3GPP TSG_CN#7 **NP-000179**

ETSI SMG3 Plenary Meeting #7,

Madrid, Spain

13th – 15th March 2000

Agenda item: **5.2.3**

Source: **Mannesmann Mobilfunk**

Title: **CRs to 3G Work Item Security on enhance IMEI security**

Introduction:

This document contains **"5"** CRs on **Work Item Security,** that were revised and now represented to **TSG_N Plenary** meeting #7 for approval.

TDoc	SPEC	CR	REV	CAT	Rel	Old vers	New vers	SUBJECT
NP-000178	03.03	A038	1	C	R98	7.3.1		Modification of section 6.2 to enhance IMEI security
NP-000177	03.03	A039	1	C	R97	6.4.1		Modification of section 6.2 to enhance IMEI security
NP-000176	03.03	A040	1	C	R96	5.2.0		Modification of section 6.2 to enhance IMEI security
NP-000175	03.03	A041	1	C	Ph2	4.9.0		Modification of section 6.2 to enhance IMEI security
NP-000174	23.003	017	2	C	R99	3.3.0		Modification of section 6.2 to enhance IMEI security

3GPP TSG CN#7
Madrid, Spain, 13th –15th Mar. 2000

Document NP-000174
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

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

23.003	**CR**	**017r2~~1~~**	Current Version:	3.3.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: CN#07 *list expected approval meeting # here ↑*

for approval [X] for information [ ]

strategic [ ] non-strategic [X] *(for SMG use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [ ] UTRAN / Radio [ ] Core Network [X]

Source: N2 **Date:** 07.02.00

Subject: Modification of section 6.2 to enhance IMEI security

Work item: Security

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

F	Correction	[ ]
A	Corresponds to a correction in an earlier release	[ ]
B	Addition of feature	[ ]
C	Functional modification of feature	[X]
D	Editorial modification	[ ]

Release:

Phase 2	[ ]
Release 96	[ ]
Release 97	[ ]
Release 98	[ ]
Release 99	[X]
Release 00	[ ]

Reason for change: The security of the IMEI is not sufficiently given by the present specification. Therefore 3G TS 22.016 was modified. 3G TS 23.003 needs to be aligned with 3G TS 22.016. The modification is reflected in this CR.

This CR contains the wording agreed at SMG #30 (Document P-99-776).

Clauses affected: Section 6.2.1 and 6.2.2

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM 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: These changes were also valid for GSM 03.03 R98, R97, R96 and Phase2.
Figures 9, 10 and 11 were not changed

help.doc

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

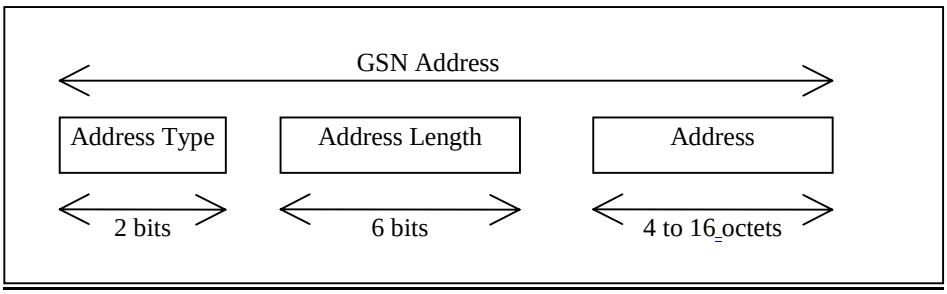

Figure 9: Structure of GSN Address

The GSN Address is composed of the following elements:

1. The Address Type which is a fixed length code (of 2 bits) identifying the type of address that is used in the Address field.
2. Address Length which is a fixed length code (of 6 bits) identifying the length of the Address field.
3. Address is a variable length field with either an IPv4 address or an IPv6 address.

Address Type 0 and Address Length 4 are used when Address is an IPv4 address.

Address Type 1 and Address Length 16 are used when Address is an IPv6 address.

The IP v4 address structure is defined in RFC 791.

The IP v6 address structure is defined in RFC 1883.

5.2 Identification of HLR for HLR restoration application

HLR may also be identified by one or several "HLR id(s)", consisting of the leading digits of the IMSI (MCC + MNC + leading digits of MSIN).

6 International Mobile Station Equipment Identity and Software Version Number

6.1 General

Below the structure and allocation principles of the International Mobile station Equipment Identity and Software Version Number (IMEISV) and the International Mobile station Equipment Identity (IMEI) are defined.

The Mobile Station Equipment is uniquely defined by the IMEI or the IMEISV.

6.2 Composition of IMEI and IMEISV

6.2.1 Composition of IMEI

The International Mobile station Equipment Identity (IMEI) is composed as shown in figure 10.

