Source: **SMG**

Title: **Change Request to GSM 02.16 to ensure IMEI security**

Document for: **Approval**

Agenda Item: **5.1.4**

Summary:

The changes encompassed in this document were approved in principle at SMG #30.

They are the result of substantial discussion at SMG #30 with eventual agreement.

CHANGE REQUEST No :	**A005 r1**	*Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.*

Technical Specification GSM/UMTS	02.16	Version	4.5.0

Submitted to SMG #30 *list plenary meeting or STC here ↑*	For approval for information	**X**	Without presentation ("non-strategic") with presentation ("strategic")	**X**

Proposed change affects: *(at least one should be marked with an X)* SIM ☐ ME **X** Network ☐ **Workitem:**

Source: SMG#30 **Date:** 12.15.1999

Subject: Modification of section 2 to enhance IMEI security

Category: *(one category and one release shall be marked with an X)*

				Release:		
F	Correction	**X**		Phase 2	**X**
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	
				UMTS	

Reason for change: The security of the IMEI was not sufficiently given by the core specification. Therefore GSM 02.09 was modified. GSM 02.16 needs to be aligned with GSM 02.09. The modification is reflected in this CR.

Clauses affected: Section 2

Other specs affected: *(One or more may be marked with an X)*

Other releases of same spec	**X**	→ List of CRs:
Other core specifications		→ List of CRs:
MS test specifications / TBRs		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments:

0 Introduction

0.1 Scope

The purpose of this specification is to define the principal purpose and use of International Mobile station Equipment Identities (IMEI).

The specification GSM 03.03 describes the technical manner of numbering, addressing and identification.

0.2 Normative references

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

[1]   GSM 01.04 (ETR 100): "European digital cellular telecommunication system (Phase 2); Definitions, abbreviations and acronyms".

[2]   GSM 02.17 (ETS 300 509): "European digital cellular telecommunication system (Phase 2); Subscriber identity modules Functional characteristics".

[3]   GSM 03.03 (ETS 300 523): "European digital cellular telecommunication system (Phase 2); Numbering, addressing and identification".

[4]   ISO/IEC 7812 (1989): "Identification cards - Numbering system and registration procedure for issuer identifiers".

0.3 Definitions and abbreviations

In addition to the following, abbreviations used in this specification are listed in GSM 01.04.

International Mobile Station Equipment Identity (IMEI)
An "International Mobile Station Equipment Identity" is a unique number which shall be allocated to each individual mobile station equipment in the GSM system and shall be unconditionally implemented by the MS manufacturer.

1 Not used

2 General

As described in specification GSM 02.17, an MS can only be operated if a valid "International Mobile Subscriber Identity" (IMSI) is present. An IMSI is primarily intended for obtaining information on the use of the GSM network by subscribers for individual charging purposes.

Besides the IMSI, the implementation of IMEI is found necessary in order to obtain knowledge about the presence of specific mobile station equipment in the network, disregarding whatever subscribers are making use of these equipments.

The main objective is to be able to take measures against the use of stolen equipment or against equipment of which the use in the GSM system can not or no longer be tolerated for technical reasons.

The IMEI is incorporated in an MS module which is contained within the MS equipment. The IMEI shall not be changed after the ME's final production process. It shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software).

> NOTE: This requirement is valid for new GSM Phase 2 and Release 96, 97, 98 and 99 MEs type approved after 1st June 2002.

This implementation of each individual module should be carried out by the manufacturer who is also responsible for ascertaining that each IMEI is unique and keeping detailed records of produced and delivered MS.

