

3GPP2 C.S0068-0

Version 1.0

Version Date: May 26, 2006



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

ME Personalization for cdma2000 Spread Spectrum Systems

COPYRIGHT NOTICE

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

Revision History

<u>Revision</u>	<u>Description</u>	<u>Date</u>
C.S0068-0 v1.0	Release 0	April 24 th , 2006

CONTENTS

1			
2			
3	1	INTRODUCTION	1
4	2	REFERENCES	3
5	3	DEFINITIONS AND ABBREVIATIONS.....	5
6	3.1	Definitions.....	5
7	3.2	Abbreviations	6
8	4	GENERAL FEATURE DESCRIPTION	9
9	5	NETWORK PERSONALIZATION	13
10	5.1	Network Type 1 personalization for CDMA 1x ME	13
11	5.1.1	Operation of a Network Type 1 personalized ME.....	13
12	5.1.2	Network Type 1 personalization cycle	14
13	5.2	Network Type 2 personalization for CDMA 1x ME	15
14	5.2.1	Operation of Network Type 2 personalized ME.....	15
15	5.2.2	Network Type 2 personalization cycle	16
16	5.3	Network personalization for HRPD terminal.....	17
17	5.3.1	Operation of HRPD Network personalized ME.....	17
18	5.3.2	HRPD Network personalization cycle	18
19	6	SERVICE PROVIDER PERSONALIZATION.....	21
20	6.1	Operation of SP personalized MEs	21
21	6.2	SP personalization cycle	22
22	6.2.1	Personalization cycle.....	22
23	6.2.2	De-personalization cycle.....	22
24	7	CORPORATE PERSONALIZATION.....	25
25	7.1	Operation of corporate personalized MEs.....	25
26	7.2	Corporate personalization cycle	26
27	7.2.1	Personalization cycle	26
28	7.2.2	De-personalization cycle.....	26
29	8	R-UIM PERSONALIZATION	29
30	8.1	Operation of R-UIM personalized ME	29
31	8.2	R-UIM personalization cycle.....	30
32	8.2.1	Personalization cycle	30

1	8.2.2	De-personalization cycle.....	31
2	9	OVER THE AIR DE-PERSONALIZATION CYCLE.....	33
3	10	DISABLE PERSONALIZATION.....	35
4	11	MANUFACTURER PERSONALIZATION AND DE-PERSONALIZATION	37
5	12	AUTOMATIC PERSONALIZATION.....	39
6	13	PERSONALIZATION CYCLE RESTRICTIONS	41
7	14	SECURITY	43
8		ANNEX A (NORMATIVE); TECHNICAL INFORMATION	45

1
2
3
4
5
6

TABLES

Table 4-1: Codes used by each personalization category for CDMA 1x..... 10
Table 4-2: Codes used by each personalization category for HRPD 10
Table 4-3: Codes used by each personalization category for HAT..... 11

1 No text.

1

2 1 INTRODUCTION

3 This document defines the ME Personalization feature. The ME Personalization feature will
4 allow operators to protect their investments in MEs by restricting the ME to operate with an R-
5 UIM containing specific personalization parameters. In effect, the ME Personalization feature
6 allows operators the ability to “lock” a handset (ME – mobile equipment) to a particular R-UIM
7 or set of R-UIMs. The locking feature works by storing personalization information in the ME
8 that limits the R-UIMs with which it will work and by checking this information against the R-
9 UIM upon power up or insertion of an R-UIM.

1 No text.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

2 REFERENCES

The following standards are referenced in this text. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based upon this document are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. ANSI and TIA maintain registers of currently valid national standards published by them.

1. 3GPP TS 22.022 v5.0.0, *“3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Personalisation of Mobile Equipment (ME); Mobile functionality specification”*, September 2002.
2. C.S0005-D, *Upper Layer (Layer 3) Signaling Standard for cdma2000 Spread Spectrum Systems*, March 2004.
3. 3GPP TS 31.102, *“3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM application”*, (Release 6).
4. C.S0023-C, *Removable User Identity Module for Spread Spectrum Systems*, April 2006.
5. Reserved.
6. C.S0015-B, *Short Message Service for Wideband Spread Spectrum Systems*, May 2004.
7. C.S0035-A, *CDMA Card Application Toolkit*, February 2005.
8. C.S0024-A, *cdma2000 High Rate Packet Data Air Interface Specification*, March 2004.
9. C.S0016-C, *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*, October 2004.

- 1 No text.

3 DEFINITIONS AND ABBREVIATIONS

The terms and abbreviations used within this specification are defined as follows:

3.1 Definitions

Corporate code. A code which when combined with a network (Type 1 or Type 2) and SP codes refers to a unique Corporation. The code is provided in the GID2 file on the R-UIM (see Annex A.1.) and is correspondingly stored on the ME.

Corporate code group. Combination of the Corporate code and the associated SP and network codes.

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 R-UIMs.

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

HAT. An access terminal supporting both CDMA 1x and HRPD technologies.

HRPD Network code(s). REALM part of the NAI.

HRPD Network personalization. Allows the network operator to personalize a ME so that it can only be used with that particular HRPD network operator's R-UIMs. HRPD Network personalization is based on the REALM part of the NAI.

IMSI. Can be either an IMSI_M (MIN based IMSI) or an IMSI_T (True IMSI) in the context of this specification.

Mobile Station. In the context of this specification, a mobile station consists of two parts – ME and R-UIM.

NAI. HRPD Network Access Identifier, as defined in [9] Section 3.5.8.13.

Network Type 1 code. A decimal value of MCC and MNC of the IMSI_M or IMSI_T.

Network Type 1 personalization. Allows the network operator to personalize a ME so that it can only be used with that particular network operator's R-UIMs. Network Type 1 personalization is based on MCC and MNC.

Network Type 2 code, or IRM code. The first 4 digits of the decimal value of the IRM based MIN of the IMSI_M.

Network Type 2 personalization. Allows the network operator to personalize a ME so that it can only be used with that particular network operator's R-UIMs. Network Type 2 personalization is based on the 4 Most Significant Digits of the IRM based MIN.

Normal mode of operation. Is the mode of operation into which the ME would have gone if it had no personalization checks to process.

