:	**Secretary**
Title:	**22.022 V 3.0.1: Personalisation of GSM ME Mobile functionality specification - Stage 1**
Document for:	**Information**
Agenda Item:	

22.022 V 3.0.1 is attached.

3G TS 22.022 V3.0.1 (1999-08)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Personalisation of GSM Mobile Equipment (ME); Mobile functionality specification (3G TS 22.022 version 3.0.1)

Reference
DTS/TSGSA-0122022U

Keywords
3GPP, SA

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3GPP.

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of this TS, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version 3.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 Indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the specification;

1 Scope

The present document provides functional specifications of five features to personalise Mobile Equipment (ME). These features are called:

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

The present document specifies requirements for MEs which provide these personalisation features.

Note: The present document covers description for GSM only. The document needs to be updated to make it applicable to 3GPP.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.
- For this Release 1999 document, references to GSM documents are for Release 1999 versions (version 8.x.y).

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

[2] TS 22.011: "Service accessibility".

[3] TS 23.003: " Numbering, addressing and identification".

[4] TS 23.022: "Functions related to Mobile Station (MS) in idle mode and group receive mode".

[5] TS 23.038: "Alphabets and language-specific information".

[6] TS 23.040: "Technical realization of the Short Message Service (SMS); Point-to-Point (PP)".

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

[8] 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".

[9] TR 21.905: "Vocabulary for 3GPP Specifications".

3 Definitions and abbreviations

3.1 Abbreviations

For the purposes of the present document, 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	Personalisation 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 [1].

3.2 Definitions

For the purposes of the present document, the following definitions apply:

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

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

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

network subset personalisation: A refinement of network personalisation, 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 if it had no personalisation checks to process.

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

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

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

network code: MCC and MNC.

network subset code: digits 6 and 7 of the IMSI.

SP code: code which when combined with the network code refers to a unique SP. The code is provided in the GID1 file on the SIM (see Annex A.1.) and is correspondingly stored on the ME.

Corporate code: code which when combined with the network and SP codes refers to a unique Corporate. The code is provided in the GID2 file on the SIM (see Annex A.1.) and is correspondingly stored on the ME.

SIM code : code which when combined with the network and NS codes refers to a unique SIM. The code is provided by the digits 8 to 15 of the IMSI

network code group: same as network code

network subset code group: combination of a network subset code and the associated network code.

SP code group: combination of the SP code and the associated network code.

Corporate code group: combination of the Corporate code and the associated SP and network codes.

SIM code group : combination of the SIM code and the associated network subset and network codes (it is equivalent to the IMSI).

Personalisation entity: Network, network subset, SP, Corporate or SIM to which the ME is personalised

4 General description

The personalisation 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 personalisation categories of varying granularity; network, network subset, SP, corporate and SIM. The personalisation categories are independent is so far as each category can be activated or de-activated regardless of the status of the others. Each category has a separate personalisation indicator to show whether it is active or not. The ME can be personalised to one network, one network subset, one SP, one Corporate, one SIM or any combination thereof. The ME may optionally be personalised to multiple networks, network subsets, SPs, Corporates, SIMs or any combinations thereof.

The codes used for each personalisation category are shown in Table 1. Some categories require several codes (e.g. SP and network for SP personalisation) and each combination of codes relating to a particular entity (network, SP etc.) is referred to as a code group. To personalise to multiple entities, multiple code groups are stored in the ME. For each activated personalisation category, the ME retrieves the relevant codes from the SIM and checks the retrieved code group against the (list of) code group(s) stored in the ME. If a match is found with any of the code groups stored in the ME, the check is passed for that category. If checks for all active categories are passed, then the MS goes into normal operation.

Table 1: Codes used by each personalisation category

Code	Network (MCC, MNC)	Network Subset (IMSI digits 6 and 7)	SP	Corporate	SIM (IMSI digits 8 to 15)
Personalisation category					
Network	✓				
Network subset	✓	✓			
SP	✓		✓		
Corporate	✓		✓	✓	
SIM	✓	✓			✓

Precautions must be taken to ensure that when more than one personalisation category is to be activated or when the ME is to be personalised to more than one entity of a personalisation category, 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 personalisation cycle, as described in clause 13.