CHANGE REQUEST No :	**A006 r1**	*Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.*

Technical Specification GSM/UMTS	02.16	Version	5.0.0

Submitted to SMG	#30	For approval	**X**	Without presentation ("non-strategic")	
list plenary meeting or STC here ↑		for information		with presentation ("strategic")	**X**

PT SMG CR cover form. Filename: crf26_2.doc

Proposed change affects:
(at least one should be marked with an X)

SIM [ ]   ME [X]   Network [ ]   **Workitem:**

Source: ETSI SMG10, GSMA Security Group & GSMA Terminal Working Group   **Date:** 15.12.1999

Subject: Modification of section 2 to enhance IMEI security

Category:

(one category

and one release

shall be marked

with an X)

			Release:		
F	Correction	**X**		Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	**X**
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	
				UMTS	

Reason for change: The security of the IMEI was not sufficiently given by the core specification. Therefore GSM 02.09 was modified. GSM 02.16 needs to be aligned with GSM 02.09. The modification is reflected in this CR.

Clauses affected: Section 2

Other specs affected:

(One or more may be marked with an X)

Other releases of same spec	**X**	→ List of CRs:
Other core specifications		→ List of CRs:
MS test specifications / TBRs		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments:

0 Introduction

0.1 Scope

The purpose of this specification is to define the principal purpose and use of International Mobile station Equipment Identities (IMEI).

The specification GSM 03.03 describes the technical manner of numbering, addressing and identification.

0.2 Normative references

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

[1]   GSM 01.04 (ETR 100): "European digital cellular telecommunication system (Phase 2); Definitions, abbreviations and acronyms".

[2]   GSM 02.17 (ETS 300 509): "European digital cellular telecommunication system (Phase 2); Subscriber identity modules Functional characteristics".

[3]   GSM 03.03 (ETS 300 523): "European digital cellular telecommunication system (Phase 2); Numbering, addressing and identification".

[4]   ISO/IEC 7812 (1989): "Identification cards - Numbering system and registration procedure for issuer identifiers".

0.3 Definitions and abbreviations

In addition to the following, abbreviations used in this specification are listed in GSM 01.04.

International Mobile Station Equipment Identity (IMEI)
An "International Mobile Station Equipment Identity" is a unique number which shall be allocated to each individual mobile station equipment in the GSM system and shall be unconditionally implemented by the MS manufacturer.

1 Not used

2 General

As described in specification GSM 02.17, an MS can only be operated if a valid "International Mobile Subscriber Identity" (IMSI) is present. An IMSI is primarily intended for obtaining information on the use of the GSM network by subscribers for individual charging purposes.

Besides the IMSI, the implementation of IMEI is found necessary in order to obtain knowledge about the presence of specific mobile station equipment in the network, disregarding whatever subscribers are making use of these equipments.

The main objective is to be able to take measures against the use of stolen equipment or against equipment of which the use in the GSM system can not or no longer be tolerated for technical reasons.

The IMEI is incorporated in an MS module which is contained within the. The IMEI shall not be changed after the ME's final production process. It shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software).

NOTE: This requirement is valid for new GSM Phase 2 and Release 96, 97, 98 and 99 MEs type approved after 1st June 2002.

This implementation of each individual module should be carried out by the manufacturer who is also responsible for ascertaining that each IMEI is unique and keeping detailed records of produced and delivered MS.

CHANGE REQUEST No :	**A007 r1**	*Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.*

Technical Specification GSM/UMTS 02.16 Version 6.0.0

Submitted to SMG #30
list plenary meeting or STC here ↑

For approval **X**
for information

Without presentation ("non-strategic")
with presentation ("strategic") **X**

PT SMG CR cover form. Filename: crf26_2.doc

Proposed change affects:
(at least one should be marked with an X)

SIM ☐ ME **X** Network ☐   **Workitem:**

Source: ETSI SMG10, GSMA Security Group & GSMA Terminal Working Group   **Date:** 15.12.1999

Subject: Modification of section 2 to enhance IMEI security

Category: *(one category and one release shall be marked with an X)*

			Release:	
F	Correction	**X**	Phase 2	
A	Corresponds to a correction in an earlier release		Release 96	
B	Addition of feature		Release 97	**X**
C	Functional modification of feature		Release 98	
D	Editorial modification		Release 99	
			UMTS	

Reason for change: The security of the IMEI was not sufficiently given by the core specification. Therefore GSM 02.09 was modified. GSM 02.16 needs to be aligned with GSM 02.09. The modification is reflected in this CR.