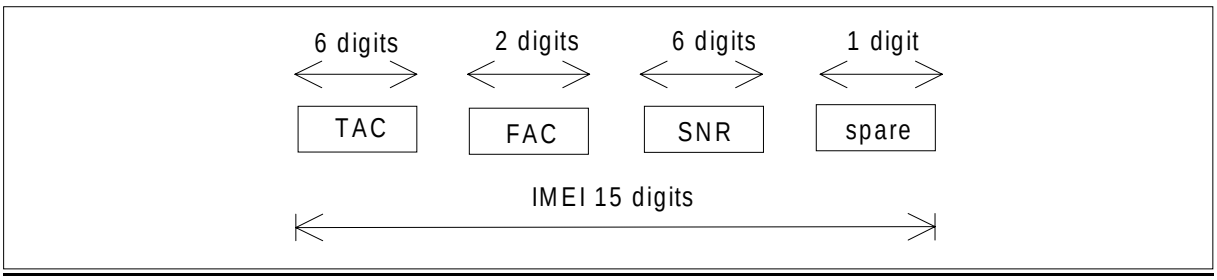

Figure 10: Structure of IMEI

The IMEI is composed of the following elements (each element shall consist of decimal digits only):

- Type Approval Code (TAC). Its length is 6 digits;
- Final Assembly Code (FAC) identifies the place of manufacture/final assembly. Its length is 2 digits;
- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC and FAC. Its length is 6 digits.
- Spare digit: this digit shall be zero, when transmitted by the MS.

The security requirements of the IMEI are defined in 3G TS 22.016

~~The TAC, FAC and SNR shall not be changed after the ME's final production process. These shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software) (see TS GSM 02.16).~~

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

~~In addition, the agreed time after which no equipment is first placed on the market without improved IMEI security functionality as specified is considered as the very latest date. It is understood that typically requirements should be satisfied one year earlier.~~

~~The TAC, FAC and SNR shall be physically protected against unauthorized change (see GSM 02.09).~~

6.2.2 Composition of IMEISV

The International Mobile station Equipment Identity and Software Version Number (IMEISV) is composed as shown in figure 11.

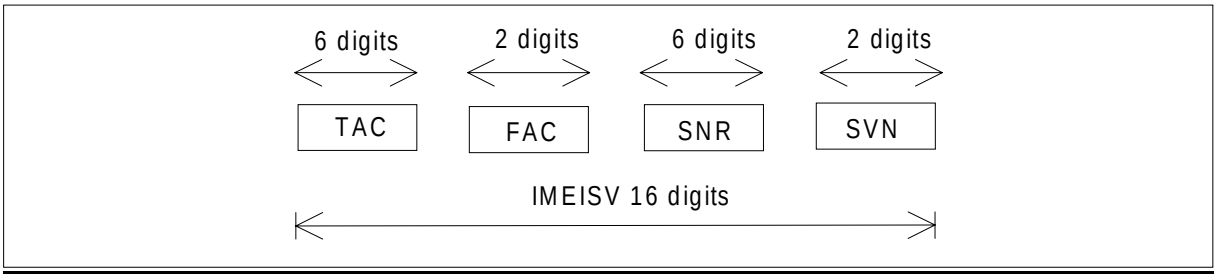

Figure 11: Structure of IMEISV

The IMEISV is composed of the following elements (each element shall consist of decimal digits only):

- Type Approval Code (TAC). Its length is 6 digits;

- Final Assembly Code (FAC) identifies the place of manufacture/final assembly. Its length is 2 digits;
- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC and FAC. Its length is 6 digits.
- Software Version Number (SVN) identifies the software version number of the mobile equipment. Its length is 2 digits.

Regarding updates of the IMEISV: The TAC, FAC and SNR shall ~~not~~ be protected against changed ~~after the ME's final production process. These shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software) (see TS GSM 0.16)the TAC, FAC and SNR shall be physically protected against unauthorized change (see GSM 02.09)~~; i.e. only the SVN part of the IMEISV can be modified.(see 3G TS 22.016)

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

~~In addition, the agreed time after which no equipment is first placed on the market without improved IMEI security functionality as specified is considered as the very latest date. It is understood that typically requirements should be satisfied one year earlier.~~

3GPP TSG CN#7
Madrid , Spain, 13th –15th Mar. 2000

Document *NP-000175*

CHANGE REQUEST

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

03.03	**CR**	**A041r1**	Current Version:	4.9.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	CN#07	for approval	X	strategic		*(for SMG use only)*
list expected approval meeting # here ↑		for information		non-strategic	X	

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME		UTRAN / Radio		Core Network	X

Source:	N2
Date:	07.02.00
Subject:	Modification of section 6.2 to enhance IMEI security
Work item:	Securiry

Category: *(only one category shall be marked with an X)*				**Release:**	
	F	Correction			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	X		Release 98	
	D	Editorial modification			Release 99	
					Release 00	

Reason for change:	The security of the IMEI is not sufficiently given by the present specification. Therefore GSM 02.16 was modified. GSM 03.03 needs to be aligned with GSM 02.16. The modification is reflected in this CR. This CR contains the wording agreed at SMG #30 (Document P-99-776).
Clauses affected:	Section 6.2.1 and 6.2.2

Other specs affected:			
	Other 3G core specifications		→ List of CRs:
	Other GSM 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:	Category C3

4.4 Location Number

A location number is a number which defines a specific location within a GSM PLMN. The Location number is formatted according to CCITT Recommendation E.164, as shown in figure 7. The country code (CC) and national destination code (NDC) fields of the location number are those which define the GSM PLMN of which the location is part.