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

5 Network personalisation

5.1 Network personalisation

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

The ME is network personalised by storing the code (MCC+MNC) (see TS 223.003 [3]) of the relevant network(s) in the ME and setting a network personalisation 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 values differ, the MS shall go into emergency calls only mode as defined in annex A.2.

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

In order to support the network personalisation feature the ME shall have storage for the network personalisation indicator, the network code(s) and the NCK.

5.1.1 Operation of network personalised ME

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

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

a) **check the ME is network personalised:** The ME checks its network personalisation indicator, if it is set to "off" the personalisation 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 personalisation cycle

5.1.2.1 Personalisation cycle

The process of personalisation can only be carried out on a currently unpersonalised ME, i.e., if the network personalisation indicator is set to "off". Access to the personalisation process shall be restricted in order to prevent unauthorised, accidental or unwanted personalisation. Other restrictions are described in clause 13. The personalisation process results in the NCK being set, the network personalisation indicator being set to "on" and the storage in the ME of the network code(s) to which the ME is being personalised.

The network personalisation 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 personalisation;
- keypad entry;
- a manufacturer defined process.

b) The ME carries out the pre-personalisation checks contained in clause 13. If they all pass, the network code(s) are stored in the ME. If any fail, the personalisation 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 personalisation indicator is set to "on".

5.1.2.2 De-personalisation cycle

To de-personalise the ME, the correct NCK shall be entered. It is optional whether or not a SIM is inserted in the ME. If a SIM is inserted, then de-personalisation shall be offered whether or not the network personalisation check passes or fails.

Network subset de-personalisation shall be possible by keypad entry. If there is no keypad, then an alternative ME-based solution shall be provided. Other de-personalisation 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-personalisation 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 personalisation indicator is set to "off".

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

5.2 Network subset personalisation

Network subset personalisation is a refinement of network personalisation, 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 personalised 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 personalisation 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 subset code group is read from the SIM and checked against the stored values in the ME. If no match is found, the ME shall go into emergency calls only mode, as defined in annex A.2.

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

In order to support the network subset personalisation feature, the ME shall have storage for the network subset personalisation indicator, the network subset code group(s) and the NSCK.

5.2.1 Operation of Network subset personalised ME

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

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

a) check the ME is network subset personalised: The ME checks its network subset personalisation indicator, if it is set to "off" the personalisation 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 group: The ME reads the network subset code group from the SIM and checks it against the (list of) stored value(s) on the ME;

If no match is found in b) 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 personalisation cycle

5.2.2.1 Personalisation Cycle

The process of personalisation can only be carried out on a currently unpersonalised ME, i.e., if the network subset personalisation indicator is set to "off". Access to the personalisation process shall be restricted in order to prevent unauthorised, accidental or unwanted personalisation. Other restrictions are described in clause 13. The personalisation process results in the NSCK being set, the network subset personalisation indicator being set to "on" and the storage in the ME of the (list of) network subset code group(s) which identify the specific network subset(s) to which the ME is being personalised.

The network subset personalisation process is as follows:

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

   - for the case of a single network code group, 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 subset code group(s);
   - keypad entry;
   - a manufacturer defined process.

b) The ME carries out the pre-personalisation checks contained in clause 13, on the new codes entered into the ME. If they all pass, the network subset code group(s) is (are) stored in the ME. If any fail, the personalisation 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 personalisation indicator is set to "on".

5.2.2.2 De-personalisation cycle

To de-personalise the ME the correct NSCK shall be entered. It is optional whether or not a SIM is inserted. If a SIM is inserted, then de-personalisation shall be offered whether or not the network subset personalisation check passes or fails.

Network subset de-personalisation shall be possible by keypad entry. If there is no keypad, then an alternative ME-based solution shall be provided. Other de-personalisation 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-personalisation 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 personalisation indicator is set to "off".

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

6 SP personalisation

Service provider or SP personalisation 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 personalisation the GID1 file is programmed with an SP code that identifies the service provider.

The ME is SP personalised by storing the SP code group(s) and setting an SP personalisation indicator in the ME to "on". Whenever a SIM is inserted, or the ME is powered up with a SIM already in place, the SP code group is read from the SIM and checked against those stored in the ME. If no match is found the ME shall go into emergency calls only mode as defined in annex A.2.