Personalization category. Network Type 1, Network Type 2, SP, Corporation or R-UIM to which the ME is personalized.

1 **Personalization.** Is the process of storing information in the ME and activating the procedures
2 which verify this information against the corresponding information stored in the R-UIM
3 whenever the ME is powered up or an R-UIM is inserted, in order to limit the R-UIMs with
4 which the ME will operate.

5 **REALM.** The 'realm' part of NAI, as defined in [9] Section 3.5.8.13.

6
7 **R-UIM code.** A code which when combined with Network Type 1 and Network Type 2 codes
8 refers to a unique R-UIM.

9
10 **R-UIM code group.** A combination of the R-UIM code and the associated network codes (it is
11 equivalent to the IMSI_M or IMSI_T).

12
13 **R-UIM personalization.** Enables a user to personalize a ME so that it may only be used with
14 particular R-UIM(s).

15
16 **SP code.** A code which when combined with a network (Type 1 or Type 2) code refers to a
17 unique SP. The code is provided in the GID1 file on the R-UIM (see Annex A.1.) and is
18 correspondingly stored on the ME.

19
20 **SP code group.** A combination of the SP code and the associated network code.

21
22 **SP personalization.** Allows the service provider to personalize a ME so that it can only be used
23 with that particular service provider's R-UIMs.

24
25 **User.** Normally refers to the person performing the personalization or de-personalization
26 operations and may represent a network operator, service provider, or manufacturer of the
27 user/owner of the handset, depending on the context.

28

29 **3.2 Abbreviations**

30 **CCK.** Corporate Control Key.

31 **CNL.** Co-operative Network List.

32 **DF.** Directory File.

33 **EF.** Elementary File.

34 **GID1.** Group Identifier (level 1).

35 **GID2.** Group Identifier (level 2).

36 **HAT.** Hybrid Access Terminal.

37 **HNCK.** HRPD Network Control Key.

38 **IMSI.** International Mobile Subscriber Identity.

39 **IRM.** International Roaming MIN.

40 **MCC.** Mobile Country Code.

41 **ME.** Mobile Equipment.

42 **MIN.** Mobile Identification Number.

43 **MNC.** Mobile Network Code.

- 1 **MS.** Mobile Station.
- 2 **MSIN.** Mobile Station Identification Number ([2] 2.3.1)
- 3 **NAI.** Network Access Identifier.
- 4 **NCK1.** Network Type 1 Control Key.
- 5 **NCK2.** Network Type 2 Control Key.
- 6 **PCK.** Personalization Control Key.
- 7 **R-UIM.** Removable User Identity Module.
- 8 **SMS-PP.** SMS Point-to-Point.
- 9 **SPCK.** Service Provider Control Key.

- 1 No text.

1

2 **4 GENERAL FEATURE DESCRIPTION**

3 The ME R-UIM locking mechanism provides subsidy protection to operators by limiting the R-
 4 UIMs that will operate with their MEs. The locking feature works by storing personalization
 5 information in the ME that limits the R-UIMs with which it will work and by checking this
 6 information against the R-UIM upon power up or insertion of an R-UIM. When the ME detects
 7 an R-UIM with parameters differing from its own, it will enter a “limited service state” with only
 8 emergency calls available.

9 ME personalization linked to the CDMA locking mechanism applies independently from other
 10 ME personalization mechanisms related to other network access technologies (e.g. 3GPP
 11 locking as defined in [1]). An ME supporting multiple Network Access Technologies may provide
 12 ME personalization features independently for each technology¹. These fields would then be
 13 matched with the corresponding fields under either DF_{CDMA} or DF_{GSM} , according to the selected
 14 application, prior to using either technology. At the operator’s choice, the locking mechanism
 15 can be made technology-independent simply by aligning the data used for the locking
 16 mechanism on the CDMA and GSM side.

17 For CDMA 1x-only capable ME, five locking categories exist with varying granularity: network
 18 Type 1 (MCC/MNC) and/or Type 2 (first 4 digits of IRM based MIN), service provider (SP),
 19 corporate and R-UIM.

20 For HRPD-only capable ME, four categories exist: HRPD Network (REALM), SP, Corporate and
 21 R-UIM (NAI).

22 For HAT (i.e. CDMA 1x and HRPD capable ME), five locking categories exist as a combination:
 23 Network Type 1+HRPD (MCC/MNC+REALM) and/or Type 2+HRPD (first 4 digits of IRM based
 24 MIN+REALM), SP, corporate and R-UIM.²

25 The personalization categories act independently from the others, allowing the operator to
 26 choose any combination of the categories to lock the ME. Each category uses a separate
 27 personalization indicator to show whether it is active or not. The ME can be personalized to
 28 one network, one IRM group, one Service Provider, one Corporation, one R-UIM or any
 29 combination thereof. The ME may optionally be personalized to multiple networks, multiple
 30 IRM subset, SPs, corporate entities, R-UIMs or any combinations thereof.

31 Table 4-1 lists the codes used for each personalization category. Some categories require
 32 several codes (e.g. SP and network, for SP personalization) and each combination of codes
 33 relating to a particular entity (network, SP etc.) is referred to as a code group. To personalize to
 34 multiple entities, the ME stores multiple code groups. For each activated personalization
 35 category, the ME retrieves the relevant codes from the R-UIM and checks the retrieved code
 36 group against the (list of) code group(s) stored in the ME. If the ME matches any of the R-UIM

¹ For example, a CDMA+GSM multi-mode handset supporting GSM locking as well as CDMA locking shall provide distinct personalization fields for both features. If check result of both modes is different, it is up to operator to decide whether to depersonalize the ME or not.

² For HAT with both indicators (Network Type1+REALM or Network Type 2+REALM) are set to one, if one type of code matches (either Network Type 1 or Network Type 2 or REALM), the terminal shall go to the normal mode of operation.

1 codes with any of its internally stored code groups, the check passes for that category. If the
 2 ME passes the checks for all active categories, the MS goes into normal operation.