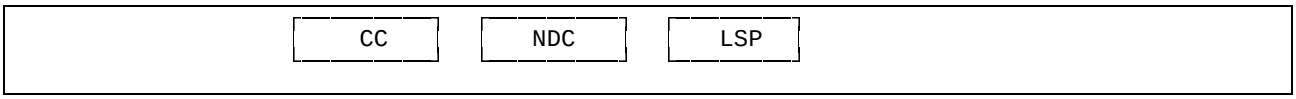

Figure 7: Location Number Structure

The structure of the locally significant part (LSP) of the location number is a matter for agreement between the PLMN operator and the national numbering authority in the PLMN's country. It is desirable that the location number can be interpreted without the need for detailed knowledge of the internal structure of the PLMN; the LSP should therefore include the national destination code in the national numbering plan for the fixed network which defines the geographic area in which the location lies.

The set of location numbers for a GSM PLMN must be chosen so that a location number can be distinguished from the MSISDN of a subscriber of the PLMN. This will allow the PLMN to trap attempts by users to dial a location number.

5 Identification of MSCs and location registers

5.1 Identification for routing purpose

MSCs and location registers are identified by international PSTN/ISDN numbers and/or Signalling Point Codes ("entity number", ie. "HLR number", "VLR number", "MSC number") in each GSM PLMN.

5.2 Identification of HLR for HLR restoration application

HLR may also be identified by one or several "HLR id(s)", consisting of the leading digits of the IMSI (MCC + MNC + leading digits of MSIN).

6 International mobile station equipment identity and software version number

6.1 General

Below the structure and allocation principles of the International Mobile station Equipment Identity and Software Version Number (IMEISV) and the International Mobile Station Equipment Identity (IMEI) are defined.

The Mobile Station Equipment is uniquely defined by the IMEI or the IMEISV.

6.2 Composition of IMEI and IMEISV

6.2.1 Composition of IMEI

The International Mobile station Equipment Identity (IMEI) is composed as shown in figure 8.

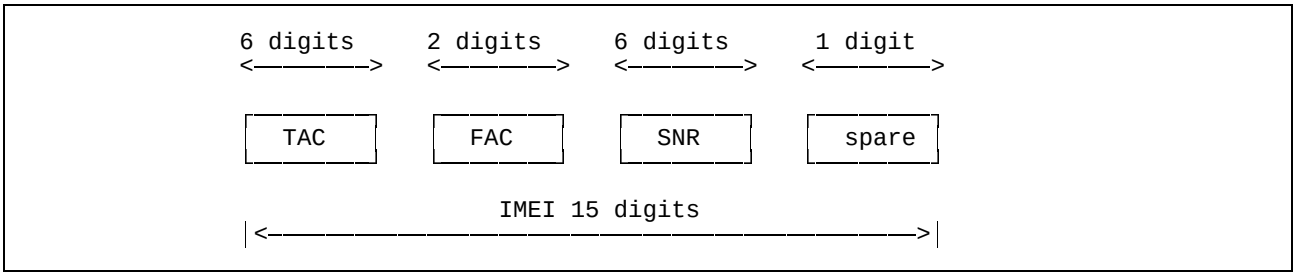

Figure 8: Structure of IMEI

The IMEI is composed of the following elements (each element shall consist of decimal digits only):

- Type Approval Code (TAC). Its length is 6 digits;

- Final Assembly Code (FAC) identifies the place of manufacture/final assembly. Its length is 2 digits;

- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC and FAC. Its length is 6 digits.

- ~~-~~Spare digit: this digit shall be zero, when transmitted by the Mobile Station.

The security requirements of the IMEI are defined in TS GSM 02.16

~~The TAC, FAC and SNR shall not be changed after the ME's final production process. These shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software) (see TS GSM 02.16).~~

~~Note: This requirement is valid for new GSM Phase 2 MEs type approved after 1st June 2002.~~

~~In addition, the agreed time after which no equipment is first placed on the market without improved IMEI security functionality as specified is considered as the very latest date. It is understood that typically requirements should be satisfied one year earlier.~~

~~The TAC, FAC and SNR shall be pysikally protected against unauthorized change (see GSM 02.09).~~

6.2.2 Composition of IMEISV

The International Mobile station Equipment Identity and Software Version Number (IMEISV) is composed as shown in figure 9.

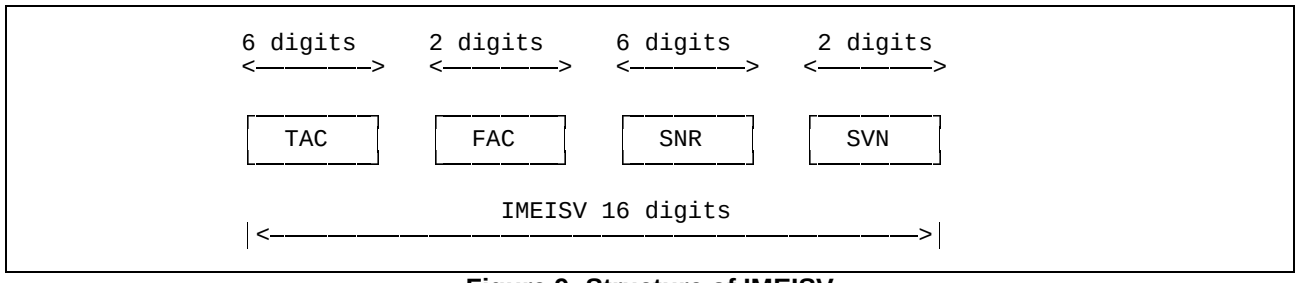

Figure 9: Structure of IMEISV

The IMEISV is composed of the following elements (each element shall consist of decimal digits only):

- Type Approval Code (TAC). Its length is 6 digits;

- Final Assembly Code (FAC) identifies the place of manufacture/final assembly. Its length is 2 digits;

- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC and FAC. Its length is 6 digits.