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

In order to support the SP personalisation feature the ME shall have storage for the SP personalisation indicator, the (list of) SP code group(s) and the SPCK.

6.1 Operation of SP personalised MEs

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

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

a) **check the ME is SP personalised:** The ME checks the SP personalisation indicator, if it is set to "off" the personalisation 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 group:** The ME reads the SP code group from the SIM. and checks it against the (list of) stored value(s) on the ME;

If b) fails or no match is found in 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.

6.2 SP personalisation cycle

6.2.1 Personalisation cycle

The process of personalisation can only be carried out on a currently unpersonalised ME, i.e., if the SP personalisation indicator is set to "off". Access to the personalisation process shall be restricted in order to prevent unauthorised, accidental or unwanted personalisation. Other restrictions are described in clause 13. The personalisation process results in the SPCK being set, the SP personalisation indicator being set to "on" and the storage in the ME of the (list of) SP code group(s) to which the ME is being personalised.

The SP personalisation process is as follows:

a) The SP code group(s) is (are) 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 personalisation process is aborted with an appropriate error message. The ME reads the SP code group from the SIM. If the SP code is set to the default value (see annex A.1) then the personalisation process shall be aborted with an appropriate error message. Otherwise the SP code group is entered into the ME.

- the ME reads the Co-operative Network List (CNL) from the SIM and extracts the (list of) SP code group(s);

- keypad entry;

- a manufacturer defined process.

b) The ME carries out the pre-personalisation checks contained in clause 13 on the new codes entered into the ME. If they all pass, the SP code group(s) is (are) stored in the ME. If any fail, the personalisation process shall be terminated.

c) 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 personalisation indicator is set to "on".

6.2.2 De-personalisation cycle

To de-personalise the ME, the correct SPCK shall be entered. It is optional whether or not a SIM is inserted in the ME. If a SIM is inserted, then de-personalisation shall be offered whether or not the SP personalisation check passes or fails.

SP de-personalisation shall be possible by keypad entry. If there is no keypad, then an alternative ME-based solution shall be provided. Other de-personalisation 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-personalisation 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 personalisation indicator is set to "off".

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

7 Corporate personalisation

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

This feature only works with SIMs which support both the GID1 and GID2 files. For the purpose of corporate personalisation the GID1 file is programmed at pre-personalisation 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 personalised by storing the corporate code group(s) and setting a corporate personalisation indicator in the ME to "on". Whenever a SIM is inserted, or the ME is powered up with a SIM already in place, the corporate code group is read from the SIM and checked against those stored in the ME. If there is no match the ME shall go into emergency calls only mode, as defined in annex A.2.

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

In order to support the corporate personalisation feature the ME shall have storage for the corporate personalisation indicator, a (list of) corporate code group(s) and the CCK.

7.1 Operation of corporate personalised MEs

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

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

a) **check the ME is corporate personalised:** The ME checks the corporate personalisation indicator, if it is set to "off" the personalisation 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 group:** The ME reads the corporate code group from the SIM and checks it against the (list of) stored value(s) on the ME;

If b) fails, or no match is found in 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.

7.2 Corporate personalisation cycle

7.2.1 Personalisation cycle

The process of personalisation can only be carried out on a currently unpersonalised ME, i.e., if the corporate personalisation indicator is set to "off". Access to the personalisation process shall be restricted in order to prevent unauthorised, accidental or unwanted personalisation. Other restrictions are described in clause 13. The personalisation process results in the CCK being set, the corporate personalisation indicator being set to "on" and the storage in the ME of a (list of) corporate group(s) codes to which the ME is being personalised.

The corporate personalisation process is as follows:

a) The corporate code group(s) is (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 personalisation process shall be aborted with an appropriate error message;

  the ME reads the corporate code group(s) from the SIM. If either the SP code or the corporate code is set to the default value (see Annex A.1), then the corporate personalisation process shall be aborted with an appropriate error message. Otherwise the corporate code group is are entered into the ME;

- the ME reads the Co-operative Network List (CNL) from the SIM and extracts the (list of) Corporate code group(s);

- keypad entry;

- a manufacturer defined process.

b) The ME carries out the pre-personalisation checks contained in clause 13 on the new codes entered into the ME. If they all pass, the corporate code group(s) are stored in the ME. If any fail, the personalisation process shall be terminated.

