Technical Specification Group Services and System Aspects
Meeting #8, Dusseldorf, Germany, 26-28 June 2000

TSGS#8(00)271

Source **TSG-SA WG3**

Title **5 Miscellaneous Release 1999 CRs to 33.102, 22.022, 33.103 and 33.105**

S3 Tdoc.	Spec.	Ver.	CR	Rev.	Cat.	Rel.	Subject
S3-000261	22.022	3.0.1	002		D	R99	Update of the ME personalisation to make it applicable to 3GPP
S3-000323	33.102	3.4.0	097	1	D	R99	Align of note and star in figure 18
S3-000323	33.102	3.4.0	103	2	D	R99	Clarification on terminology in user domain
S3-000337	33.103	3.2.0	009		F	R99	SQN length
S3-000342	33.105	3.3.0	11		F	R99	Clarification of BEARER and DIRECTION parameters

3GPP TSG SA WG 3 (Security) meeting #13
Yokohama (Japan), 24—26 May, 2000

Document **S3-000383**
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.

22.022 CR 002 Current Version: 3.0.1

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

For submission to:	SA #8	for approval	☒	strategic	□	*(for SMG*
list expected approval meeting # here ↑		for information	□	non-strategic	□	*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: (U)SIM □ ME □ UTRAN / Radio □ Core Network ☒
(at least one should be marked with an X)

Source: SA WG3 **Date:** 2000-05-19

Subject: Update of the ME personalisation to make it applicable to 3GPP

Work item: Security

Category:	F	Correction	□	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	□		Release 98	□
with an X)	D	Editorial modification	☒		Release 99	☒
					Release 00	□

Reason for change: Update of the specification of ME personalisation to make it applicable for 3GPP

Clauses affected: 4.2.1, 4.3.4, 4.5.2, 4.7.

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:

help.doc

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

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

Technical Specification

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

Reference

DTS/TSGSA-~~0122022U~~0322022U

Keywords

3GPP, SA

3GPP

Postal address

3GPP support office address

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

Internet

http://www.3gpp.org

Copyright Notification

Contents

Foreword

This Technical Specification has been produced by the 3GPP.

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

Version 3.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 Indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

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

1 Scope

The present document provides functional specifications of five features to personalise Mobile Equipment (ME) for GSM and 3G systems. These features are called:

- Network personalisation;
- Network subset personalisation;
- Service Provider (SP) personalisation;
- Corporate personalisation;
- ~~Subscriber Identity Module (SIM)~~SIM/USIM personalisation (SIM for GSM systems or USIM for 3G systems).

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

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

2 References

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

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

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

[2] TS 22.011: "Service accessibility".

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

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

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

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

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

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

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

[10] TS 31.102: “Characteristics of the USIM application”.

[11] TS 31.111: “USIM Application Tool Kit”.

3 Definitions and abbreviations

3.1 Abbreviations

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

CCK	Corporate Control Key
CNL	Co-operative Network List
GID1	Group Identifier (level 1)
GID2	Group Identifier (level 2)
EF	Elementary File
~~IM~~	~~Identity Module (SIM or USIM)~~
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
MCC	Mobile Country Code
ME	Mobile Equipment
MS	GSM Mobile Station (ME + SIM)
MNC	Mobile Network Code
NCK	Network Control Key
NSCK	Network Subset Control Key
PCK	Personalisation Control Key
SIM	Subscriber Identity Module
SMS	Short Message Service
SP	Service Provider
SPCK	Service Provider Control Key
TMSI	Temporary Mobile Subscriber Identity
UE	3G User Equipment (ME + USIM)
USIM	User Services Identity Module

Further GSM abbreviations are given in GSM 01.04 [1].

Further 3G abbreviations are given in TR 21.905 [9].

3.2 Definitions

~~Within this document, the term Identity Module (IM) refers to either a GSM Subscriber Identity module (SIM) or a 3G User Services Identity Module (USIM). When necessary to distinguish between the two systems, the terms SIM and USIM will be used.~~

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

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

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

network personalisation: Allows the network operator to personalise a ME so that it can only be used with that particular network operator's ~~SIMsIMs~~SIM/USIMs.

network subset personalisation: A refinement of network personalisation, which allows network operators to limit the usage of a ME to a subset of ~~SIMsIMs~~SIM/USIMs.

normal mode of operation: Is the mode of operation into which the ME would have gone if it had no personalisation checks to process.

personalisation: Is the process of storing information in the ME and activating the procedures which verify this information against the corresponding information stored in the ~~SIM~~SIM/USIM~~s~~ whenever the ME is powered up or a ~~SIMIM~~SIM/USIM is inserted, in order to limit the ~~SIMsIMs~~SIM/USIMs with which the ME will operate.

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

SP personalisation: Allows the service provider to personalise a ME so that it can only be used with that particular service provider's ~~SIMsIMs~~SIM/USIMs.

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

network code: MCC and MNC.

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

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

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

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

network code group: same as network code

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

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

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

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

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

4 General description

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

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

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

MS goes into normal operation.

Table 1: Codes used by each personalisation category

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

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

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

5 Network personalisation

5.1 Network personalisation

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

The ME is network personalised by storing the code (MCC+MNC) (see TS 2~~2~~3.003 [3]) of the relevant network(s) in the ME and setting a network personalisation indicator in the ME to "on". Whenever ~~an~~a ~~SIM~~SIM/USIM is inserted, or the ME~~S~~ is powered up with ~~an~~a ~~SIM~~SIM/USIM already in place, the International Mobile Subscriber Identity (IMSI) is read from the ~~SIM~~SIM/USIM and the embedded network code (MCC+MNC) checked against that stored in the ME. If the values differ, the MS shall go into emergency calls only mode as defined in annex A.2.

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

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

5.1.1 Operation of network personalised ME

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

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

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

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

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

5.1.2 Network personalisation cycle

5.1.2.1 Personalisation cycle

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

The network personalisation process is as follows:

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

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

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

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

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

5.1.2.2 De-personalisation cycle

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

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

The network de-personalisation process is as follows:

a) the NCK is entered into the ME;

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

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

5.2 Network subset personalisation

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

The ME is network subset personalised by storing the network code and the Network Subset Code (digits 6 and 7 of the IMSI) as an identification of the network subset and setting ~~an~~a network subset personalisation indicator in the ME to "on". Whenever ~~an~~a ~~SIM~~SIM/USIM is inserted, or the MS is powered up with ~~an~~a ~~SIM~~SIM/USIM already in place, the network subset code group is read from the ~~SIM~~SIM/USIM and checked against the stored values in the ME. If no match is found, the ME shall go into emergency calls only mode, as defined in annex A.2.

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

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

5.2.1 Operation of Network subset personalised ME

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

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

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

b) **check network subset code group:** The ME reads the network subset code group from the ~~SIM~~SIM/USIM and checks it against the (list of) stored value(s) on the ME;

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

5.2.2 Network subset personalisation cycle

5.2.2.1 Personalisation Cycle

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

The network subset personalisation process is as follows:

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

- for the case of a single network code group, the ME reads the IMSI from the ~~SIM~~SIM/USIM and extracts the network and network subset codes;
- the ME reads the Co-operative Network List (CNL) from the ~~SIM~~SIM/USIM and extracts the list of network subset code group(s);
- keypad entry;
- a manufacturer defined process.

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

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

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

5.2.2.2 De-personalisation cycle

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

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

The network subset de-personalisation process is as follows:

a) the NSCK is entered into the ME;

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

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

6 SP personalisation

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

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

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

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

6.1 Operation of SP personalised MEs

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

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

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

b) **check whether the ~~SIM~~SIM/USIM supports GID1:** The ME checks that the ~~SIM~~SIM/USIM supports the GID1 file;

c) **check the SP code group:** The ME reads the SP code group from the ~~SIM~~SIM/USIM. and checks it against the (list of) stored value(s) on the ME;

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

6.2 SP personalisation cycle

6.2.1 Personalisation cycle

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

The SP personalisation process is as follows:

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

- the ME checks that the ~~SIM~~SIM/USIM supports the GID1 file, if not the SP personalisation process is aborted with an appropriate error message. The ME reads the SP code group from the ~~SIM~~SIM/USIM. If the SP code is set to the default value (see annex A.1) then the personalisation process shall be aborted with an appropriate error message. Otherwise the SP code group is entered into the ME.
- the ME reads the Co-operative Network List (CNL) from the ~~SIM~~SIM/USIM and extracts the (list of) SP code group(s);
- keypad entry;
- a manufacturer defined process.

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

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

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

6.2.2 De-personalisation cycle

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

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

The SP de-personalisation process is as follows:

a) the SPCK is entered into the ME;

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

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

7 Corporate personalisation

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

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

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

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

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

7.1 Operation of corporate personalised MEs

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

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

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

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

c) **check the corporate code group:** The ME reads the corporate code group from the ~~SIM~~SIM/USIM and checks it against the (list of) stored value(s) on the ME;

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

7.2 Corporate personalisation cycle

7.2.1 Personalisation cycle

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

The corporate personalisation process is as follows:

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

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

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

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

- keypad entry;

- a manufacturer defined process.