- Software Version Number (SVN) identifies the software version number of the mobile equipment. Its length is 2 digits.

Regarding updates of the IMEISV: The TAC, FAC and SNR shall be protected against change after the ME's final production process~~. These shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software) (see TS GSM 02.16) the TAC, FAC and SNR shall be physically protected against unauthorized change (see GSM 02.09)~~; i.e. only the SVN part of the IMEISV can be modified.(see TS GSM 02.16)

~~Note: This requirement is valid for new GSM Phase 2 MEs type approved after 1st June 2002.~~

~~In addition, the agreed time after which no equipment is first placed on the market without improved IMEI security functionality as specified is considered as the very latest date. It is understood that typically requirements should be satisfied one year earlier.~~

6.3 Allocation principles

The Type Approval Code (TAC) is issued by a central body.

The place of final assembly (FAC) is encoded by the manufacturer.

Manufacturers shall allocate individual serial numbers (SNR) in a sequential order.

For a given ME, the combination of TAC, FAC and SNR used in the IMEI shall duplicate the combination of TAC, FAC and SNR used in the IMEISV.

The Software Version Number is allocated by the manufacturer after authorisation by the type approval authority. SVN value 99 is reserved for future use.

3GPPTSG CN#7
Madrid, Spain, 13th –15th Mar. 2000

Document *NP-000176*
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

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

03.03	**CR**	**A040r1**	Current Version:	5.2.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	CN#07	for approval	X	strategic		*(for SMG use only)*
list expected approval meeting # here ↑		for information		non-strategic	X	

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)*	(U)SIM		ME		UTRAN / Radio		Core Network	X

Source: Mannesmann Mobilfunk GmbH **Date:** 07.02.00

Subject: Modification of section 6.2 to enhance IMEI security

Work item: Security

Category: *(only one category shall be marked with an X)*				**Release:**	
	F	Correction		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	X	Release 98	
	D	Editorial modification		Release 99	
				Release 00	

Reason for change: The security of the IMEI is not sufficiently given by the present specification. Therefore GSM 02.16 was modified. GSM 03.03 needs to be aligned with GSM 02.16. The modification is reflected in this CR.

This CR contains the wording agreed at SMG #30 (Document P-99-776).

Clauses affected: Section 6.2.1 and 6.2.2

Other specs affected:			
Other 3G core specifications		→ List of CRs:	
Other GSM 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: Category C3

4.4 Location Number

A location number is a number which defines a specific location within a GSM PLMN. The Location number is formatted according to CCITT Recommendation E.164, as shown in figure 7. The country code (CC) and national destination code (NDC) fields of the location number are those which define the GSM PLMN of which the location is part.

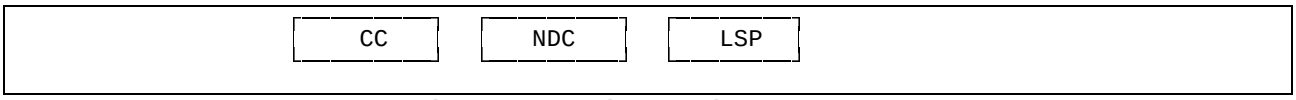

Figure 7: Location Number Structure

The structure of the locally significant part (LSP) of the location number is a matter for agreement between the PLMN operator and the national numbering authority in the PLMN's country. It is desirable that the location number can be interpreted without the need for detailed knowledge of the internal structure of the PLMN; the LSP should therefore include the national destination code in the national numbering plan for the fixed network which defines the geographic area in which the location lies.

The set of location numbers for a GSM PLMN must be chosen so that a location number can be distinguished from the MSISDN of a subscriber of the PLMN. This will allow the PLMN to trap attempts by users to dial a location number.

5 Identification of MSCs and location registers

5.1 Identification for routing purpose

MSCs and location registers are identified by international PSTN/ISDN numbers and/or Signalling Point Codes ("entity number", ie. "HLR number", "VLR number", "MSC number") in each GSM PLMN.

5.2 Identification of HLR for HLR restoration application

HLR may also be identified by one or several "HLR id(s)", consisting of the leading digits of the IMSI (MCC + MNC + leading digits of MSIN).

6 International mobile station equipment identity and software version number

6.1 General

Below the structure and allocation principles of the International Mobile station Equipment Identity and Software Version Number (IMEISV) and the International Mobile Station Equipment Identity (IMEI) are defined.

The Mobile Station Equipment is uniquely defined by the IMEI or the IMEISV.