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

d) The corporate personalisation indicator is set to "on".

7.2.2 De-personalisation cycle

To de-personalise the ME the correct CCK shall be entered. It is optional whether or not a SIM is inserted in the ME. If a SIM is inserted, then de-personalisation shall be offered whether or not the corporate personalisation check passes or fails.

The corporate de-personalisation shall be possible by keypad entry. If there is no keypad, then an alternative ME-based solution shall be provided. Other de-personalisation 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-personalisation 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 personalisation indicator is set to "off".

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

8 SIM personalisation

SIM personalisation is an anti-theft feature. When a ME is SIM personalised 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 personalised are stolen together the ME would become unusable once the SIM is reported stolen and is disconnected.

The ME is SIM personalised by storing the SIM code group (which is equivalent to the IMSI) of the relevant SIM in the ME and setting a SIM personalisation indicator in the ME to "on". Whenever a SIM is inserted, or the ME is powered up with a SIM already in place, the SIM code group (IMSI) is read from the SIM and checked against the SIM code group(s) stored in the ME. If there is no match the ME shall go into emergency calls only mode as described in annex A.2.

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

In order to support the SIM personalisation feature the ME should have storage for the SIM personalisation indicator, a (list of) SIM code group(s) and the PCK.

Multiple instances of SIM personalisation 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 SIM code groups stored in the ME.

8.1 Operation of SIM personalised ME

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

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

a) **check the ME is SIM personalised:** The ME checks its SIM personalisation indicator, if it is set to "off" the personalisation 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 personalisation check:** The ME checks the read IMSI against the (list of) SIM code group(s) stored in the ME. If no match is found, 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. Otherwise, the ME goes into the normal mode of operation.

8.2 SIM personalisation cycle

8.2.1 Personalisation cycle

The process of personalisation can only be carried out on a currently unpersonalised ME, i.e., if the SIM personalisation indicator is set to "off". Access to the personalisation process shall be restricted in order to prevent unauthorised , accidental or unwanted personalisation. Other restrictions are described in clause 13. The personalisation process results in the PCK being set, the SIM personalisation indicator being set to "on" and the storage in the ME of a (list of) SIM code group(s) to which the ME is being personalised.

The SIM personalisation process is as follows:

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

- the ME reads the SIM code group (IMSI) from the SIM and stores it;

- a manufacturer defined process.

b) the ME carries out the pre-personalisation checks contained in clause 13. If they all pass, the SIM code group(s) is(are) stored in the ME. If any fail, the personalisation process shall be terminated;

c) to personalise the ME to more than one SIM and if the reading of the IMSI from the SIM is used to enter the SIM code group in the ME, 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 personalisation;

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

8.2.2 De-personalisation cycle

To de-personalise the ME, the correct PCK shall be entered. It is optional whether or not a SIM is inserted in the ME. If a SIM is inserted, then de-personalisation shall be offered whether or not the SIM personalisation check passes or fails.

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

The SIM de-personalisation 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 personalisation indicator is set to "off".

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

9 Over the air de-personalisation cycle

As an optional ME feature, the ME may be de-personalised over-the-air (OTA) by the network. The network, network subset, SP and corporate categories may be de-personalised in this way. More than one category may be de-personalised at the same time. The process results in the relevant personalisation 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-personalised and the Control Key(s) of the personalisation categories to be de-personalised 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-personalisation(s) is acknowledged to the network.

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

The network de-personalises 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-personalisation (see TS 23.040 [6]). The User Data of the SMS contains the de-personalisation 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 personalisation indicator(s) is (are) set to "off".

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

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

c) The MS sends a SMS acknowledgement to the network indicating the result of the attempted de-personalisation 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 [8]).

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 initialisation procedure. During the initialisation procedure the ME reads the de-personalisation key field(s) from EF_{DCK} stored in the SIM after performing all personalisation checks.

d) For each control key in EF_{DCK} which is empty (set to default), the corresponding personalisation 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 personalisation 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 personalisation indicator is set to "off".