3

4

Table 4-1: Codes used by each personalization category for CDMA 1x

Code	Network Type 1 (MCC, MNC)	Network Type 2 (first 4 digits of IRM based MIN)	SP	Corporate	R-UIM (IMSI_M or IMSI_T)
Personalization category					
Network Type 1	✓				
Network Type 2		✓			
SP [Case 1]	✓		✓		
SP [Case 2]		✓	✓		
SP [Case 3]	✓	✓	✓		
Corporate [Case 1]	✓		✓	✓	
Corporate [Case 2]		✓	✓	✓	
Corporate [Case 3]	✓	✓	✓	✓	
R-UIM					✓

5

6

7

Table 4-2: Codes used by each personalization category for HRPD

Code	HRPD Network (REALM)	SP	Corporate	R-UIM (NAI)
Personalization category				
HRPD Network	✓			
SP	✓	✓		
Corporate	✓	✓	✓	
R-UIM				✓

8

9

1

Table 4-3: Codes used by each personalization category for HAT

Code	Network Type 1 (MCC, MNC)	Network Type 2 (first 4 digits of IRM based MIN)	HRPD Network (REALM)	SP	Corporate	R-UIM (IMSI_M or IMSI_T) and NAI
Personalization category						
Network Type 1 + HRPD	✓		✓			
Network Type 2 + HRPD		✓	✓			
SP [Case 1]	✓		✓	✓		
SP [Case 2]		✓	✓	✓		
SP [Case 3]	✓	✓	✓	✓		
Corporate [Case 1]	✓		✓	✓	✓	
Corporate [Case 2]		✓	✓	✓	✓	
Corporate [Case 3]	✓	✓	✓	✓	✓	
R-UIM						✓

2

3 Precautions must be taken to ensure that when more than one personalization category is to
4 be activated or when the ME is to be personalized to more than one entity of a personalization
5 category, the new codes are not in conflict with any existing valid codes. To avoid such
6 conflicts, checks are carried out by the ME during the personalization cycle, as described in
7 Section 13.

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

- 1 No text.

1 **5 NETWORK PERSONALIZATION**

2 **5.1 Network Type 1 personalization for CDMA 1x ME**

3 Network Type 1 personalization allows the personalization of an ME to a particular network, for
4 example to prevent the use of stolen MEs on other networks. The option exists to personalize
5 the ME to more than one network.

6 The ME becomes Network Type 1 personalized by storing the network code (MCC+MNC) of the
7 relevant network(s) in the ME and setting a Network Type 1 personalization indicator in the ME
8 to "on".

9 Example:

10 If the IMSI_M or IMSI_T value is '987 65 1234567890', where: MCC = 987, MNC = 65,
11 and MSIN = 1234567890, then the Network Type 1 code stored in the ME is '987 65'.

12 According to [4] Section 3.4.2 and 3.4.3, MCC and MNC of IMSI_M or IMSI_T are located in
13 EF_{IMSI_M} or EF_{IMSI_T}, and encoded as described in [2] Section 2.3.1.2 and 2.3.1.3.

14 A flag in the ME shall indicate whether the IMSI file in the R-UIM used for this feature is
15 EF_{IMSI_M} (flag value = 0) or EF_{IMSI_T} (flag set to 1). Upon insertion of an R-UIM, or when the ME
16 powers up with an R-UIM already in place, the ME reads the MCC and MNC from the IMSI file
17 of the R-UIM indicated by the flag (IMSI_M or IMSI_T) and checks against that stored values in
18 the ME. If the values differ, the MS shall go into emergency calls only mode as defined in Annex
19 A.2.

20 The Network Type 1 personalization feature is controlled by a Network Type 1 Control Key
21 (NCK1) that has to be entered into the ME in order to de-personalize it.

22 In order to support the Network Type 1 personalization feature the ME shall have storage for
23 the Network Type 1 personalization indicator, the network code(s), the flag indicating the use of
24 IMSI_M or IMSI_T, and the NCK1.

25

26 **5.1.1 Operation of a Network Type 1 personalized ME**

27 An ME performs the Network Type 1 personalization check described below upon the insertion
28 of an R-UIM or during power up with an R-UIM already in place.

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

- 32 a. **check whether the ME is Network Type 1 personalized:** The ME checks its Network
33 Type 1 personalization indicator, if it is set to "off" the personalization check shall stop
34 and the MS enters normal mode of operation, omitting the remaining steps of the check;
- 35 b. **check the Network Type 1 code(s):** The ME reads from DF_{CDMA} the IMSI file indicated
36 by the flag (IMSI_M or IMSI_T) on the R-UIM, extracts the Network Type 1 code from it
37 and checks it against the list of value(s) stored on the ME.

1 If no match is found in (b), the ME may display an appropriate message, (e.g., "Incorrect R-
2 UIM") and shall go into the emergency calls only mode as defined in Annex A.2. If the ME does
3 find a match it shall go into the normal mode of operation.

4

5 **5.1.2 Network Type 1 personalization cycle**

6 **5.1.2.1 Personalization cycle**

7 The process of personalization can only be carried out on a currently unpersonalized ME, i.e., if
8 the network personalization indicator is set to "off". Access to the personalization process shall
9 be restricted in order to prevent unauthorized, accidental or unwanted personalization. Other
10 restrictions are described in Section 13. The personalization process results in setting the
11 NCK1, setting the Network Type 1 personalization indicator to "on" and the storage in the ME
12 of the Network Type 1 code(s) to which the ME is being personalized.

13 The Network Type 1 personalization process is as follows:

- 14 a. Entering the MCCs and MNCs into the ME. This may be accomplished by one of the
15 following means:
 - 16 - For the case of a single Network Type 1 code, the ME first checks whether an
17 IMSI_M value has been provisioned on the R-UIM. If this is not the case, the ME
18 sets its IMSI flag to 1, otherwise it is set to 0. Then the ME reads the IMSI (IMSI_M
19 or IMSI_T as indicated by the flag) from the R-UIM and extracts the Network Type 1
20 code;
 - 21 - The ME reads the CDMA Co-operative Network List (EF_{CDMACNL}) from the R-UIM and
22 extracts the list of Network Type 1 code(s) associated with Network Type 1
23 personalization. In this case, the IMSI flag indicating the use of IMSI_M or IMSI_T
24 shall be entered either by keypad entry, or by a manufacturer defined process.
 - 25 - keypad entry;
 - 26 - a manufacturer defined process.
- 27 b. The ME carries out the pre-personalization checks contained in Section 13 on the new
28 codes entered into the ME. If they all pass, the IMSI flag, MCC(s) and MNC(s) is (are)
29 stored in the ME. If any fail, the personalization process shall be terminated.
- 30 c. Storing the NCK1 in the ME. This may be entered via the keypad by the user or by a
31 manufacturer defined process.
- 32 d. Setting the Network Type 1 personalization indicator to "on".