6.2 Composition of IMEI and IMEISV

6.2.1 Composition of IMEI

The International Mobile station Equipment Identity (IMEI) is composed as shown in figure 8.

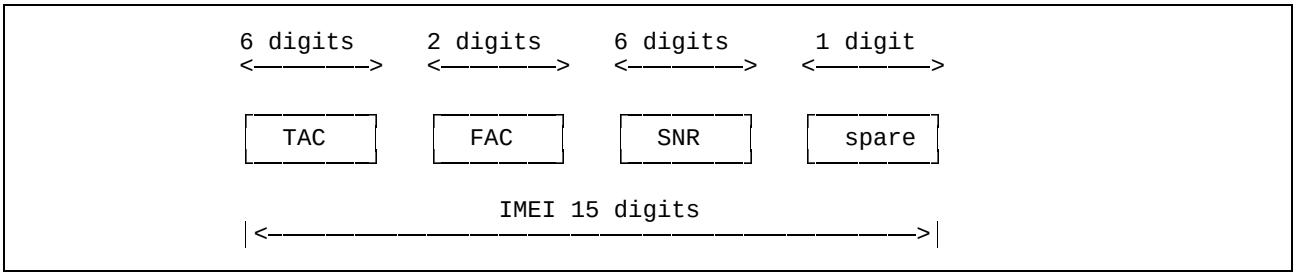

Figure 8: Structure of IMEI

The IMEI is composed of the following elements (each element shall consist of decimal digits only):

- Type Approval Code (TAC). Its length is 6 digits;

- Final Assembly Code (FAC) identifies the place of manufacture/final assembly. Its length is 2 digits;

- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC and FAC. Its length is 6 digits.

- ~~-~~Spare digit: this digit shall be zero, when transmitted by the Mobile Station.

The security requirements of the IMEI are defined in TS GSM 02.16

~~The TAC, FAC and SNR shall not be changed after the ME's final production process. These shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software) (see TS GSM 02.16).~~

~~Note: This requirement is valid for new GSM Phase 2 and Release 96 MEs type approved after 1st June 2002.~~

~~In addition, the agreed time after which no equipment is first placed on the market without improved IMEI security functionality as specified is considered as the very latest date. It is understood that typically requirements should be satisfied one year earlier.~~

~~The TAC, FAC and SNR shall be pysikally protected against unauthorized change (see GSM 02.09).~~

6.2.2 Composition of IMEISV

The International Mobile station Equipment Identity and Software Version Number (IMEISV) is composed as shown in figure 9.

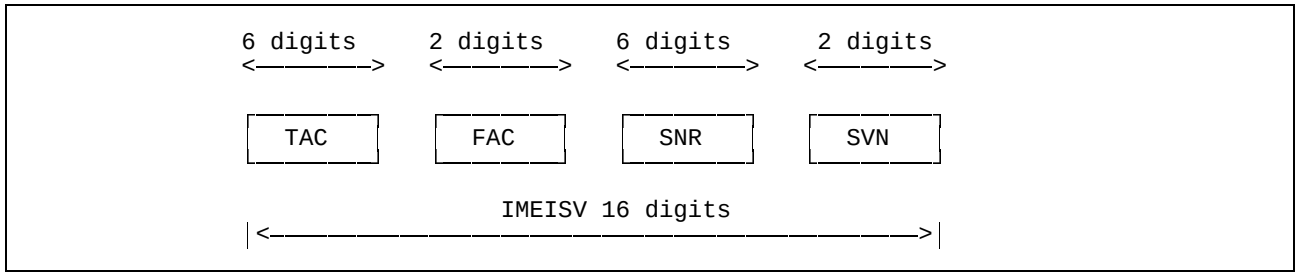

Figure 9: Structure of IMEISV

The IMEISV is composed of the following elements (each element shall consist of decimal digits only):

- Type Approval Code (TAC). Its length is 6 digits;

- Final Assembly Code (FAC) identifies the place of manufacture/final assembly. Its length is 2 digits;

- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC and FAC. Its length is 6 digits.

- Software Version Number (SVN) identifies the software version number of the mobile equipment. Its length is 2 digits.

Regarding updates of the IMEISV: The TAC, FAC and SNR shall be protected against change after the ME's final production process. ~~These shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software) (see TS GSM 02.16) the TAC, FAC and SNR shall be physically protected against unauthorized change (see GSM 02.09)~~; i.e. only the SVN part of the IMEISV can be modified.(see TS GSM 02.16)

~~Note: This requirement is valid for new GSM Phase 2 and Release 96 MEs type approved after 1st June 2002.~~

~~In addition, the agreed time after which no equipment is first placed on the market without improved IMEI security functionality as specified is considered as the very latest date. It is understood that typically requirements should be satisfied one year earlier.~~

6.3 Allocation principles

The Type Approval Code (TAC) is issued by a central body.

The place of final assembly (FAC) is encoded by the manufacturer.

Manufacturers shall allocate individual serial numbers (SNR) in a sequential order.

For a given ME, the combination of TAC, FAC and SNR used in the IMEI shall duplicate the combination of TAC, FAC and SNR used in the IMEISV.

The Software Version Number is allocated by the manufacturer after authorisation by the type approval authority. SVN value 99 is reserved for future use.