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

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

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

7.2.2 De-personalisation cycle

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

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

The corporate de-personalisation process is as follows:

a) the CCK is entered into the ME;

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

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

8 ~~SIM~~SIM/USIM personalisation

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

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

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

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

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

Multiple instances of ~~SIM~~SIM/USIM personalisation can be supported, i.e. whenever ~~an~~a ~~SIM~~SIM/USIM is inserted, or the ME is powered up with ~~an~~a ~~SIM~~SIM/USIM already in place, the IMSI is read from the ~~SIM~~SIM/USIM and checked against a list of ~~SIM~~SIM/USIM code groups stored in the ME.

8.1 Operation of ~~SIM~~SIM/USIM personalised ME

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

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

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

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

c) **~~SIM~~SIM/USIM personalisation check:** The ME checks the read IMSI against the (list of) ~~SIM~~SIM/USIM code group(s) stored in the ME. If no match is found, the ME shall display an appropriate message (e.g. "Insert correct SIM" or “Insert correct USIM”) and shall go into emergency calls only mode as described in annex A.2. Otherwise, the ME goes into the normal mode of operation.

8.2 ~~SIM~~SIM/USIM personalisation cycle

8.2.1 Personalisation cycle

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

The ~~SIM~~SIM/USIM personalisation process is as follows:

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

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

- a manufacturer defined process.

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

c) to personalise the ME to more than one ~~SIM~~SIM/USIM and if the reading of the IMSI from the ~~SIM~~SIM/USIM is used to enter the ~~SIM~~SIM/USIM code group in the ME, the procedures given in a) and b) shall be repeated;

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

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

8.2.2 De-personalisation cycle

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

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

The ~~SIM~~SIM/USIM de-personalisation process is as follows:

a) the user enters the PCK in the ME;

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

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

9 Over the air de-personalisation cycle

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

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

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

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

(i) SMS-PP, ME-specific:

a) A point-to-point SMS message is sent by the network to the MS or UE, the message being marked as being destined for the ME only and for the purposes of ME de-personalisation (see TS 23.040 [6]). The User Data of the SMS contains the de-personalisation key(s) and the IMEI (see annex A.4). If the ME supports the feature, then it shall not display the data on the ME.

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

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

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

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

(ii) SMS-PP~~ SIM~~ Data Download:

a) A SMS message is sent by the network to the ~~S~~IM updating the EF_{DCK} . In the GSM system, it is done by using the SMS-PP SIM Data Download of the SIM Tool Kit (see GSM 11.14 [8]). In the 3G system, it is done by using the SMS-PP Data Download of the USIM Tool Kit (see 3G TS 31.111 [11]).

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

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

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

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

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

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

10 Disable Personalisation

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

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

11 Manufacturer personalisation and de-personalisation

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

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

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

12 Automatic personalisation

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

13 Personalisation Cycle Restrictions

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

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

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

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

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

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

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

14 Security

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

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

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

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

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

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

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

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

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

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

j) ME manufacturers should ensure that the personalisation processes (except for ~~SIM~~SIM/USIM personalisation) are protected against unauthorised, accidental or malicious operation.

Annex A (normative): Technical information

A.1 GID1 and GID2 files

The GID1 and GID2 elementary files on the SIM are specified in GSM 11.11 (ETS 300 977) [7].

The GID1 and GID2 elementary files on the USIM are specified in 3GPP TS 31.102 [10].

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

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

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

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

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

A.2 Emergency calls only mode

The expression "emergency calls only mode" is used in this TS to describe the state the MS (combined ME and SIM) or UE (combined ME and USIM) enters when a personalisation check fails. In this mode, the state of the MS/UE is equivalent to the "limited service state" (see TS 23.022) [4]. Although the personalisation has failed, the ME will be able to access the TMSI and IMSI from the ~~SIM~~SIM/USIM, and therefore any emergency call request shall use these as the MS/UE identity.

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

A.3 Co-operative Network List

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

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

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

A.4 Over-the-air de-personalisation

a) The ME-specific de-personalisation SMS messages sent by the network to de-personalise the ME shall be coded according to TS 23.040 [6] with the TP-UD field coded as follows:

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

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

All characters are coded according to the default alphabet described in TS 23.038 [5].

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

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

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

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

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

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

c) The format for the control keys stored on the SIM is specified in GSM 11.11 [8]. The format for the control keys stored on the USIM is specified in 3G TS 31.102 [10].

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

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

Annex B: Change history

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

History

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

3GPP TSG SA 3 Meeting #13
Yokohama, Japan, 24-26 Mai 2000

Document S3-000323a_r1
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.

33.102	**CR**	**097r1**	Current Version:	3.4.0

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

For submission to:	SA#8	for approval	☒	strategic	□	*(for SMG use only)*
list expected approval meeting # here ↑		for information	□	non-strategic	□	

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 □
(at least one should be marked with an X)

Source:	TSG SA WG3	**Date:**	18 Mai 2000
Subject:	Align of note and star in figure 18		
Work item:	Security		

Category:	F	Correction	□	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	□		Release 98	□
with an X)	D	Editorial modification	☒		Release 99	☒
					Release 00	☒

Reason for change:	Clarification
Clauses affected:	6.8.1.1

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:	

help.doc

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

6.8.1.1 General

For UMTS subscribers, authentication and key agreement will be performed as follows:

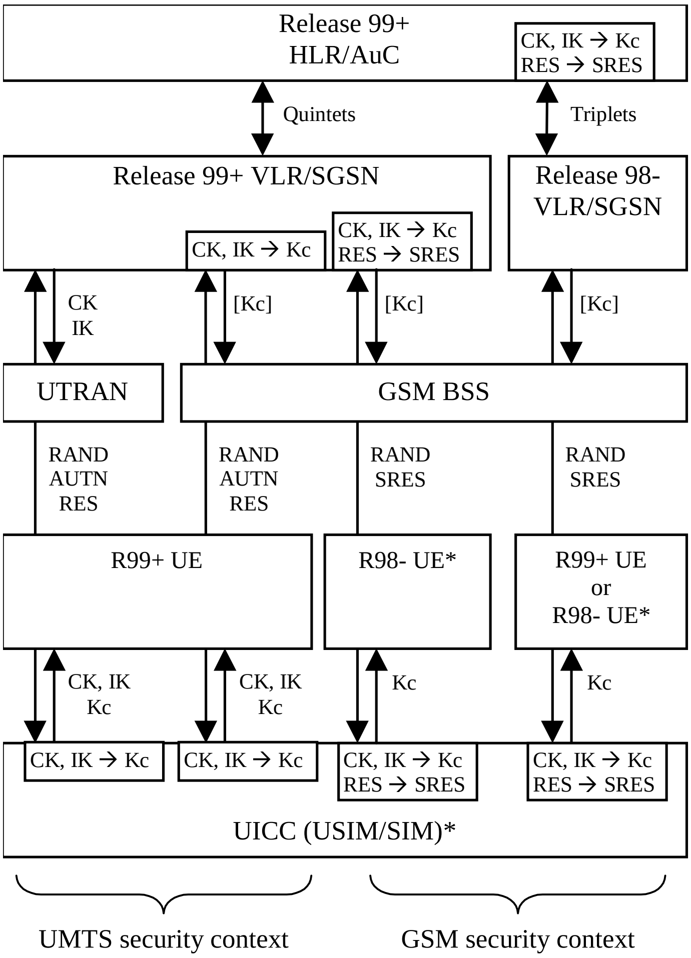
- UMTS AKA shall be applied when the user is attached to a UTRAN.
- UMTS AKA shall be applied when the user is attached to a GSM BSS, in case the user has R99+ UE and also the VLR/SGSN is R99+. In this case, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys CK and IK, by the VLR/SGSN on the network side and by the USIM on the user side.
- GSM AKA shall be applied when the user is attached to a GSM BSS, in case the user has R98- UE. In this case, the GSM user response SRES and the GSM cipher key Kc are derived from the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. A R98- VLR/SGSN uses the stored Kc and RES and a R99+ VLR/SGSN derives the SRES from RES and Kc from CK, IK.

NOTE: To support R98- UE the UICC may contain a GSM SIM application which provides the corresponding GSM functionality for calculating SRES and Kc based on the 3G authentication key K and the 3G authentication algorithm implemented in the USIM. Due to the fact that the 3G authentication algorithm only computes CK/IK and RES, conversion of CK/IK to Kc shall be achieved by using the conversion function c3, and conversion of RES to SRES by c2.

- GSM AKA shall be applied when the user is attached to a GSM BSS, in case the VLR/SGSN is R98-. In this case, the USIM derives the GSM user response SRES and the GSM cipher key Kc from the UMTS user response RES and the UMTS cipher/integrity keys CK, IK.

The execution of the UMTS (resp. GSM) AKA results in the establishment of a UMTS (resp. GSM) security context between the user and the serving network domain to which the VLR/SGSN belongs. The user needs to separately establish a security context with each serving network domain.

Figure 18 shows the different scenarios that can occur with UMTS subscribers using either R98- or R99+ UE in a mixed network architecture.



(See the note above for further explanation on * in figure 18.)

Figure 18: Authentication and key agreement of UMTS subscribers

Note that the UMTS parameters RAND, AUTN and RES are sent transparently through the UTRAN or GSM BSS and that the GSM parameters RAND and SRES are sent transparently through the GSM BSS.

In case of a GSM BSS, ciphering is applied in the GSM BSS for services delivered via the MSC/VLR, and by the SGSN for services delivered via the SGSN. In the latter case the GSM cipher key Kc is not sent to the GSM BSS.