33

34 **5.1.2.2 De-personalization cycle**

35 To de-personalize the ME, the correct NCK1 shall be entered. It is optional whether or not an
36 R-UIM is inserted in the ME. If an R-UIM is inserted, then de-personalization shall be offered
37 whether or not the network personalization check passes or fails.

38 Network Type 1 de-personalization shall be possible by keypad entry. If there is no keypad,
39 then an alternative ME-based solution shall be provided. Other de-personalization methods

1 may also be provided such as a network initiated process whereby the control key is sent to the
2 MS over-the-air (see Section 9).

3 The Network Type 1 de-personalization process is as follows:

- 4 a. Entering the NCK1 into the ME;
- 5 b. Setting the personalization indicator to "off" if the entered NCK1 equals the one
6 stored in the ME.

7 If the entered and stored NCK1 values differ, the de-personalization process shall be stopped.
8 The ME remains personalized and the stored Network Type 1 code(s) and NCK1 shall be left
9 unchanged.

10

11 **5.2 Network Type 2 personalization for CDMA 1x ME**

12 Network Type 2 personalization allows network operators to limit the usage of a ME to a well
13 defined subset of R-UIM having particular IRM codes. This can only be used with the IMSI_M,
14 i.e., when the IMSI flag value is set to 0.

15 The ME is Network Type 2 personalized by storing the Network Type 2 code (four most
16 significant digits of MIN) as an identification of the IRM and setting a Network Type 2
17 personalization indicator in the ME to "on".

18 Example:

19 If the IMSI_M value is '987 65 1234567890', where: MCC = 987, MNC = 65, and MIN =
20 1234567890, then the Network Type 2 code stored in the ME is '1234'.

21 According to [4] Section 3.4.2, MIN of IMSI_M are located in EF_{IMSI_M}, and encoded as described
22 in [2] Section 2.3.1.1.

23 Whenever an R-UIM is inserted, or the MS is powered up with an R-UIM already in place, the
24 Network Type 2 code is read from the R-UIM and checked against the stored values in the ME.
25 If no match is found, the ME shall go into emergency calls only mode, as defined in Annex A.2.

26 The Network Type 2 personalization feature is controlled by a Network Type 2 Control Key
27 (NCK2) that has to be entered into the ME in order to de-personalize it.

28 In order to support the Network Type 2 personalization feature, the ME shall have storage for
29 the Network Type 2 personalization indicator, the Network Type 2 code and the NCK2.

30

31 **5.2.1 Operation of Network Type 2 personalized ME**

32 The Network Type 2 personalization check described below is performed whenever an R-UIM is
33 inserted or the ME is powered up with an R-UIM already in place.

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

- 36 **a) check whether the ME is Network Type 2 personalized:** The ME checks its Network
37 Type 2 personalization indicator, if it is set to "off" the personalization check shall be

1 stopped and the ME goes into the normal mode of operation, omitting the remaining steps
2 of the check;

3 **b) check Network Type 2 code:** The ME reads the IMSI_M file from DF_{CDMA} on the R-UIM,
4 extracts the Network Type 2 code from it and checks it against the list of value(s) stored on
5 the ME.

6 If no match is found in (b) the ME may display an appropriate message (e.g. "Insert correct R-
7 UIM") and shall go into emergency calls only mode, as defined in Annex A.2. Otherwise the ME
8 goes into the normal mode of operation.

9

10 **5.2.2 Network Type 2 personalization cycle**

11 **5.2.2.1 Personalization Cycle**

12 The process of personalization can only be carried out on a currently unpersonalized ME, i.e., if
13 the Network Type 2 personalization indicator is set to "off". Access to the personalization
14 process shall be restricted in order to prevent unauthorized, accidental or unwanted
15 personalization. Other restrictions are described in Section 13. The personalization process
16 results in the NCK2 being set, the Network Type 2 personalization indicator being set to "on"
17 and the storage in the ME of the (list of) Network Type 2 code, which identify the specific IRM
18 code(s) to which the ME is being personalized.

19 The Network Type 2 personalization process is as follows:

20 a) The Network Type 2 code is entered into the ME. This may be accomplished by one of the
21 following means:

22 - For the case of a single Network Type 2 code, the ME first sets the IMSI flag value to 0 to
23 indicate use of the IMSI_M. Then the ME reads the IMSI_M from the R-UIM and extracts
24 the IRM code;

25 - The ME first sets the IMSI flag value to 0 to indicate use of the IMSI_M. Then the ME
26 reads the CDMA Co-operative Network List (EF_{CDMACNL}) from the R-UIM and extracts the
27 list of IRM code(s) associated with network personalization.

28 - keypad entry;

29 - a manufacturer-defined process

30 b) The ME carries out the pre-personalization checks contained in Section 13, on the new
31 codes entered into the ME. If they all pass, the IRM code group(s) is (are) stored in the ME.
32 If any fails, the personalization process shall be terminated.

33 c) The NCK2 is stored in the ME. This may be entered via the keypad by the user or by a
34 manufacturer defined process.

35 d) The Network Type 2 personalization indicator is set to "on".

36

1 **5.2.2.2 De-personalization cycle**

2 To de-personalize the ME the correct NCK2 shall be entered. It is optional whether or not an R-
3 UIM is inserted. If an R-UIM is inserted, then de-personalization shall be offered whether or not
4 the Network Type 2 personalization check passes or fails.

5 Network Type 2 de-personalization shall be possible by keypad entry. If there is no keypad,
6 then an alternative ME-based solution shall be provided. Other de-personalization methods
7 may also be provided such as a network initiated process whereby the control key is sent to the
8 MS over-the-air (see Section 9).

9 The Network Type 2 de-personalization process is as follows:

10 a) the NCK2 is entered into the ME;

11 b) if the entered NCK2 is the same as the one stored in the ME, then the Subset
12 personalization indicator is set to "off".