Clauses affected: Section 2

Other specs affected: *(One or more may be marked with an X)*

Other releases of same spec	**X**	→ List of CRs:
Other core specifications		→ List of CRs:
MS test specifications / TBRs		→ List of CRs:
BSS test specifications		→ List of CRs:
O&M specifications		→ List of CRs:

Other comments:

1 Scope

This Technical Specification (TS) defines the principal purpose and use of International Mobile station Equipment Identities (IMEI).

GSM 03.03 describes the technical manner of numbering, addressing and identification.

1.1 Normative 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.

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

[2]   GSM 02.17: "Digital cellular telecommunications system (Phase 2+); Subscriber Identity Modules (SIM) Functional characteristics".

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

[4]   ISO/IEC 7812 (1989): "Identification cards - Numbering system and registration procedure for issuer identifiers".

1.2 Definitions and abbreviations

In addition to the following, abbreviations used in this specification are listed in GSM 01.04.

International Mobile Station Equipment Identity (IMEI) :An "International Mobile Station Equipment Identity" is a unique number which shall be allocated to each individual mobile station equipment in the GSM system and shall be unconditionally implemented by the MS manufacturer.

2 General

As described in GSM 02.17, an MS can only be operated if a valid "International Mobile Subscriber Identity" (IMSI) is present. An IMSI is primarily intended for obtaining information on the use of the GSM network by subscribers for individual charging purposes.

Besides the IMSI, the implementation of IMEI is found necessary in order to obtain knowledge about the presence of specific mobile station equipment in the network, disregarding whatever subscribers are making use of these equipments.
The main objective is to be able to take measures against the use of stolen equipment or against equipment of which the use in the GSM system can not or no longer be tolerated for technical reasons.

The IMEI is incorporated in an MS module which is contained within the MS equipment. The IMEI shall not be changed after the ME's final production process. It shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software).

> NOTE: This requirement is valid for new GSM Phase 2 and Release 96, 97, 98 and 99 MEs type approved after 1st June 2002.

This implementation of each individual module should be carried out by the manufacturer who is also responsible for ascertaining that each IMEI is unique and keeping detailed records of produced and delivered MS.

ETSI

<table>
<tr><td colspan="3">**CHANGE REQUEST No :**   **A008r1**</td><td>*Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.*</td></tr>
<tr><td colspan="4">**Technical Specification GSM/UMTS** 02.16   Version   7.0.0</td></tr>
<tr><td>Submitted to SMG #30
list plenary meeting or STC here ↑</td><td>For approval   **X**
for information</td><td colspan="2">Without presentation ("non-strategic")
with presentation ("strategic")   **X**</td></tr>
<tr><td colspan="4" align="right">*PT SMG CR cover form. Filename: crf26_2.doc*</td></tr>
</table>

Proposed change affects:
(at least one should be marked with an X)

SIM [ ]   ME [X]   Network [ ]   **Workitem:**

Source: ETSI SMG10, GSMA Security Group & GSMA Terminal Working Group   **Date:**   15.12.1999

Subject: Modification of section 2 to enhance IMEI security

Category:

(one category

and one release

shall be marked

with an X)

				Release:		
F	Correction	**X**			Phase 2	
A	Corresponds to a correction in an earlier release				Release 96	
B	Addition of feature				Release 97	
C	Functional modification of feature				Release 98	**X**
D	Editorial modification				Release 99	
					UMTS	

Reason for change: The security of the IMEI was not sufficiently given by the core specification. Therefore GSM 02.09 was modified. GSM 02.16 needs to be aligned with GSM 02.09. The modification is reflected in this CR.