In case of a UTRAN, ciphering and integrity are always applied in the RNC, and the UMTS cipher/integrity keys CK an IK are always sent to the RNC.

TSG SA WG3 #13 **S3-000391**
Yokohama, Japan, 24-26 May 2000

3G CHANGE REQUEST

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

TS 33.102 CR 103r2 Current Version: V3.4.0

3G specification number ↑ *↑ CR number as allocated by 3G support team*

For submission to TSG SA#8 for approval ☒ *(only one box should*
list TSG meeting no. here ↑ for information □ *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: USIM □ ME ☒ UTRAN □ Core Network □
(at least one should be marked with an X)

Source: TSG SA WG3 **Date:** 07-06-00

Subject: Clarification on terminology in user domain

3G Work item: Security

Category:

	F	Correction	□
	A	Corresponds to a correction in a 2G specification	□
(only one category	B	Addition of feature	□
shall be marked	C	Functional modification of feature	□
with an X)	D	Editorial modification	☒

Reason for change:

3GPP-wide the terminology ME is used to refer to the mobile equipment (instead of user equipment/UE).

Clause 6.8.1.5 is changed to clarify that also a USIM may be able to perform GSM AKA, GSM ciphering key derivation, and may support the SIM-ME interface.

Rev. 1 includes the change that the option to support GSM AKA and the option to support GSM cipher key derivation are independent.

Clauses affected: 3.3, 4, 6.4, 6.5, 6.6, 6.8, 7.6

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:

3.3 Abbreviations

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

AK	Anonymity Key
AKA	Authentication and key agreement
AMF	Authentication management field
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
CKSN	Cipher key sequence number
CS	Circuit Switched
EMSI	Encrypted Mobile Subscriber Identity
EMSIN	Encrypted MSIN
$D_{SK(X)}$(data)	Decryption of "data" with Secret Key of X used for signing
$E_{KSXY(i)}$(data)	Encryption of "data" with Symmetric Session Key #i for sending data from X to Y
$E_{PK(X)}$(data)	Encryption of "data" with Public Key of X used for encryption
GI	Group Identifier
GK	Group Key
Hash(data)	The result of applying a collision-resistant one-way hash-function to "data"
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
IV	Initialisation Vector
KAC_X	Key Administration Centre of Network X
KS_{XY}(i)	Symmetric Session Key #i for sending data from X to Y
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAP	Mobile Application Part
MAC	Message Authentication Code
MAC-A	The message authentication code included in AUTN, computed using f1
MS	Mobile Station
MSC	Mobile Services Switching Centre
MSIN	Mobile Station Identity Number
~~MT~~	~~Mobile Termination~~
NE_X	Network Element of Network X
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier
RAND	Random challenge
RND_X	Unpredictable Random Value generated by X
SQN	Sequence number
SQN_{UIC}	Sequence number user for enhanced user identity confidentiality
SQN_{HE}	Sequence number counter maintained in the HLR/AuC
SQN_{MS}	Sequence number counter maintained in the USIM
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
T	Triplet, GSM authentication vector
~~TE~~	~~Terminal Equipment~~
TEMSI	Temporary Encrypted Mobile Subscriber Identity used for paging instead of IMSI
Text1	Optional Data Field
Text2	Optional Data Field
Text3	Public Key algorithm identifier and Public Key Version Number (eventually included in Public Key Certificate)
TMSI	Temporary Mobile Subscriber Identity
TTP	Trusted Third Party
~~UE~~ME	~~User~~ Mobile equipment

UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS IC Card
UIDN	User Identity Decryption Node
USIM	User Services Identity Module
VLR	Visitor Location Register
X	Network Identifier
XEMSI	Extended Encrypted Mobile Subscriber Identity
XRES	Expected Response
Y	Network Identifier

4 Overview of the security architecture

Figure 1 gives an overview of the complete 3G security architecture.

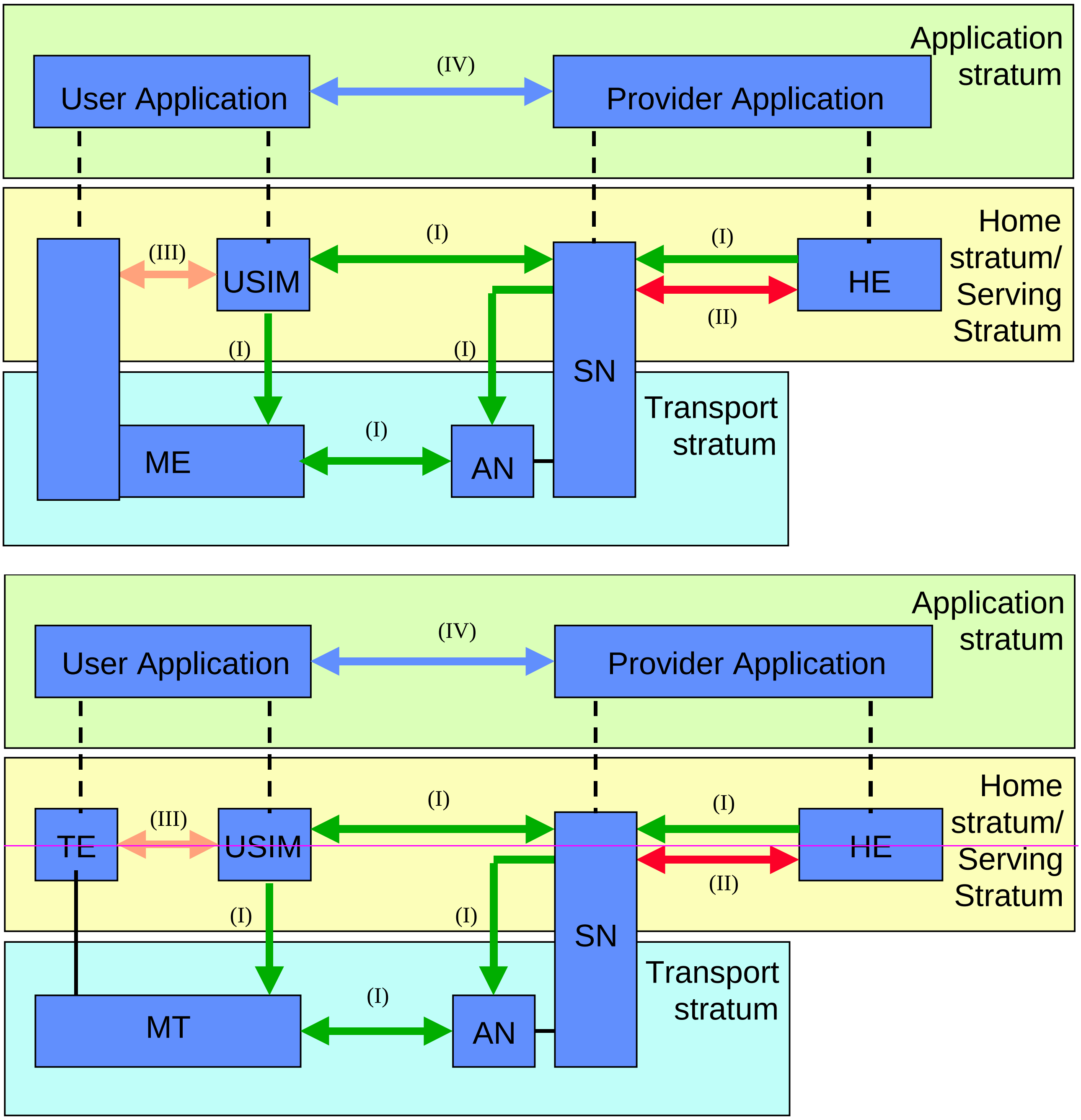


Figure 1: Overview of the security architecture

Five security feature groups are defined. Each of these feature groups meets certain threats, accomplishes certain security objectives:

- **Network access security (I):** the set of security features that provide users with secure access to 3G services, and which in particular protect against attacks on the (radio) access link;
- **Network domain security (II):** the set of security features that enable nodes in the provider domain to securely exchange signalling data, and protect against attacks on the wireline network;
- **User domain security (III):** the set of security features that secure access to mobile stations

- **Application domain security (IV):** the set of security features that enable applications in the user and in the provider domain to securely exchange messages.

- **Visibility and configurability of security (V):** the set of features that enables the user to inform himself whether a security features is in operation or not and whether the use and provision of services should depend on the security feature.

Figure 2 gives an overview of the ~~UE~~ME registration and connection principles within UMTS with a CS service domain and a PS service domain. As in GSM/GPRS, user (temporary) identification, authentication and key agreement will take place independently in each service domain. User plane traffic will be ciphered using the cipher key agreed for the corresponding service domain while control plane data will be ciphered and integrity protected using the cipher and integrity keys from either one of the service domains. In clause 6 the detailed procedures are defined and when not otherwise stated they are used in both service domains.