13 If the entered and stored NCK2 values differ, the de-personalization process shall be stopped
14 and the ME remains personalized. The stored Network Type 2 code and the NCK2 are left
15 unchanged.

16

17 **5.3 Network personalization for HRPD terminal**

18 HRPD Network personalization allows the personalization of an ME to a particular network, for
19 example to prevent the use of stolen MEs on other networks. The option exists to personalize
20 the ME to more than one HRPD network.

21 The ME becomes HRPD Network personalized by storing the REALM code of the relevant
22 network(s) in the ME and setting a HRPD Network personalization indicator in the ME to "on".

23 An HNCK (HRPD Network Control Key) controls the HRPD Network personalization feature.
24 The HNCK shall be entered into the ME in order to HRPD Network de-personalize it.

25 In order to support the HRPD Network personalization feature the ME shall have storage for
26 the HRPD Network personalization indicator, the REALM code(s), and the HNCK.

27

28 **5.3.1 Operation of HRPD Network personalized ME**

29 An ME performs the HRPD Network personalization check described below upon the insertion
30 of an R-UIM or during power up with an R-UIM already in place.

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

34 a. **check whether the ME is HRPD Network personalized:** The ME checks its HRPD
35 Network personalization indicator, if it is set to "off" the personalization check shall stop
36 and the MS enters normal mode of operation, omitting the remaining steps of the check;

37 b. **check the HRPD Network code(s):** The ME reads the $EF_{HRPDUPP}$ (HRPD Access
38 Authentication User Profile Parameter file) from DF_{CDMA} on the R-UIM, extracts the
39 REALM from NAI and checks it against the list of value(s) stored on the ME.

1 If no match is found in (b), the ME may display an appropriate message, (e.g., "Incorrect R-
2 UIM") and shall go into the emergency calls only mode as defined in Annex A.2. If the ME does
3 find a match it shall go into the normal mode of operation.

4

5 **5.3.2 HRPD Network personalization cycle**

6 **5.3.2.1 Personalization Cycle**

7 The process of personalization can only be carried out on a currently unpersonalized ME, i.e., if
8 the HRPD network personalization indicator is set to "off". Access to the personalization
9 process shall be restricted in order to prevent unauthorized, accidental or unwanted
10 personalization. Other restrictions are described in Section 13. The personalization process
11 results in setting the HNCK, the HRPD Network personalization indicator to "on" and the
12 storage in the ME of the HRPD Network code(s) to which the ME is being personalized.

13 The HRPD Network personalization process is as follows:

- 14 a. Entering the REALM into the ME. This may be accomplished by one of the following
15 means:
 - 16 - keypad entry;
 - 17 - a manufacturer defined process.
- 18 b. The ME carries out the pre-personalization checks contained in Section 13 on the new
19 codes entered into the ME. If they all pass, the HRPD Network code(s) are stored in the
20 ME. If any fail, the personalization process shall be terminated.
- 21 c. Storing the HNCK in the ME. This may be entered via the keypad by the user or by a
22 manufacturer defined process.
- 23 d. Setting the HRPD Network personalization indicator to "on".

24

25 **5.3.2.2 De-personalization cycle**

26 To de-personalize the ME, the correct HNCK shall be entered. It is optional whether or not an
27 R-UIM is inserted in the ME. If an R-UIM is inserted, then de-personalization shall be offered
28 whether or not the HRPD Network personalization check passes or fails.

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

33 The HRPD Network de-personalization process is as follows:

- 34 a. Entering the HNCK into the ME;
- 35 b. Setting the personalization indicator to "off" if the entered HNCK equals the one stored
36 in the ME.

- 1 If the entered and stored HNCK values differ, the de-personalization process shall be stopped.
- 2 The ME remains personalized and the stored HRPD Network code(s) and HNCK shall be left
- 3 unchanged.

1 No text.

1 **6 SERVICE PROVIDER PERSONALIZATION**

2 Service provider or SP personalization is a feature that allows a service provider to associate a
3 ME with the SP. This feature only works with R-UIMs that support the GID1 file under DF_{CDMA}.
4 For the purpose of SP personalization, the GID1 file contains an SP code that identifies the
5 service provider.

6 The ME is SP personalized by storing the SP code group(s) and setting a SP personalization
7 indicator in the ME to "on". Whenever an R-UIM is inserted, or the ME powers up with an R-
8 UIM already in place, the SP code group is read from the R-UIM and checked against those
9 stored in the ME. If the ME does not find a match, it shall go into emergency calls only mode as
10 defined in Annex A.2.

11 SP Personalization is used in conjunction with Network personalization.

12 For CDMA 1x ME, if IMSI_T is used, then the Network personalization is Network Type 1
13 personalization. If IMSI_M is used, then the Network personalization may be either Network
14 Type 1 or Network Type 2, or both (see Table 4-1).

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

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

19 **6.1 Operation of SP personalized MEs**

20 The personalization check described below is performed whenever an R-UIM is inserted or the
21 ME is powered up with an R-UIM already in place.

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

- 24 a. **check whether the ME is SP personalized:** The ME checks the SP personalization
25 indicator, if it is set to "off" the personalization check shall be stopped and the ME goes
26 into its normal mode of operation;
- 27 b. **check whether the R-UIM supports GID1:** The ME checks that the R-UIM supports
28 the GID1 file under DF_{CDMA};
- 29 c. **check the SP code group:** The ME reads the SP code group from DF_{CDMA} in the R-UIM
30 and checks it against the (list of) stored value(s) on the ME;

31 If (b) fails or no match is found in (c), the ME may display an appropriate message (e.g. "Insert
32 correct R-UIM ") and shall go into emergency calls only mode, as defined in Annex A.2.
33 Otherwise, the ME goes into the normal mode of operation.
34

35

1 **6.2 SP personalization cycle**

2 **6.2.1 Personalization cycle**

3 The process of personalization can only be carried out on a currently unpersonalized ME, i.e., if
 4 the SP personalization indicator is set to "off". Access to the personalization process shall be
 5 restricted in order to prevent unauthorized, accidental or unwanted personalization. Other
 6 restrictions are described in Section 13. The personalization process results in the SPCK being
 7 set, the SP personalization indicator being set to "on" and the storage in the ME of the (list of)
 8 SP code group(s) to which the ME is being personalized.