3GPP TSG CN#7
Madrid, Spain, 13th –15th Mar. 2000

Document *NP-000177*
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

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

03.03	**CR**	**A039r1**	Current Version:	6.4.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: CN#07 *list expected approval meeting # here ↑*

for approval [X] for information [ ]

strategic [ ] non-strategic [X] *(for SMG use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [ ] UTRAN / Radio [ ] Core Network [X]

Source: N2 **Date:** 07.02.00

Subject: Modification of section 6.2 to enhance IMEI security

Work item: Security

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

F	Correction	[ ]
A	Corresponds to a correction in an earlier release	[ ]
B	Addition of feature	[ ]
C	Functional modification of feature	[X]
D	Editorial modification	[ ]

Release:

Phase 2	[ ]
Release 96	[ ]
Release 97	[X]
Release 98	[ ]
Release 99	[ ]
Release 00	[ ]

Reason for change: The security of the IMEI is not sufficiently given by the present specification. Therefore GSM 02.16 was modified. GSM 03.03 needs to be aligned with GSM 02.16. The modification is reflected in this CR.

This CR contains the wording agreed at SMG #30 (Document P-99-776).

Clauses affected: Section 6.2.1 and 6.2.2

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM 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: Category C3
Figures 9, 10 and 11 were not changed

help.doc

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

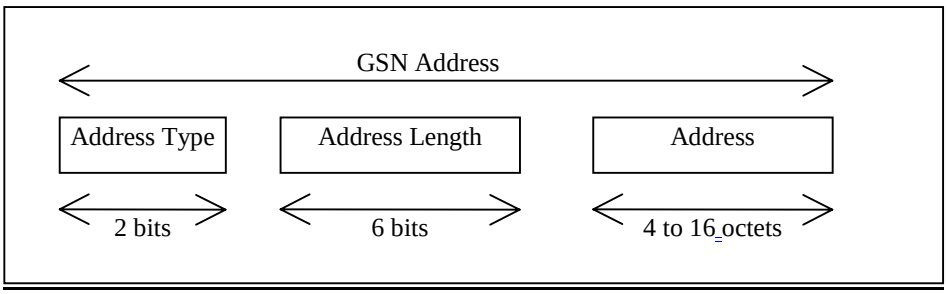

Figure 9: Structure of GSN Address

The GSN Address is composed of the following elements:

1. The Address Type which is a fixed length code (of 2 bits) identifying the type of address that is used in the Address field.

2. Address Length which is a fixed length code (of 6 bits) identifying the length of the Address field.

3. Address is a variable length field with either an IPv4 address or an IPv6 address.

Address Type 0 and Address Length 4 are used when Address is an IPv4 address.

Address Type 1 and Address Length 16 are used when Address is an IPv6 address.

The IP v4 address structure is defined in RFC 791.

The IP v6 address structure is defined in RFC 1883.

5.2 Identification of HLR for HLR restoration application

HLR may also be identified by one or several "HLR id(s)", consisting of the leading digits of the IMSI (MCC + MNC + leading digits of MSIN).

6 International Mobile Station Equipment Identity and Software Version Number

6.1 General

Below the structure and allocation principles of the International Mobile station Equipment Identity and Software Version Number (IMEISV) and the International Mobile station Equipment Identity (IMEI) are defined.

The Mobile Station Equipment is uniquely defined by the IMEI or the IMEISV.

6.2 Composition of IMEI and IMEISV

6.2.1 Composition of IMEI

The International Mobile station Equipment Identity (IMEI) is composed as shown in figure 10.

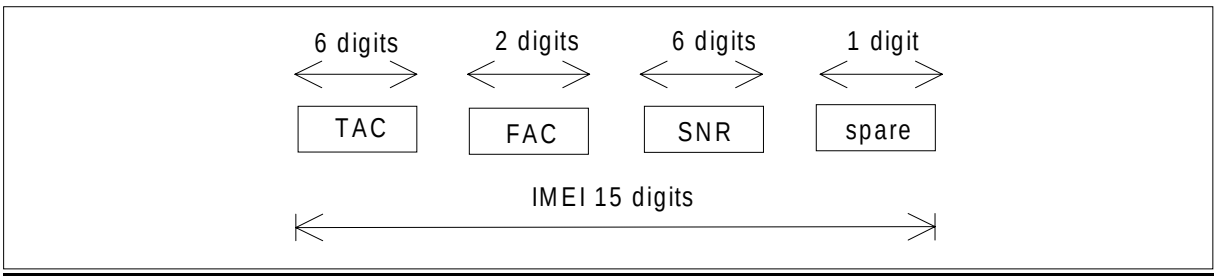

Figure 10: Structure of IMEI

The IMEI is composed of the following elements (each element shall consist of decimal digits only):

- Type Approval Code (TAC). Its length is 6 digits;
- Final Assembly Code (FAC) identifies the place of manufacture/final assembly. Its length is 2 digits;
- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC and FAC. Its length is 6 digits.
- Spare digit: this digit shall be zero, when transmitted by the MS.