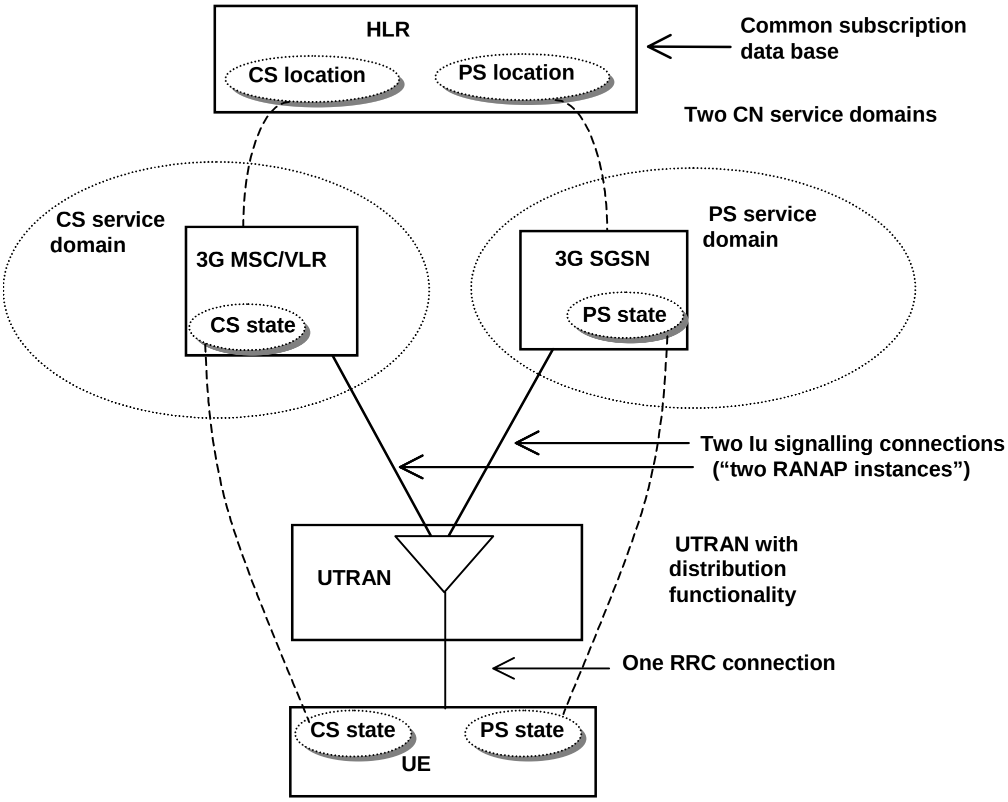


Figure 2: Overview of the ~~UE~~ME registration and connection principles within UMTS for the separate CN architecture case when the CN consists of both a CS service domain with evolved MSC/VLR, 3G_MSC/VLR, as the main serving node and an PS service domain with evolved SGSN/GGSN, 3G_SGSN and 3G GGSN, as the main serving nodes (Extract from TS 23.121 – Figure 4-8)

6.3.3 Authentication and key agreement

The purpose of this procedure is to authenticate the user and establish a new pair of cipher and integrity keys between the VLR/SGSN and the USIM. During the authentication, the USIM verifies the freshness of the authentication vector that is used.

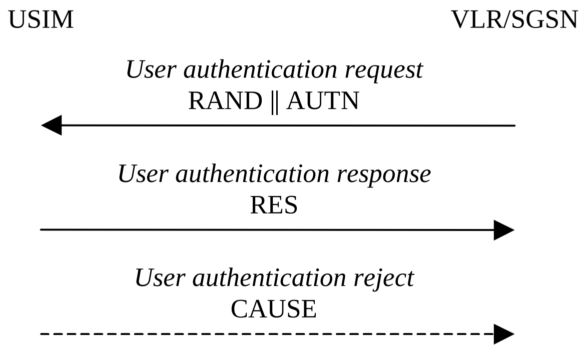

USIM
VLR/SGSN
User authentication request
RAND || AUTN
User authentication response
RES
User authentication reject
CAUSE

Figure 8: Authentication and key establishment

The VLR/SGSN invokes the procedure by selecting the next unused authentication vector from the ordered array of authentication vectors in the VLR/SGSN database. The VLR/SGSN sends to the USIM the random challenge RAND and an authentication token for network authentication AUTN from the selected authentication vector.

Upon receipt the user proceeds as shown in Figure 9.

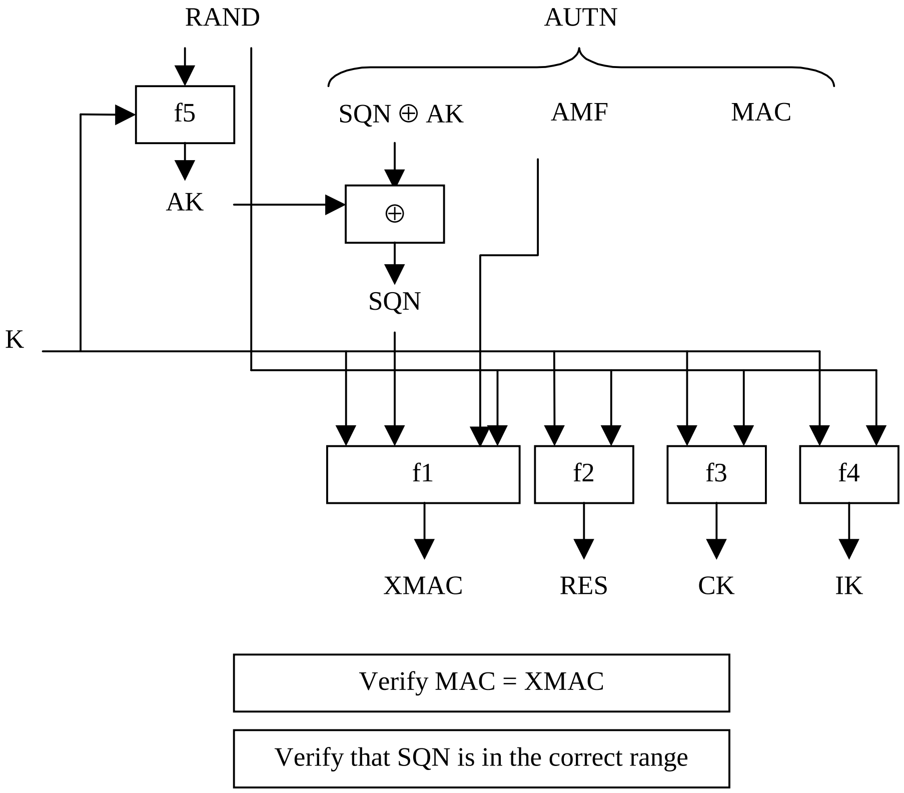


Figure 9: User authentication function in the USIM

Upon receipt of RAND and AUTN the USIM first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ AK.

Next the USIM computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with MAC which is included in AUTN. If they are different, the user sends *user authentication reject* back to the VLR/SGSN with an indication of the cause and the user abandons the procedure. In this case, VLR/SGSN shall initiate an Authentication Failure Report procedure towards the HLR as specified in section 6.3.6. VLR/SGSN may also decide to initiate a new identification and authentication procedure towards the user.

Next the USIM verifies that the received sequence number SQN is in the correct range.

If the USIM considers the sequence number to be not in the correct range, it sends *synchronisation failure* back to the VLR/SGSN including an appropriate parameter, and abandons the procedure.

The synchronisation failure message contains the parameter AUTS. It is AUTS = Conc(SQN_{MS}) || MACS. Conc(SQN_{MS}) = $SQN_{MS} \oplus$ $f5_K$(MACS) is the concealed value of the counter SEQ_{MS} in the MS, and MACS = $f1*_K$(SEQ_{MS} || RAND || AMF) where RAND is the random value received in the current user authentication request. f1* is a message authentication code (MAC) function with the property that no valuable information can be inferred from the function values of f1* about those of f1, ... , f5 and vice versa.

The AMF used to calculate MACS assumes a dummy value of all zeros so that it does not need to be transmitted in the clear in the re-synch message.

The construction of the parameter AUTS in shown in the following Figure 10:

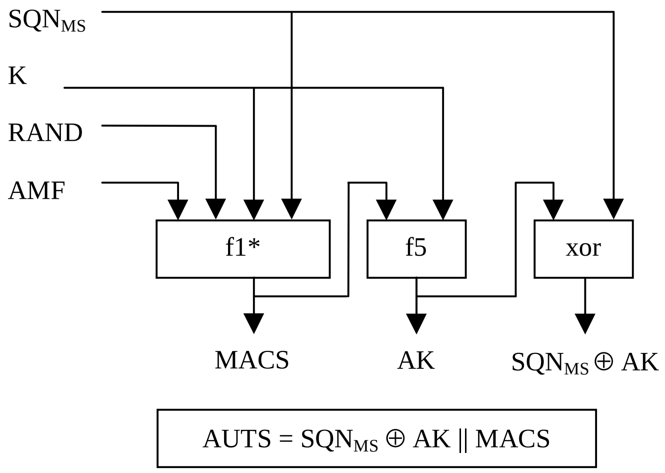


Figure 10: Construction of the parameter AUTS

If the sequence number is considered to be in the correct range however, the USIM computes RES = $f2_K$ (RAND) and includes this parameter in a *user authentication response* back to the VLR/SGSN. Finally the USIM computes the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND). Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND. If the USIM also supports ~~GSM AKA~~ conversion function c3, it shall derive the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK ~~using conversion function c3~~. UMTS keys are sent to the MS along with the derived GSM key for UMTS-GSM interoperability purposes. USIM shall store original CK, IK until the next successful execution of AKA. The USIM also stores RAND until completion of the current AKA, for re-synchronisation purposes.