9 The SP personalization process is as follows:

- 10 a. The SP code group(s) is (are) entered into the ME. This may be accomplished by one of
 11 the following means:
 - 12 - the ME checks that the R-UIM supports the GID1 file under DF_{CDMA} , and if not the
 13 SP personalization process is aborted with an appropriate error message. Then the
 14 ME reads the SP code group from the R-UIM. If the SP code is set to the default
 15 value (see Annex A.1) then the personalization process shall be aborted with an
 16 appropriate error message; otherwise the SP code group is entered into the ME.
 - 17 - the ME reads the CDMA Co-operative Network List ($EF_{CDMACNL}$) from the R-UIM and
 18 extracts the (list of) SP code group(s);
 - 19 - keypad entry;
 - 20 - a manufacturer defined process.
- 21 b. The ME carries out the pre-personalization checks contained in Section 13 on the new
 22 codes entered into the ME. If they all pass, the SP code group(s) is (are) stored in the
 23 ME. If any fail, the personalization process shall be terminated.
- 24 c. The SPCK is stored in the ME. This may be entered via the keypad by the user or by a
 25 manufacturer defined process.
- 26 d. The SP personalization indicator is set to "on".

27

28 **6.2.2 De-personalization cycle**

29 To de-personalize the ME, the correct SPCK shall be entered. It is optional whether or not an R-
 30 UIM is inserted in the ME. If an R-UIM is inserted, then de-personalization shall be offered
 31 whether or not the SP personalization check passes or fails.

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

36 The SP de-personalization process is as follows:

- 37 a. the SPCK is entered into the ME;

- 1 b. if the entered SPCK is the same as the one stored in the ME, the SP personalization
- 2 indicator is set to "off".
- 3 If the entered and stored SPCK values differ, the de-personalization process shall be stopped
- 4 and the ME remains SP personalized. The stored Network and SP codes and SPCK shall be left
- 5 unchanged.

1 No text.

1 **7 CORPORATE PERSONALIZATION**

2 Corporate personalization refines SP personalization by allowing companies to prevent the use
3 of MEs they provide for their employees or customers with other R-UIMs without corporate
4 personalization.

5 This feature only works with R-UIMs that support both the GID1 and GID2 files under DF_{CDMA}.
6 For the purpose of corporate personalization the GID1 file is programmed at
7 pre-personalization with an SP code that identifies the service provider and the GID2 file is
8 programmed by the service provider or corporate customer with a code that identifies the
9 corporate customer.

10 The ME is Corporate personalized by storing the Corporate code group(s) and setting a
11 Corporate personalization indicator in the ME to "on". Whenever an R-UIM is inserted, or the
12 ME is powered up with an R-UIM already in place, the Corporate code group is read from
13 DF_{CDMA} in the R-UIM and checked against those stored in the ME. If there is no match the ME
14 shall go into emergency calls only mode, as defined in Annex A.2.

15 Corporate personalization is used in conjunction with Network Personalization and SP
16 Personalization. For CDMA 1x ME, if IMSI_T is used, then the Network personalization is
17 Network Type 1 personalization. If IMSI_M is used, then the Network personalization may be
18 either Network Type 1 or Network Type 2, or both (see Table 4-1).

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

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

23

24 **7.1 Operation of corporate personalized MEs**

25 The personalization check described below is performed whenever an R-UIM is inserted or the
26 ME is powered up with an R-UIM already in place.

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

- 29 a. **check whether the ME is corporate personalized:** The ME checks the Corporate
30 personalization indicator, if it is set to "off" the personalization check shall be stopped
31 and the ME goes into its normal mode of operation;
- 32 b. **check whether the R-UIM supports GID1 and GID2 under DF_{CDMA}:** The ME checks
33 that the R-UIM supports the GID1 and GID2 files under DF_{CDMA};
- 34 c. **check the corporate code group:** The ME reads the corporate code group from the R-
35 UIM and checks it against the (list of) stored value(s) on the ME.

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

39

1 **7.2 Corporate personalization cycle**

2 **7.2.1 Personalization cycle**

3 The process of personalization can only be carried out on a currently unpersonalized ME, i.e., if
 4 the corporate personalization indicator is set to "off". Access to the personalization process
 5 shall be restricted in order to prevent unauthorized, accidental or unwanted personalization.
 6 Other restrictions are described in Section 13. The personalization process results in the CCK
 7 being set, the Corporate personalization indicator being set to "on" and the storage in the ME of
 8 a (list of) corporate group(s) codes to which the ME is being personalized.

9 The Corporate personalization process is as follows:

- 10 a. The Corporate code group(s) is (are) entered into the ME. This may be accomplished by
 11 one of the following means:
 - 12 - the ME checks that the R-UIM supports the GID1 and GID2 files under DF_{CDMA}, if
 13 not the Corporate personalization process shall be aborted with an appropriate error
 14 message. Then the ME reads the corporate code group(s) from DF_{CDMA} in the R-UIM .
 15 If either the SP code or the Corporate code is set to the default value (see Annex
 16 A.1), then the corporate personalization process shall be aborted with an
 17 appropriate error message. Otherwise the corporate code group is entered into the
 18 ME;
 - 19 - The ME reads the CDMA Co-operative Network List (EF_{CDMACNL}) from DF_{CDMA} in the R-
 20 UIM and extracts the (list of) Corporate code group(s);
 - 21 - keypad entry;
 - 22 - a manufacturer defined process.
- 23 b. The ME carries out the pre-personalization checks contained in Section 13 on the new
 24 codes entered into the ME. If they all pass, the Corporate code group(s) is (are) stored in
 25 the ME. If any fail, the personalization process shall be terminated.
- 26 c. The CCK is stored in the ME. This may be entered via the keypad by the user or by a
 27 manufacturer defined process;
- 28 d. The corporate personalization indicator is set to "on".

29

30 **7.2.2 De-personalization cycle**

31 To de-personalize the ME the correct CCK shall be entered. It is optional whether or not an R-
 32 UIM is inserted in the ME. If an R-UIM is inserted, then de-personalization shall be offered
 33 whether or not the Corporate personalization check passes or fails.