The security requirements of the IMEI are defined in TS GSM 02.16

~~The TAC, FAC and SNR shall not be changed after the ME's final production process. These shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software) (see TS GSM 02.16).~~

~~Note: This requirement is valid for new GSM Phase 2 and Release 96 and 97 MEs type approved after 1st June 2002.~~

~~In addition, the agreed time after which no equipment is first placed on the market without improved IMEI security functionality as specified is considered as the very latest date. It is understood that typically requirements should be satisfied one year earlier.~~

~~The TAC, FAC and SNR shall be physically protected against unauthorized change (see GSM 02.09).~~

6.2.2 Composition of IMEISV

The International Mobile station Equipment Identity and Software Version Number (IMEISV) is composed as shown in figure 11.

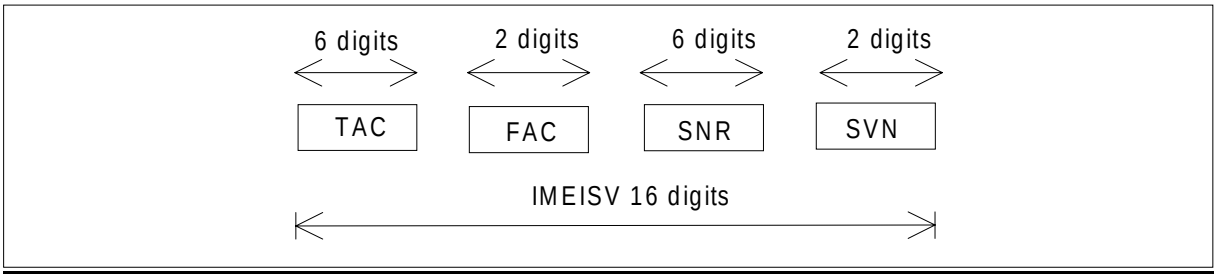

Figure 11: Structure of IMEISV

The IMEISV is composed of the following elements (each element shall consist of decimal digits only):

- Type Approval Code (TAC). Its length is 6 digits;

- Final Assembly Code (FAC) identifies the place of manufacture/final assembly. Its length is 2 digits;
- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC and FAC. Its length is 6 digits.
- Software Version Number (SVN) identifies the software version number of the mobile equipment. Its length is 2 digits.

Regarding updates of the IMEISV: The TAC, FAC and SNR shall ~~not~~ be protected against changed ~~after the ME's final production process. These shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software) (see TS GSM 02.16)the TAC, FAC and SNR shall be physically protected against unauthorized change (see GSM 02.09)~~; i.e. only the SVN part of the IMEISV can be modified.(see TS GSM 02.16)

~~Note: This requirement is valid for new GSM Phase 2 and Release 96 and 97 MEs type approved after 1st June 2002.~~

~~In addition, the agreed time after which no equipment is first placed on the market without improved IMEI security functionality as specified is considered as the very latest date. It is understood that typically requirements should be satisfied one year earlier.~~

3GPPTSG CN#7
Madrid, Spain, 13th - 15th Mar. 2000

Document *NP-000178*
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

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

03.03	**CR**	**A038r1**	Current Version:	7.3.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: CN#07	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑	for information		non-strategic	X	

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: (U)SIM [ ] ME [ ] UTRAN / Radio [ ] Core Network [X]
(at least one should be marked with an X)

Source: N2 **Date:** 07.02.00

Subject: Modification of section 6.2 to enhance IMEI security

Work item: Security

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

F	Correction		**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature	X		Release 98	X
D	Editorial modification			Release 99	
				Release 00	

Reason for change: The security of the IMEI is not sufficiently given by the present specification. Therefore GSM 02.16 was modified. GSM 03.03 needs to be aligned with GSM 02.16. The modification is reflected in this CR.

This CR contains the wording agreed at SMG #30 (Document P-99-776).

Clauses affected: Section 6.2.1 and 6.2.2

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM 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: Category C3
Figures 9, 10 and 11 were not changed

help.doc

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

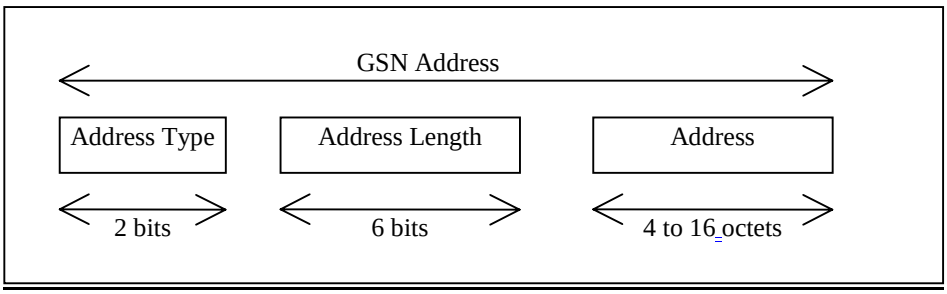

Figure 9: Structure of GSN Address

The GSN Address is composed of the following elements:

1. The Address Type which is a fixed length code (of 2 bits) identifying the type of address that is used in the Address field.

2. Address Length which is a fixed length code (of 6 bits) identifying the length of the Address field.

3. Address is a variable length field with either an IPv4 address or an IPv6 address.

Address Type 0 and Address Length 4 are used when Address is an IPv4 address.