Upon receipt of *user authentication response* the VLR/SGSN compares RES with the expected response XRES from the selected authentication vector. If XRES equals RES then the authentication of the user has passed. The VLR/SGSN also selects the appropriate cipher key CK and integrity key IK from the selected authentication vector. If XRES and RES are different, VLR/SGSN shall initiate an Authentication Failure Report procedure towards the HLR as specified in section 6.3.6. VLR/SGSN may also decide to initiate a new identification and authentication procedure towards the user.

Conditions on the use of authentication information by the VLR/SGSN: The VLR/SGSN shall use a UMTS authentication vector (i.e. a quintuplet) only once and, hence, shall send out each user authentication request RAND || AUTN only once no matter whether the authentication attempt was successful or not. A consequence is that UMTS authentication vectors (quintuplets) cannot be reused.

6.4 Local authentication and connection establishment

Local authentication is obtained by integrity protection functionality.

6.4.1 Cipher key and integrity key setting

Authentication and key setting are triggered by the authentication procedure and described in 6.3. Authentication and key setting may be initiated by the network as often as the network operator wishes. Key setting can occur as soon as the identity of the mobile subscriber (i.e. P-TMSI, TMSI or IMSI) is known by the VLR/SGSN. The CK and IK are stored in the VLR/SGSN and transferred to the RNC when needed. The CK and IK for the CS domain are stored on the USIM and updated at the next authentication from this domain. The CK and IK for the PS domain are stored on the USIM and updated at the next authentication from this domain.

If an authentication procedure is performed during a connection (PS or CS mode), the new cipher key CK and integrity key IK shall be taken in use in both the RNC and the ~~UE~~ME as part of the security mode negotiation (see 6.4.5) that follows the authentication procedure.

6.4.2 Ciphering and integrity mode negotiation

When an MS wishes to establish a connection with the network, the MS shall indicate to the network in the MS/USIM Classmark which cipher and integrity algorithms the MS supports. This information itself must be integrity protected. As it is the case that the RNC does not have the integrity key IK when receiving the MS/USIM Classmark this information must be stored in the RNC. The data integrity of the classmark is performed, during the security mode set-up procedure by use of the most recently generated IK (see section 6.4.5).

The network shall compare its integrity protection capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and act according to the following rules:

1) If the MS and the SN have no versions of the UIA algorithm in common, then the connection shall be released.

2) If the MS and the SN have at least one version of the UIA algorithm in common, then the network shall select one of the mutually acceptable versions of the UIA algorithm for use on that connection.

The network shall compare its ciphering capabilities and preferences, and any special requirements of the subscription of the MS, with those indicated by the MS and act according to the following rules:

1) If the MS and the network have no versions of the UEA algorithm in common and the network is not prepared to use an unciphered connection, then the connection shall be released.

2) If the MS and the network have at least one version of the UEA algorithm in common, then the network shall select one of the mutually acceptable versions of the UEA algorithm for use on that connection.

3) If the MS and the network have no versions of the UEA algorithm in common and the user (respectively the user's HE) and the SN are willing to use an unciphered connection, then an unciphered connection shall be used.

Because of the separate mobility management for CS and PS services, one CN domain may, independent of the other CN, establish a connection to one and the same MS. Change of ciphering and integrity mode (algorithms) at establishment of a second MS to CN connection shall not be permitted. The preferences and special requirements for the ciphering and integrity mode setting shall be common for both domains. (e.g. the order of preference of the algorithms).

6.4.3 Cipher key and integrity key lifetime

Authentication and key agreement which generates cipher/integrity keys is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. A mechanism is needed to ensure that a particular cipher/integrity key set is not used for an unlimited period of time, to avoid attacks using compromised keys. The USIM shall therefore contain a mechanism to limit the amount of data that is protected by an access link key set.

Each time an RRC connection is released the highest value of the hyperframe number (the current value of COUNT) of the bearers that were protected in that RRC connection is stored in the USIM. When the next RRC connection is established that value is read from the USIM and incremented by one.

The ~~UE~~ME shall trigger the generation of a new access link key set (a cipher key and an integrity key) if the counter reaches a maximum value set by the operator and stored in the USIM at the next RRC connection request message sent out or during an RRC connection. When this maximum value is reached the cipher key and integrity key stored on USIM shall be deleted.

This mechanism will ensure that a cipher/integrity key set cannot be reused beyond the limit set by the operator.

6.4.4 Cipher key and integrity key identification

The key set identifier (KSI) is a number which is associated with the cipher and integrity keys derived during authentication. The key set identifier is allocated by the network and sent with the authentication request message to the mobile station where it is stored together with the calculated cipher key CK and integrity key IK. KSI in UMTS corresponds to CKSN in GSM. The USIM stores one KSI/CKSN for the PS domain key set and one KSI/CKSN for the CS domain key set.

The purpose of the key set identifier is to make it possible for the network to identify the cipher key CK and integrity key IK which are stored in the mobile station without invoking the authentication procedure. This is used to allow re-use of the cipher key CK and integrity key IK during subsequent connection set-ups.

KSI and CKSN have the same format. The key set identifier is three bits. Seven values are used to identify the key set. A value of '111' is used by the mobile station to indicate that a valid key is not available for use. At deletion of the cipher key and integrity key, the KSI is set to '111'. The value '111' in the other direction from network to mobile station is reserved.

6.4.5 Security mode set-up procedure

This section describes one common procedure for both ciphering and integrity protection set-up. It is mandatory to start integrity protection of signalling messages by use of this procedure at each new signalling connection establishment between MS and MSC/VLR respective SGSN. The three exceptions when it is not mandatory to start integrity protection are:

- If the only purpose with the signalling connection establishment and the only result is periodic location registration, i.e. no change of any registration information.
- If there is no MS-MSC/VLR (or MS–SGSN) signalling after the initial L3 signalling message sent from MS to MSC/VLR (or SGSN), i.e. in the case of deactivation indication sent from the MS followed by connection release.
- If the only MS-MSC/VLR (or MS–SGSN) signalling after the initial L3 signalling message sent from MS to MSC/VLR (or SGSN), and possible user identity request and authentication (see below), is a reject signalling message followed by a connection release.

When the integrity protection shall be started, the only procedures between MS and MSC/VLR respective SGSN that are allowed after the initial connection request (i.e. the initial Layer 3 message sent to MSC/VLR or SGSN) and before the security mode set-up procedure are the following:

- Identification by a permanent identity (i.e. request for IMSI), and
- Authentication and key agreement

The message sequence flow below describes the information transfer at initial connection establishment, possible authentication and start of integrity protection and possible ciphering.