Clauses affected: Section 2

Other specs affected:

(One or more may

be marked with an X)

Other releases of same spec	**X**	→ List of CRs:	
Other core specifications		→ List of CRs:	
MS test specifications / TBRs		→ List of CRs:	
BSS test specifications		→ List of CRs:	
O&M specifications		→ List of CRs:	

Other comments:

1 Scope

The present document defines the principal purpose and use of International Mobile station Equipment Identities (IMEI).

GSM 03.03 describes the technical manner of numbering, addressing and identification.

1.1 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 1998 document, references to GSM documents are for Release 1998 versions (version 7.x.y).

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

[2]   GSM 02.17: "Digital cellular telecommunications system (Phase 2+); Subscriber Identity Modules (SIM) Functional characteristics".

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

[4]   ISO/IEC 7812 (1989): "Identification cards - Numbering system and registration procedure for issuer identifiers".

1.2 Definitions and abbreviations

In addition to the following, abbreviations used in the present document are listed in GSM 01.04.
International Mobile Station Equipment Identity (IMEI) : An "International Mobile Station Equipment Identity" is a unique number which shall be allocated to each individual mobile station equipment in the GSM system and shall be unconditionally implemented by the MS manufacturer.

2 General

As described in GSM 02.17, an MS can only be operated if a valid "International Mobile Subscriber Identity" (IMSI) is present. An IMSI is primarily intended for obtaining information on the use of the GSM network by subscribers for individual charging purposes.

Besides the IMSI, the implementation of IMEI is found necessary in order to obtain knowledge about the presence of specific mobile station equipment in the network, disregarding whatever subscribers are making use of these equipments.

The main objective is to be able to take measures against the use of stolen equipment or against equipment of which the use in the GSM system can not or no longer be tolerated for technical reasons.
The IMEI is incorporated in an MS module which is contained within the. The IMEI shall not be changed after the ME's final production process. It shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software).

> NOTE: This requirement is valid for new GSM Phase 2 and Release 96, 97, 98 and 99 MEs type approved after 1st June 2002.

This implementation of each individual module should be carried out by the manufacturer who is also responsible for ascertaining that each IMEI is unique and keeping detailed records of produced and delivered MS.

3G CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

22.016 CR

3G specification number ↑

Current Version: **3.0.1**

↑ CR number as allocated by 3G support team

For submission to TSG **SA#6**

list TSG meeting no. here ↑

for approval **X**
for information

(only one box should be marked with an X)

Form: 3G CR cover sheet, version 1.0   The latest version of this form is available from: ftp://ftp.3gpp.org/Information/3GCRF-xx.rtf

---

Proposed change affects:
(at least one should be marked with an X)

USIM ☐   ME **X**   UTRAN ☐   Core Network ☐

Source: ETSI SMG10, GSMA Security Group & GSMA Terminal Working Group   **Date:** 04.06.1999

Subject: Modification of section 2 to enhance IMEI security

3G Work item:

Category:
(only one category shall be marked with an X)

F	Correction	**X**
A	Corresponds to a correction in a 2G specification	
B	Addition of feature	
C	Functional modification of feature	
D	Editorial modification	

Reason for change: The security of the IMEI was not sufficiently given by the core specification. Therefore GSM 02.09 was modified. GSM 02.16 needs to be aligned with GSM 02.09. The modification is reflected in this CR.

Clauses affected: Section 2

Other specs affected:

Other 3G core specifications	☐	→ List of CRs:
Other 2G core specifications	☐	→ List of CRs:
MS test specifications	☐	→ List of CRs:
BSS test specifications	☐	→ List of CRs:
O&M specifications	☐	→ List of CRs:

Other comments:

help.doc

<---------- double-click here for help and instructions on how to create a CR.

ETSI

1 Scope

The present document defines the principal purpose and use of International Mobile station Equipment Identities (IMEI).
TS 23.003 describes the technical manner of numbering, addressing and identification.