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

- 38 a. the CCK is entered into the ME;

- 1 b. if the entered CCK is the same as the one stored in the ME, the corporate
- 2 personalization indicator is set to "off".
- 3 If the entered and stored CCK values differ the de-personalization process shall be stopped and
- 4 the ME remains Corporate personalized. The stored Network, SP, Corporate codes and CCK are
- 5 left unchanged.

1 No text.

1 **8 R-UIM PERSONALIZATION**

2 R-UIM personalization operates as an anti-theft feature. When an ME is R-UIM personalized to
 3 a particular R-UIM it will not operate with any other R-UIM. Hence, if a thief steals an R-UIM
 4 personalized ME, the thief cannot use it with another R-UIM. While this does not stop the ME
 5 being stolen, it makes the ME less attractive to steal. Additionally, by locking the ME to a
 6 particular R-UIM, the operator can render the ME useless once it disconnects service to that
 7 account.

8 NOTE: If the ME and the R-UIM to which it has been personalized are stolen together
 9 the ME would become unusable once the R-UIM is reported stolen and is disconnected.

10 The ME is R-UIM personalized by storing the R-UIM code group (which is equivalent to the
 11 IMSI for CDMA 1x ME, or NAI for HRPD ME) of the relevant R-UIM in the ME and setting the R-
 12 UIM personalization indicator in the ME to "on". Whenever an R-UIM is inserted, or the ME is
 13 powered up with an R-UIM already in place, the R-UIM code group (IMSI_M or IMSI_T
 14 according to the IMSI flag mentioned in Section 5 for CDMA 1x ME, or NAI for HRPD ME) is
 15 read from the R-UIM and checked against the R-UIM code group(s) stored in the ME. If there is
 16 no match the ME shall go into emergency calls only mode as described in Annex A.2.

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

20 In order to support the R-UIM personalization feature the ME should have storage for the R-
 21 UIM personalization indicator, the IMSI flag indicating use of IMSI_M or IMSI_T (for CDMA 1x
 22 ME), a (list of) R-UIM code group(s) and the PCK.

23 **For CDMA 1x ME:**

24 Multiple instances of R-UIM personalization can be supported, i.e. whenever an R-UIM is
 25 inserted, or the ME is powered up with an R-UIM already in place, the IMSI file (IMSI_M or
 26 IMSI_T) indicated by the IMSI flag is read from DF_{CDMA} in the R-UIM and checked against a list
 27 of R-UIM code groups stored in the ME.

28 **For HRPD ME:**

29 Multiple instances of R-UIM personalization can be supported, i.e. whenever an R-UIM is
 30 inserted, or the ME is powered up with an R-UIM already in place, the NAI of EF_{HRPDUPP} (HRPD
 31 Access Authentication User Profile Parameter file) is read from DF_{CDMA} in the R-UIM and
 32 checked against a list of R-UIM code groups stored in the ME.

34 **8.1 Operation of R-UIM personalized ME**

35 The R-UIM personalization check described below is performed whenever an R-UIM is inserted
 36 or the ME is powered up with an R-UIM already in place.

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

- 1 a. **check whether the ME is R-UIM personalized:** The ME checks its R-UIM
 2 personalization indicator, if it is set to "off" the personalization check shall be stopped
 3 and the ME goes into the normal mode of operation, omitting the remaining steps of the
 4 check;
- 5 b. **read IMSI or NAI:** For CDMA 1x ME, the ME reads the IMSI_M or the IMSI_T from the
 6 R-UIM, according to the value of its IMSI flag (0 for IMSI_M and 1 for IMSI_T). For HRPD
 7 ME, the ME reads the NAI of EF_{HRPDUPP} (HRPD Access Authentication User Profile
 8 Parameter file) in DF_{CDMA} from the R-UIM
- 9 c. **R-UIM personalization check:** For CDMA 1x ME, the ME checks the read IMSI
 10 (IMSI_M or IMSI_T according to the value of the IMSI flag) against the (list of) R-UIM
 11 code group(s) stored in the ME. For HRPD ME, the ME checks the NAI against the (list
 12 of) R-UIM code group(s) stored in the ME. If no match is found, the ME shall display an
 13 appropriate message (e.g. "Insert correct R-UIM") and shall go into emergency calls only
 14 mode as described in Annex A.2. Otherwise, the ME goes into the normal mode of
 15 operation.

16

17 **8.2 R-UIM personalization cycle**

18 **8.2.1 Personalization cycle**

19 The process of personalization can only be carried out on a currently unpersonalized ME, i.e., if
 20 the R-UIM personalization indicator is set to "off". Access to the personalization process shall
 21 be restricted in order to prevent unauthorized, accidental or unwanted personalization. Other
 22 restrictions are described in Section 13. The personalization process results in the PCK being
 23 set, the R-UIM personalization indicator being set to "on" and the storage in the ME of a (list of)
 24 R-UIM code group(s) to which the ME is being personalized.

25 The R-UIM personalization process is as follows:

- 26 a. For CDMA 1x ME, the IMSI flag and R-UIM code group(s) is (are) entered into the ME.
 27 This may be accomplished by one of the following means :
- 28 - The ME reads the R-UIM code group (IMSI_M or IMSI_T) from the R-UIM and stores
 29 it. If an IMSI_M is provisioned in the R_UIM, the IMSI flag value is 0 and the IMSI_M
 30 is used, otherwise the IMSI flag is set to 1 and the IMSI_T is used;
 - 31 - a manufacturer defined process.

32 For HRPD ME, the R-UIM code group(s) is (are) entered into the ME. This may be
 33 accomplished by one of the following means:

- 34 - the ME reads the R-UIM code group (NAI) from the R-UIM and stores it;
- 35 - a manufacturer defined process.

36 b. The ME carries out the pre-personalization checks contained in Section 13. If they all
 37 pass, the R-UIM code group(s) is (are) stored in the ME. If any fails, the personalization
 38 process shall be terminated;

39 c. to personalize the ME to more than one R-UIM and for CDMA 1x ME, if the reading of
 40 the IMSI from the R-UIM is used to enter the R-UIM code group in the ME, the

1 procedures given in (a) and (b) shall be repeated; the IMSI flag value however is decided
2 at the time the first R-UIM is inserted and is then used to decide which IMSI (IMSI_M or
3 IMSI_T) will be read from the following R-UIMs (the ME cannot be personalized to accept
4 a mix of IMSI_M and IMSI_T). For HRPD ME, if the reading of NAI from the R-UIM is
5 used to enter the R-UIM code group in the ME, the procedures given in (a) and (b) shall
6 be repeated;

- 7 d. The PCK is then stored in the ME. A single value of PCK shall be used for both single
8 and multiple R-UIM personalization;
- 9 e. The R-UIM personalization indicator is set to "on".