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

10 Disable Personalisation

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

The process of disable-personalisation can only be carried out on a currently unpersonalised ME, i.e., if the personalisation indicator for that level is set to "off". It results in the personalisation 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 personalisation and de-personalisation

Manufacturers may enter into private arrangements to personalise MEs before delivery or at other times. They may also have the capability to de-personalise/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-personalisation.

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-personalisation processes, the manufacturer controlled processes should be secure and be key or password controlled.

12 Automatic personalisation

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

13 Personalisation Cycle Restrictions

Security mechanisms shall be implemented to ensure that additions or changes to any personalisation category shall only be made by persons authorised to do so for that category (see Section 14).

During the Personalisation cycle of a category, before any changes are made to the existing personalisation data, it shall be checked that :

- the category to be personalised is not currently activated;
- the new codes to be stored are a subset of the existing codes.

(e.g. for a ME which is already network-personalised with the network code N1 and that is to be personalised for the SP category, N1-SP1 can be added but N2-SP2 cannot be added).

NOTE 1: If no personalisation category are active, then no checks are necessary.

NOTE 2: If the entities of an active personalisation category are to be modified, then this shall only be possible if the personalisation category is first de-personalised by means of the appropriate Control Key.

NOTE 3: After each personalisation cycle, the number of SIMs with which the ME can operate decreases. If further personalisation cycles of specific personalisation categories are to be prevented, the disable-personalisation feature can be used (see clause 10).

14 Security

This clause lists a number of security requirements which should be satisfied if the personalisation 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 personalisation. 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 personalisation 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 personalisation indicators, the control keys, the stored IMSI or the stored network operator, SP and corporate codes, other than by the defined personalisation and de-personalisation 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-personalisation procedure, there shall be a mechanism to prevent unauthorised attempts to de-personalise the ME. These may include blocking the ME if the number of failed attempts to de-personalise the ME exceeds a certain limit, or alternatively introducing an increasing delay after each successive failed de-personalisation attempt. Other mechanisms may be also be used.

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

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

j) ME manufacturers should ensure that the personalisation processes (except for SIM personalisation) are protected against unauthorised, 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) [7].

For the purposes of this TS, 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 personalisation 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 TS to describe the state the MS (combined ME and SIM) enters when a personalisation check fails. In this mode, the state of the MS is equivalent to the "limited service state" (see TS 23.022) [4]. Although the personalisation 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.

Set up of emergency calls remains as usual dependent on the status of Access Class 10 being broadcast in the cell (see TS 22.011) [2].

A.3 Co-operative Network List

The Co-operative Network List is specified in GSM 11.11 (ETS 300 977) [7].

For the purposes of this TS, 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-personalisation

a) The ME-specific de-personalisation SMS messages sent by the network to de-personalise the ME shall be coded according to TS 23.040 [6] 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 TS 23.038 [5].

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

b) The acknowledgement to the ME De-personalisation Short Message shall be a SMS-DELIVER-REPORT for RP-ACK as described in TS 23.040 [6] with the TP-User-Data coded according to the default alphabet described in TS 23.038 [5] as below:

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

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

Status code	Description
0	Currently not personalised
1	Permanently not personalised
2	Personalised
3	IMEI mismatch
Other	RFU

If the IMEI of the ME does not match the IMEI included in the De-personalisation Short Message, then the status of all the personalisation categories shall be coded "IMEI mismatch".

c) The format for the control keys stored on the SIM is specified in GSM 11.11 [8].

For the purposes of this TS, 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.

Annex B:
Change history

Change history						
TSG SA#	**Spec**	**Version**	**CR**	**<Phase>**	**New Version**	**Subject/Comment**
Jun 1999	GSM 02.22	7.0.0				Transferred to 3GPP SA1
SA#04	22.022				3.0.0	
SA#05	22.022	3.0.0	001	R99	3.0.1	Editorial update of references for GSM/3GPP use

History

Document history		
V3.0.0	August 1999	Transferred to TSG SA at ETSI SMG#29. Under TSG TSG SA Change Control.
V3.0.1	October 1999	CR approved at SA #05.