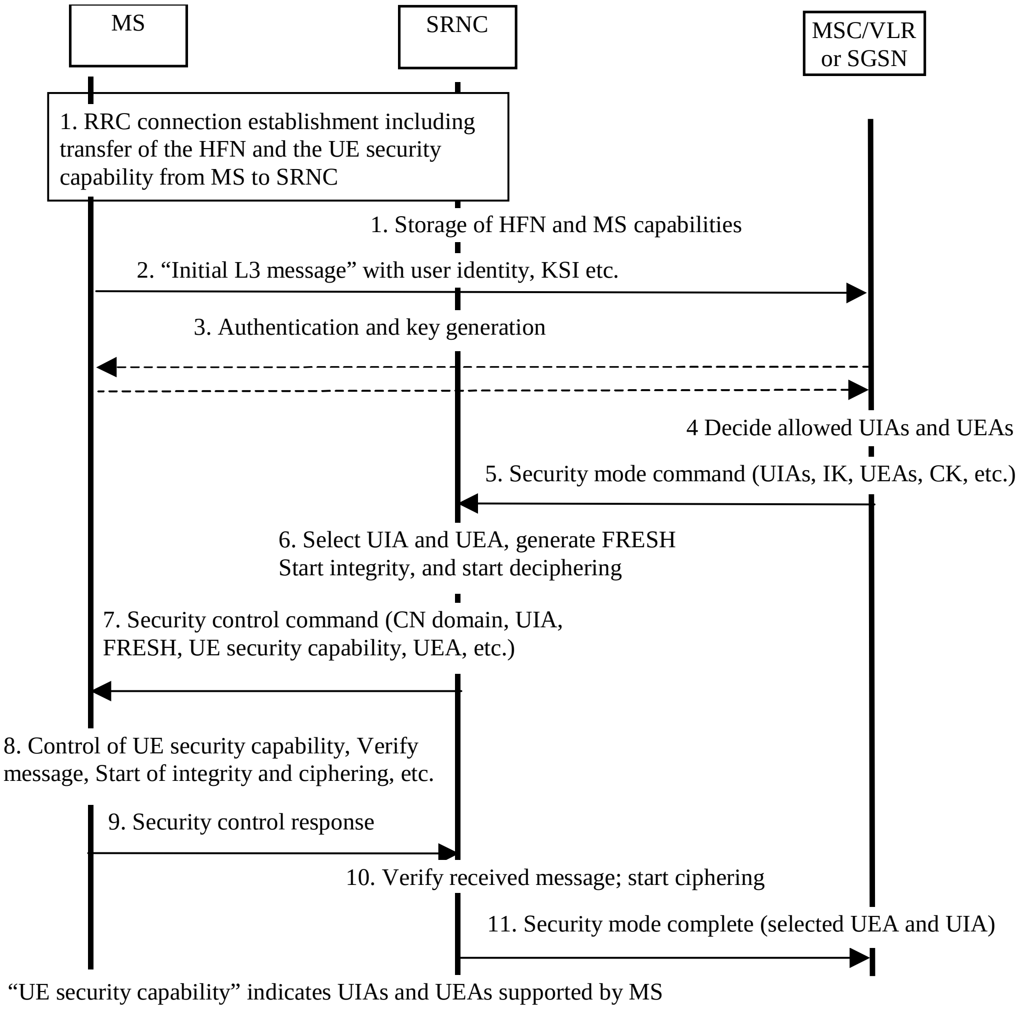

MS
SRNC
MSC/VLR or SGSN
1. RRC connection establishment including transfer of the HFN and the UE security capability from MS to SRNC
1. Storage of HFN and MS capabilities
2. "Initial L3 message" with user identity, KSI etc.
3. Authentication and key generation
4 Decide allowed UIAs and UEAs
5. Security mode command (UIAs, IK, UEAs, CK, etc.)
6. Select UIA and UEA, generate FRESH Start integrity, and start deciphering
7. Security control command (CN domain, UIA, FRESH, UE security capability, UEA, etc.)
8. Control of UE security capability, Verify message, Start of integrity and ciphering, etc.
9. Security control response
10. Verify received message; start ciphering
11. Security mode complete (selected UEA and UIA)
"UE security capability" indicates UIAs and UEAs supported by MS

Figure 14: Local authentication and connection set-up

NOTE 1: The network must have the "~~UE~~ME security capability" information before the integrity protection can start, i.e. the "~~UE~~ME security capability" must be sent to the network in an unprotected message. Returning the "~~UE~~ME security capability" later on to the ~~UE~~ME in a protected message will give ~~UE~~ME the possibility to verify that it was the correct "~~UE~~ME security capability" that reached the network. This latter point, as well as the RRC interwork described below, is yet to be agreed in RAN WG2.

Detailed description of the flow above:

1. RRC connection establishment includes the transfer from MS to RNC of the ~~UE~~ME security capabiltiy and the hyperframe number to be used as part of one of the input parameters for the integrity algorithm and for the ciphering algorithm. The COUNT-I parameter (together with COUNT which is used for ciphering) is stored in the SRNC.

2. The MS sends the Initial L3 message (Location update request, CM service request, Routing area update request, attach request, paging response etc.) to the relevant CN domain. This message contains relevant MM information e.g. KSI. The KSI (Key Set Identifier) is the number allocated by the CN at the last authentication for this CN domain.

3. Authentication of the user and generation of new security keys (IK and CK) may be performed. A new KSI will then also be allocated.

4. The CN node determines which UIAs and UEAs that are allowed to be used.

5. The CN initiates integrity (and possible also ciphering) by sending the RANAP message Security Mode Command to SRNC. This message contains a list of allowed UIAs and the IK to be used. It may also contain the allowed UEAs and the CK to be used.

6. The SRNC decides which algorithms to use by selecting from the list of allowed algorithms, the first UEA and the first UIA it supports. The SRNC generates a random value FRESH and initiates the downlink integrity protection. If SRNC supports no UIA algorithms in the list, it sends a SECURITY MODE REJECT message to CN.

7. The SRNC generates the RRC message Security control command. The message includes the ~~UE~~ME security capability, the UIA and FRESH to be used and possibly also the UEA to be used. Additional information (start of ciphering) may also be included. Since we have two CNs with an IK each, the network must indicate which IK to use. This is obtained by including a CN type indicator information in "Security control command". Before sending this message to the MS, the SRNC generates the MAC-I (Message Authentication Code for Integrity) and attaches this information to the message.

8. At reception of the Security control command message, the MS controls that the ~~UE~~ME security capability received is equal to the ~~UE~~ME security capability sent in the initial message. The MS computes XMAC-I on the message received by using the indicated UIA, the stored COUNT-I and the received FRESH parameter. The MS verifies the integrity of the message by comparing the received MAC-I with the generated XMAC-I.

9. If all controls are successful, the MS compiles the RRC message Security control command response and generates the MAC-I for this message. If any control is not successful, a SECURITY CONTROL REJECT message is sent from the MS.

10. At reception of the response message, the SRNC computes the XMAC-I on the message. The SRNC verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I.

11. The transfer of the RANAP message Security Mode Complete response, including the selected algorithms, from SRNC to the CN node ends the procedure.

The Security mode command to MS starts the downlink integrity protection, i.e. also all following downlink messages sent to the MS are integrity protected and possibly ciphered. The Security mode command response from MS starts the uplink integrity protection and possible ciphering, i.e. also all following messages sent from the MS are integrity protected and possibly ciphered.

6.4.6 Signalling procedures in the case of an unsuccessful integrity check

The supervision of failed integrity checks shall be performed both in the MS and the SRNC. In case of failed integrity check (i.e. faulty or missing MAC) is detected after that the integrity protection is started the concerned message shall be discarded. This can happen on the RNC side or on the MS side.

6.4.7 Signalling procedure for periodic local authentication

The following procedure is used by the RNC to periodically perform a local authentication. At the same time, the amount of data sent during the RRC connection is periodically checked by the RNC and the ~~UE~~ME. The RNC is monitoring the COUNT value associated to each radio bearer. The procedure is triggered whenever any of these values reaches a critical checking value. The granularity of these checking values and the values themselves are defined by the visited network. All messages in the procedure are integrity protected.

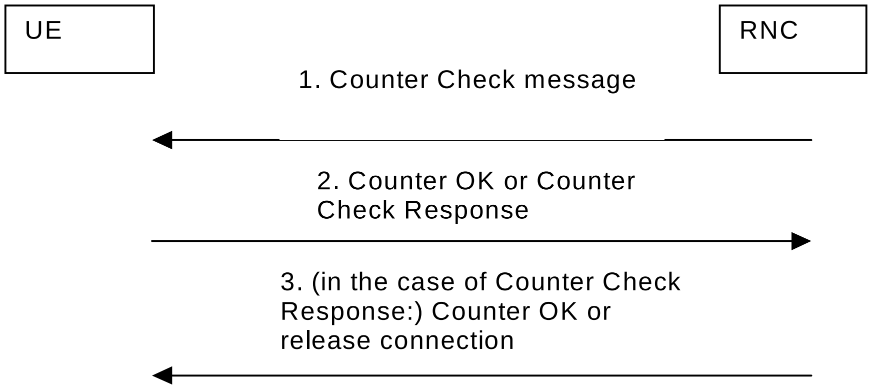

UE
RNC
1. Counter Check message
2. Counter OK or Counter Check Response
3. (in the case of Counter Check Response:) Counter OK or release connection

Figure 15a: RNC periodic local authentication procedure

1. When a checking value is reached (e.g. the value in some fixed bit position in the hyperframe number is changed), a Counter Check message is sent by the RNC. The Counter Check message contains the most significant parts of the counter values (which reflect amount of data sent and received) from each active radio bearer.

2. The counter values in the Counter Check message are checked by ~~UE~~ME and if they agree with the current status in the ~~UE~~ME, a 'Counter OK' message is returned to the RNC. If there is a difference between the counter values in the ~~UE~~ME and the values indicated in the Counter Check message, the ~~UE~~ME sends a Counter Check response to the RNC. The form of this message is similar to the Counter Check message.

3. In case the RNC receives the 'Counter OK' message the procedure is completed. In case the RNC receives the Counter Check response it compares the counter values indicated in it to counter values in the RNC. If there is no difference or if the difference is acceptable then the RNC completes the procedure by sending the 'Counter OK' message. Otherwise, the connection is released.

6.5 Access link data integrity

6.5.1 General

Most control signalling information elements that are sent between the MS and the network are considered sensitive and must be integrity protected. A message authentication function shall be applied on these signalling information elements transmitted between the ~~UE~~ME and the RNC.

After the RRC connection establishment and execution of the security mode set-up procedure, all dedicated MS <–> network control signalling messages (e.g. RRC, MM, CC, GMM, and SM messages) shall be integrity protected. The Mobility Management layer in the MS supervises that the integrity protection is started (see section 6.4.5).

All signalling messages except the following ones shall then be integrity protected:

- Paging Type 1
- RRC Connection Request
- RRC Connection Setup
- RRC Connection Setup Complete
- RRC Connection Reject
- System Information (broadcasted information).

6.5.2 Layer of integrity protection

The UIA shall be implemented in the ~~UE~~ME and in the RNC.

Integrity protection shall be apply at the RRC layer.

6.5.3 Data integrity protection method

Figure 16 illustrates the use of the integrity algorithm f9 to authenticate the data integrity of a signalling message.