Address Type 1 and Address Length 16 are used when Address is an IPv6 address.

The IP v4 address structure is defined in RFC 791.

The IP v6 address structure is defined in RFC 1883.

5.2 Identification of HLR for HLR restoration application

HLR may also be identified by one or several "HLR id(s)", consisting of the leading digits of the IMSI (MCC + MNC + leading digits of MSIN).

6 International Mobile Station Equipment Identity and Software Version Number

6.1 General

Below the structure and allocation principles of the International Mobile station Equipment Identity and Software Version Number (IMEISV) and the International Mobile station Equipment Identity (IMEI) are defined.

The Mobile Station Equipment is uniquely defined by the IMEI or the IMEISV.

6.2 Composition of IMEI and IMEISV

6.2.1 Composition of IMEI

The International Mobile station Equipment Identity (IMEI) is composed as shown in figure 10.

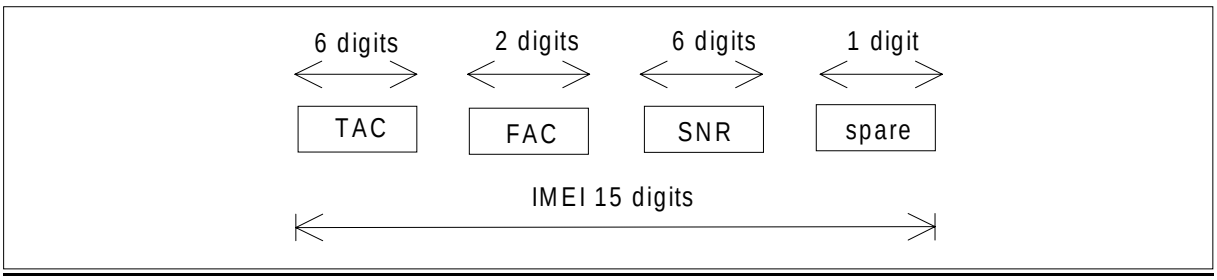

Figure 10: Structure of IMEI

The IMEI is composed of the following elements (each element shall consist of decimal digits only):

- Type Approval Code (TAC). Its length is 6 digits;
- Final Assembly Code (FAC) identifies the place of manufacture/final assembly. Its length is 2 digits;
- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC and FAC. Its length is 6 digits.
- Spare digit: this digit shall be zero, when transmitted by the MS.

The security requirements of the IMEI are defined in TS GSM 02.16.

~~The TAC, FAC and SNR shall not be changed after the ME's final production process. These shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software) (see TS GSM 02.16).~~

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

~~In addition, the agreed time after which no equipment is first placed on the market without improved IMEI security functionality as specified is considered as the very latest date. It is understood that typically requirements should be satisfied one year earlier.~~

~~The TAC, FAC and SNR shall be physically protected against unauthorized change (see GSM 02.09).~~

6.2.2 Composition of IMEISV

The International Mobile station Equipment Identity and Software Version Number (IMEISV) is composed as shown in figure 11.

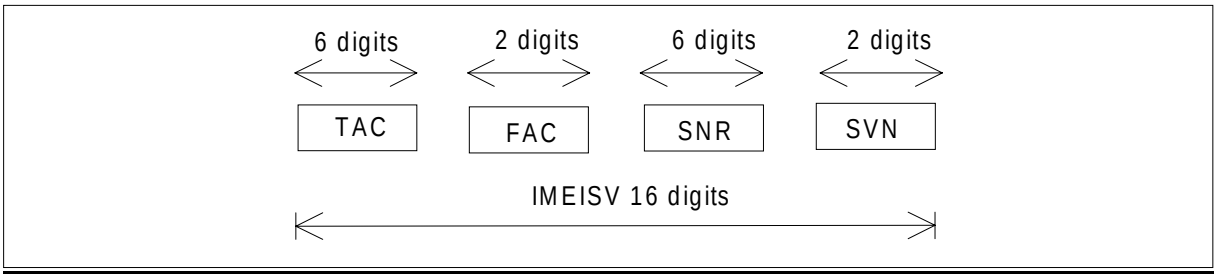

Figure 11: Structure of IMEISV

The IMEISV is composed of the following elements (each element shall consist of decimal digits only):

- Type Approval Code (TAC). Its length is 6 digits;

- Final Assembly Code (FAC) identifies the place of manufacture/final assembly. Its length is 2 digits;
- Serial Number (SNR) is an individual serial number uniquely identifying each equipment within each TAC and FAC. Its length is 6 digits.
- Software Version Number (SVN) identifies the software version number of the mobile equipment. Its length is 2 digits.

Regarding updates of the IMEISV: The TAC, FAC and SNR shall ~~not~~ be protected against changed ~~after the ME's final production process. These shall resist tampering, i.e. manipulation and change, by any means (e.g. physical, electrical and software) (see TS GSM 02.16)the TAC, FAC and SNR shall be physically protected against unauthorized change (see GSM 02.09)~~; i.e. only the SVN part of the IMEISV can be modified.(see TS GSM 02.16)

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

~~In addition, the agreed time after which no equipment is first placed on the market without improved IMEI security functionality as specified is considered as the very latest date. It is understood that typically requirements should be satisfied one year earlier.~~