10

11 **8.2.2 De-personalization cycle**

12 To de-personalize the ME, the correct PCK shall be entered. It is optional whether or not an R-
13 UIM is inserted in the ME. If an R-UIM is inserted, then de-personalization shall be offered
14 whether or not the R-UIM personalization check passes or fails.

15 R-UIM de-personalization shall be provided by keypad entry. Other de-personalization methods
16 may also be provided.

17 The R-UIM de-personalization process is as follows:

- 18 a. the user enters the PCK in the ME;
- 19 b. if the entered PCK is the same as the one stored in the ME, the R-UIM personalization
20 indicator is set to "off".

21 If the entered and stored PCK values differ, the de-personalization process shall stop and the
22 ME remains personalized. The stored IMSI or REALM and PCK are left unchanged.

1 No text.

1 **9 OVER THE AIR DE-PERSONALIZATION CYCLE**

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

6 The OTA method defined below uses Mobile Terminated SMS-PP messages. With this method,
7 the keys of the personalization categories to be de-personalized are sent to the ME via the R-
8 UIM. The ESN or MEID is not included and the de-personalization process only checks the
9 keys. The outcome of the attempted de-personalization(s) is acknowledged to the network.

10 The network de-personalizes the ME by the following method:

- 11 a) An SMS message is sent by the network to the R-UIM updating the file EF_{DCK} under
12 DF_{CDMA}. This shall be done by using the SMS-PP Data Download of the CDMA Card
13 Applications Toolkit (see [7]).
- 14 b) The R-UIM causes the ME to send an SMS acknowledgement to the network, as a result
15 of the terminal response to the ENVELOPE command.
- 16 c) The R-UIM shall issue a REFRESH command to instruct the ME to perform an
17 initialization procedure. During the initialization procedure the ME reads the
18 de-personalization key field(s) from EF_{DCK} stored under DF_{CDMA} in the R-UIM after
19 performing all personalization checks.
- 20 d) For each control key in EF_{DCK} which is empty (set to default), the corresponding
21 personalization status shall be left unchanged.
- 22 e) For each control key in the EF_{DCK} which is not the same as the corresponding stored
23 key, the personalization status shall be left unchanged.
- 24 f) For each control key in EF_{DCK} which is the same as the one stored in the ME, the
25 corresponding personalization indicator is set to "off".
- 26 g) All the keys in the EF_{DCK} under DF_{CDMA} are reset to the default value by the ME.

- 1 No text.

1 10 DISABLE PERSONALIZATION

2 There shall be a means to disable the personalization at each level individually such that the
3 ME shall operate with any R-UIM at that level.

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

1 No text.

1 11 MANUFACTURER PERSONALIZATION AND DE-PERSONALIZATION

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

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

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

10 As an optional ME feature, the ME may be de-personalized over-the-air (OTA) using Mobile
11 Terminated SMS-PP messages (as described in Section 9) or proprietary packet data
12 applications.

13

- 1 No text.

1 12 AUTOMATIC PERSONALIZATION

2 ME manufacturers may offer alternative means of personalizing the ME such as adding
3 functionality to the ME so that it automatically personalizes itself to the first R-UIM inserted in
4 it, using one or more of the four personalization levels described in Sections 5 to 8. In the case
5 of SP and corporate personalization, this is subject to the R-UIM supporting the GID1 and
6 GID2 files under DF_{CDMA} (as required) and the contents of those files being non-default.

1 No text.

1 **13 PERSONALIZATION CYCLE RESTRICTIONS**

2 Security mechanisms shall be implemented to ensure that additions or changes to any
3 personalization category shall only be made by persons authorized to do so for that category
4 (see Section 14).

5 During the Personalization cycle of a category, before any changes are made to the existing
6 personalization data, it shall be checked that:

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

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

11 NOTE 1: If no personalization category is active, then no checks are necessary.

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

15 NOTE 3: After each personalization cycle, the number of R-UIMs with which the ME can
16 operate decreases. If further personalization cycles of specific personalization categories are to
17 be prevented, the disable-personalization feature can be used (see Section 10).

1 No text.

1 **14 SECURITY**

2 This section lists a number of security requirements that should be satisfied if the
3 personalization features are to be effective. The requirements are not arranged in any
4 particular order.

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

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

10 c) The NCK1, NCK2, HNCK, SPCK and CCK should be randomly selected or
11 pseudo-randomly generated and differ from ME to ME.

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

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

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

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

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

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

33 j) ME manufacturers should ensure that the personalization processes (except for R-UIM
34 personalization) are protected against unauthorized, accidental or malicious operation.

- 1 No text.

1 **ANNEX A (NORMATIVE): TECHNICAL INFORMATION**

2 **A.1 GID1 and GID2 files**

3 The GID1 and GID2 elementary files on the R-UIM are specified in [4].

4 An R-UIM is said to support one of these two files if it is marked as both allocated and
5 activated in the CDMA service table.

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

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

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

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

15

16 **A.2 Emergency calls only mode**

17 The expression "emergency calls only mode" is used in this specification to describe the state of
18 the MS when a personalization check fails. In this mode, the MS shall only perform Emergency
19 calls as if no R-UIM was inserted into the ME. Although the personalization has failed, the ME
20 will be able to access the TMSI and IMSI from the R-UIM, and therefore any emergency call
21 request shall use these as the MS/R-UIM identity.

22

23 **A.3 CDMA Co-operative Network List**

24 The CDMA Co-operative Network List is specified in [4].

25 For the purposes of this specification, an R-UIM is said to support this feature if it is marked
26 as both allocated and activated in the CDMA service table.

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

29

30 **A.4 De-personalization Control Key**

31 This file is only used for over the air de-personalization cycle, as specified in Section 9.