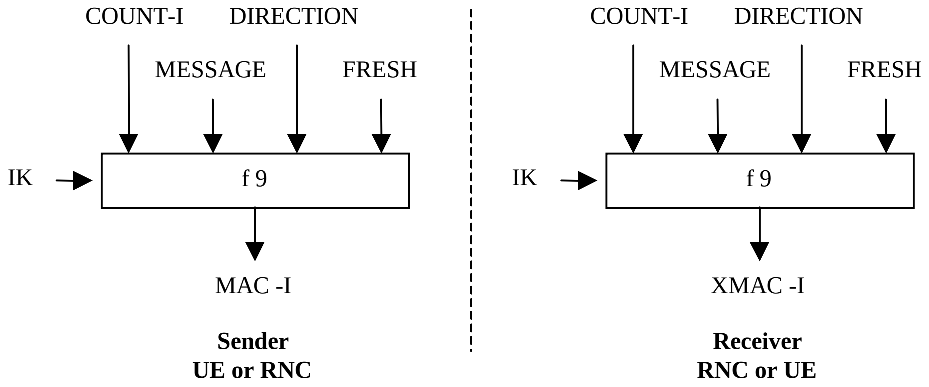


Figure 16: Derivation of MAC-I (or XMAC-I) on a signalling message

The input parameters to the algorithm are the Integrity Key (IK), the integrity sequence number (COUNT-I), a random value generated by the network side (FRESH), the direction bit DIRECTION and the signalling data MESSAGE. Based on these input parameters the user computes message authentication code for data integrity MAC-I using the integrity algorithm f9. The MAC-I is then appended to the message when sent over the radio access link. The receiver computes XMAC-I on the message received in the same way as the sender computed MAC-I on the message sent and verifies the data integrity of the message by comparing it to the received MAC-I.

6.5.4 Input parameters to the integrity algorithm

6.5.4.1 COUNT-I

The integrity sequence number COUNT-I is 32 bits long.

There is one COUNT-I value per logical signalling channel.

COUNT-I is composed of two parts: a "short" sequence number and a "long" sequence number. The "short" sequence number is the 4-bit RRC sequence number RRC SN that is available in each RRC PDU. The "long" sequence number is the 28-bit RRC hyperframe number RRC HFN which is incremented at each RRC SN cycle.

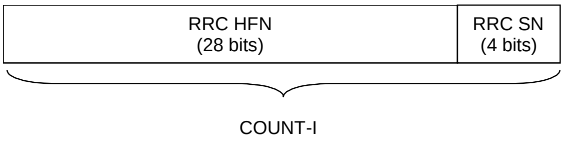


Figure 16a: The structure of COUNT-I

The hyperframe number RRC HFN is initialised by means of the parameter START, which is transmitted from ~~UE~~ME to RNC during *RRC connection establishment*. The ~~UE~~ME and the RNC then initialise the X most significant bits of the RRC HFN to START; the remaining (28-X) LSB of the RRC HFN are initialised to 0. The RRC HFN are incremented independently for each logical channel used for signalling.

Editor's note: The value of X still needs to be added.

Editor's note: The description of how START is managed in the ~~UE~~ME needs to be added.

6.5.4.2 IK

The integrity key IK is 128 bits long.

There may be one IK for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user. Which integrity key to use for a particular connection is described in 6.5.6.

For UMTS subscribers IK is established during UMTS AKA as the output of the integrity key derivation function f4, that is available in the USIM and in the HLR/AuC. For GSM subscribers, that access the UTRAN, IK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 6.8.2.

IK is stored in the USIM and a copy is stored in the ~~UE~~ME. IK is sent from the USIM to the ~~UE~~ME upon request of the ~~UE~~ME. The USIM shall send IK under the condition that 1) a valid IK is available, 2) the current value of START in the USIM is up-to-date and 3) START has not reached THRESHOLD. The ~~UE~~ME shall delete IK from memory after power-off as well as after removal of the USIM.

IK is sent from the HLR/AuC to the VLR or SGSN and stored in the VLR or SGSN as part of a quintet. It is sent from the VLR or SGSN to the RNC in the (RANAP) *security mode command*. The MSC/VLR or SGSN shall assure that the IK is updated at least once every 24 hours.

At handover, the IK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed, and the synchronisation procedure is resumed. The IK remains unchanged at handover.

6.5.4.3 FRESH

The network-side nonce FRESH is 32 bits long.

There is one FRESH parameter value per user. The input parameter FRESH protects the network against replay of signalling messages by the user. At connection set-up the RNC generates a random value FRESH and sends it to the user in the (RRC) *security mode command*. The value FRESH is subsequently used by both the network and the user throughout the duration of a single connection. This mechanism assures the network that the user is not replaying any old MAC-Is.

At handover with relocation of the S-RNC, the new S-RNC generates its own value for the FRESH parameter and sends it in a new *security mode command* to the user.

6.5.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that for the integrity algorithm used to compute the message authentication codes would use an identical set of input parameter values for the up-link and for the down-link messages.

6.5.4.5 MESSAGE

The signalling message itself.

6.5.5 Integrity key selection

There may be one IK for CS connections (IK_{CS}), established between the CS service domain and the user and one IK for PS connections (IK_{PS}) established between the PS service domain and the user.

The data integrity of logical channels for user data is not protected.

Signalling data for services delivered by either of both service domains is sent over common logical (signalling) channels. These logical channels are data integrity protected by the IK of the service domain for which the most recent security mode negotiation took place. This may require that the integrity key of an (already integrity protected) ongoing signalling connection has to be changed, when a new RRC connection is established (with another service domain), or when a security mode negotiation follow a re-authentication during an ongoing connection. This change should be completed within five seconds after the security mode negotiation.

6.5.6 UIA identification

Each UMTS Integrity Algorithm (UIA) will be assigned a 4-bit identifier. Currently, the following values have been defined:

"0001_2" : UIA1, Kasumi.

The remaining values are not defined.

6.6 Access link data confidentiality

6.6.1 General

User data and some signalling information elements are considered sensitive and must be confidentiality protected. To ensure identity confidentiality (see section 6.1), the temporary user indentity (P-)TMSI must be transferred in a protected mode at allocation time and at other times when the signalling procedures permit it.

These needs for a protected mode of transmission are fulfilled by a confidentiality function which is applied on dedicated channels between the ~~UE~~ME and the RNC.

6.6.2 Layer of ciphering

The ciphering function is performed either in the RLC sub-layer or in the MAC sub-layer, according to the following rules:

- If a logical channel is expected to be supported on a common transport channel and has to be ciphered, it shall use UM RLC mode and ciphering is performed at the RLC sub-layer.
- If a logical channel is using a non-transparent RLC mode (AM or UM), ciphering is performed in the RLC sub-layer.
- If a logical channel is using the transparent RLC mode, ciphering is performed in the MAC sub-layer (MAC-d entity).

Ciphering when applied is performed in the S-RNC and the ~~UE~~ME and the context needed for ciphering (CK, HFN, etc.) is only known in S-RNC and the ~~UE~~ME.

6.6.3 Ciphering method

Figure 16b illustrates the use of the ciphering algorithm f8 to encrypt plaintext by applying a keystream using a bit per bit binary addition of the plaintext and the ciphertext. The plaintext may be recovered by generating the same keystream using the same input parameters and applying a bit per bit binary addition with the ciphertext.

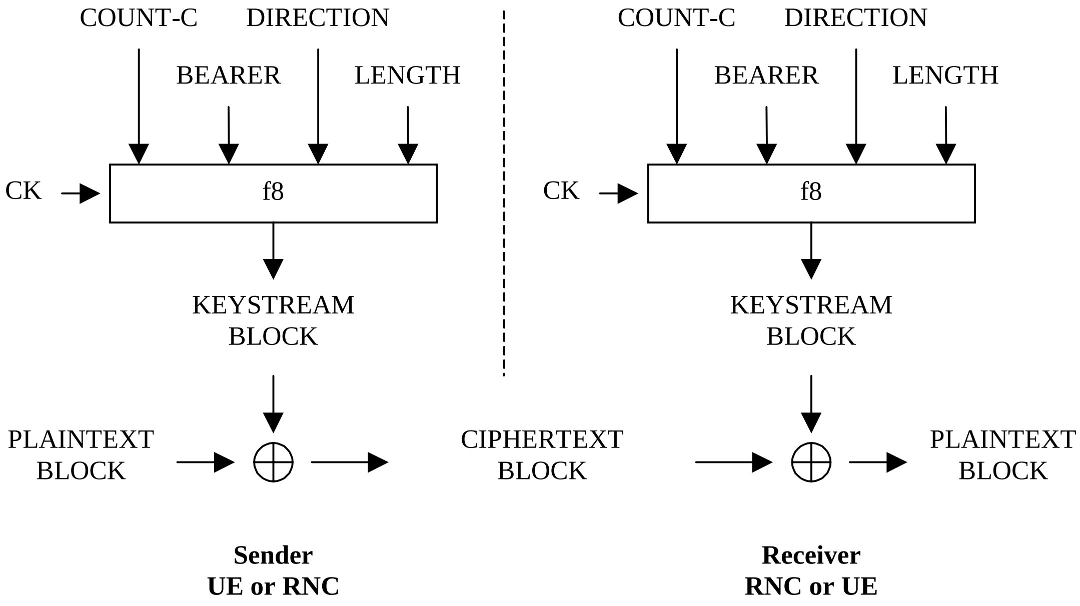


Figure 16b: Ciphering of user and signalling data transmitted over the radio access link

The input parameters to the algorithm are the cipher key CK, a time dependent input COUNT-C, the bearer identity BEARER, the direction of transmission DIRECTION and the length of the keystream required LENGTH. Based on these input parameters the algorithm generates the output keystream block KEYSTREAM which is used to encrypt the input plaintext block PLAINTEXT to produce the output ciphertext block CIPHERTEXT.

The input parameter LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.

6.6.4 Input parameters to the cipher algorithm

6.6.4.1 COUNT-C

The ciphering sequence number COUNT-C is 32 bits long.