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

1.1 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 telecommunication system (Phase 2+); Abbreviations and acronyms"

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

[3]   ISO/IEC 7812 (1989): "Identification cards - Numbering system and registration procedure for issuer identifiers".

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

1.2 Definitions and abbreviations

In addition to the following, abbreviations used in the present document are listed in GSM 01.04 [1] and TR 21.905 [4].

International Mobile Station Equipment Identity (IMEI) : An "International Mobile Station Equipment Identity" is a unique number which shall be allocated to each individual mobile station equipment in the PLMN and shall be unconditionally implemented by the MS manufacturer.

2 General

An MS can only be operated if a valid "International Mobile Subscriber Identity" (IMSI) is present. An IMSI is primarily intended for obtaining information on the use of the PLMN by subscribers for individual charging purposes.

Besides the IMSI, the implementation of IMEI is found necessary in order to obtain knowledge about the presence of specific mobile station equipment in the network, disregarding whatever subscribers are making use of these equipments.

The main objective is to be able to take measures against the use of stolen equipment or against equipment of which the use in the PLMN can not or no longer be tolerated for technical reasons.

The IMEI is incorporated in an MS module which is contained within the MS. The IMEI shall not be changed after the ME's final production process. It shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software).

> NOTE: This requirement is valid for new GSM Phase 2 and Release 96, 97, 98 and 99 MEs type

approved after 1st June 2002. However, this requirement is applicable to all UEs of UMTS from start of production.

This implementation of each individual module should be carried out by the manufacturer who is also responsible for ascertaining that each IMEI is unique and keeping detailed records of produced and delivered MS.

1. 3 Composition of IMEI

The composition of the IMEI shall be such that each individual mobile station equipment can be separately identified.

Information is contained in the IMEI by which the PLMN, after requesting it, can immediately decide whether or not to accept calls made by means of this equipment.

Secondly, the IMEI shall directly or indirectly contain all information which is necessary for the network operator to make relations through its administrative system to trace the equipment to its origin of production. TS 23.003 [2] describes the structure of the IMEI in detail.

The IMEI (14 digits) is complemented by a check digit. The check digit is not part of the digits transmitted at IMEI check occasions, as described below. The Check Digit shall avoid manual transmission errors, e.g. when customers register stolen MEs at the operators customer care desk. The Check Digit is defined according to the Luhn formula, as defined in annex A.

      NOTE: The Check Digit is not applied to the Software Version Number.

4 Use of the equipment identity register

A network operator can make administrative use of the IMEI in the following manner:

Three registers are defined, known as "white lists", "grey lists" and "black lists". The use of such lists is at the operators' discretion.

The **white list** is composed of all **number series** of equipment identities that are permitted for use. The **black list** contains all equipment identities that belong to equipment that need to be barred. Besides the black and white list, administrations have the possibility to use a **grey list**. Equipments on the grey list are not barred (unless on the black list or not on the white list), but are tracked by the network (for evaluation or other purposes).

5 Procedure

It shall be possible to perform the IMEI check at any access attempt, except IMSI detach, and during an established call at any time when a dedicated radio resource is available, in accordance with the security policy of the PLMN operator.

The network shall terminate any access attempt or ongoing call when receiving any of the answers "black-listed" (i.e., on the black list) or "unknown" equipment (i.e., not on the white list) from the EIR. An indication of "illegal ME" shall in these cases be given to the user. Furthermore this is equivalent to an authentication failure hence any call establishment or any location updating is forbidden for the MS, it cannot answer to paging, it is just allowed to perform Emergency Calls. Emergency calls must never be terminated as a result of the IMEI check procedure.

6 Use of IMEI in case of emergency calls

Emergency calls can in some PLMNs be made without having to send the subscriber identity (IMSI) to the network. In this case the misuse of MS equipments after placing invalid emergency calls can be restrained by using the equipment identity.
The network request for the equipment identity is sent to the MS after the emergency call has been set-up. The procedure is the same as for normal call set-up.