There is one COUNT-C value per logical RLC AM channel, one per logical RLC UM channel and one for all logical channels using the transparent RLC mode (and mapped onto DCH).

COUNT-C is composed of two parts: a "short" sequence number and a "long" sequence number. The update of COUNT-C depends on the transmission mode as described below (see figure 16c).

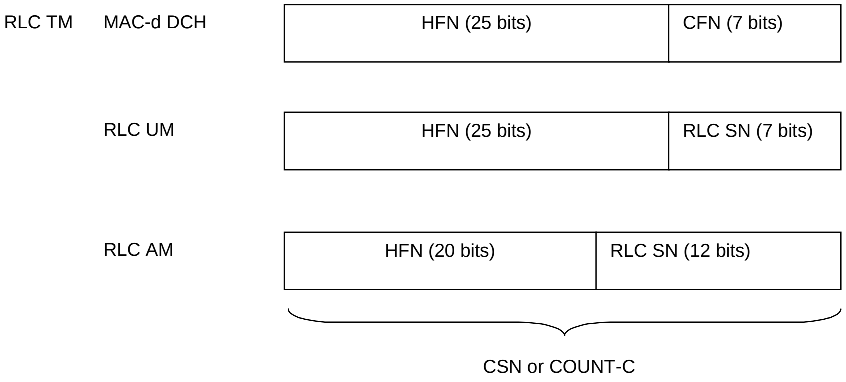


Figure 16c: The structure of COUNT-C for all transmission modes

- For RLC TM on DCH, the "short" sequence number is the 7-bit ciphering frame number CFN of the UEFN. It is independently maintained in the ~~UE~~ME MAC entity and the SRNC MAC-d entity. The "long" sequence number is the 25-bit MAC HFN which is incremented at each CFN cycle. The ciphering sequence number CSN or COUNT-C is identical to the UEFN.

- For RLC UM mode, the "short" sequence number is the 7-bit RLC sequence number RLC SN that is available in each RLC PDU (it is not ciphered). The "long" sequence number is the 25-bit RLC HFN which is incremented at each RLC SN cycle.

- For RLC AM mode, the "short" sequence number is the 12-bit RLC sequence number RLC SN that is available in each RLC PDU (it is not ciphered). The "long" sequence number is the 20-bit RLC HFN which is incremented at each RLC SN cycle.

The hyperframe number HFN is initialised by means of the parameter START, which is transmitted from ~~UE~~ME to RNC in *RRC connection establishment*. The ~~UE~~ME and the RNC then initialise the X most significant bits of the RLC HFN and MAC HFN to START; the remaining LSB of the RLC HFN and MAC HFN are initialised to 0. The RRC HFN are incremented independently for each logical channel.

Editor's note: The value of X still needs to be decided.

Editor's note: The description of how START is managed in the ~~UE~~ME needs to be added.

6.6.4.2 CK

The cipher key CK is 128 bits long.

There may be one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user. Which cipher key to use for a particular logical channel is described in 6.6.6.For UMTS subscribers, CK is established during UMTS AKA, as the output of the cipher key derivation function f3, available in the USIM and in HLR/AuC. For GSM subscribers that access the UTRAN, CK is established following GSM AKA and is derived from the GSM cipher key Kc, as described in 8.2.

CK is stored in the USIM and a copy is stored in the ~~UE~~ME. CK is sent from the USIM to the ~~UE~~ME upon request of the ~~UE~~ME. The USIM shall send CK under the condition that 1) a valid CK is available, 2) the current value of START in the USIM is up-to-date and 3) START has not reached THRESHOLD. The ~~UE~~ME shall delete CK from memory after power-off as well as after removal of the USIM.

CK is sent from the HLR/AuC to the VLR or SGSN and stored in the VLR or SGSN as part of the quintet. It is sent from the VLR or SGSN to the RNC in the (RANAP) security mode command. The VLR or SGSN shall assure that CK is updated at least once every 24 hours.

At handover, the CK is transmitted within the network infrastructure from the old RNC to the new RNC, to enable the communication to proceed. The cipher CK remains unchanged at handover.

6.6.4.3 BEARER

The logical channel identifier BEARER is 4 bits long.

There is one BEARER parameter per logical channel associated with the same user and multiplexed on a single 10ms physical layer frame. The logical channel identifier is input to avoid that for different keystream an identical set of input parameter values is used.

6.6.4.4 DIRECTION

The direction identifier DIRECTION is 1 bit long.

The direction identifier is input to avoid that for the keystreams for the up-link and for the down-link would use the an identical set of input parameter values.

6.6.4.5 LENGTH

The length indicator LENGTH is 16 bits long.

The length indicator determines the length of the required keystream block. LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.

6.6.5 Cipher key selection

There is one CK for CS connections (CK_{CS}), established between the CS service domain and the user and one CK for PS connections (CK_{PS}) established between the PS service domain and the user.

The logical channels for CS user data are ciphered with CK_{CS}.

The logical channels for PS user data are ciphered with CK_{PS}.

Signalling data (for both CS an PS services) is sent over common logical channels. These logical channels are ciphered by the CK of the service domain for which the most recent security mode negotiation took place. This may require that the cipher key of an (already ciphered) ongoing signalling connection is changed, when a new RRC connection establishment occurs, or when a security mode negotiation follows a re-authentication during an ongoing connection. This change should be completed within five seconds after the security mode negotiation.

6.6.6 UEA identification

Each UEA will be assigned a 4-bit identifier. Currently the following values have been defined:

"0000_2"	:	UEA0, no encryption.
"0001_2"	:	UEA1, Kasumi.

The remaining values are not defined.

6.8 Interoperation and handover between UMTS and GSM

6.8.1 Authentication and key agreement of UMTS subscribers

6.8.1.1 General

For UMTS subscribers, authentication and key agreement will be performed as follows:

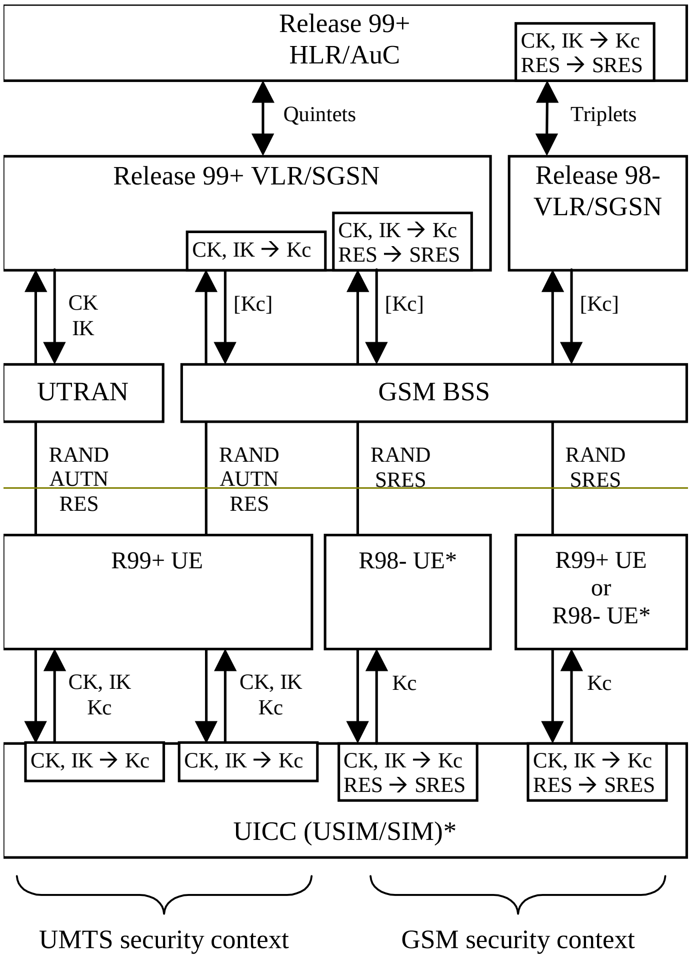
- UMTS AKA shall be applied when the user is attached to a UTRAN.
- UMTS AKA shall be applied when the user is attached to a GSM BSS, in case the user has ~~R99+ UE~~R99+ ME and also the VLR/SGSN is R99+. In this case, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys CK and IK, by the VLR/SGSN on the network side and by the USIM on the user side.
- GSM AKA shall be applied when the user is attached to a GSM BSS, in case the user has ~~R98- UE~~R98- ME. In this case, the GSM user response SRES and the GSM cipher key Kc are derived from the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. A R98- VLR/SGSN uses the stored Kc and RES and a R99+ VLR/SGSN derives the SRES from RES and Kc from CK, IK.

NOTE: To ~~support~~ operate within a ~~R98- UE~~R98- ME the ~~UICC~~ USIM may support the SIM-ME interface as defined in GSM 11.11, and support GSM AKA ~~contain a GSM SIM application~~ which provides the corresponding GSM functionality for calculating SRES and Kc based on the 3G authentication key K and the 3G authentication algorithm implemented in the USIM. Due to the fact that the 3G authentication algorithm only computes CK/IK and RES, conversion of CK/IK to Kc shall be achieved by using the conversion function c3, and conversion of RES to SRES by c2.

- GSM AKA shall be applied when the user is attached to a GSM BSS, in case the VLR/SGSN is R98-. In this case, the USIM derives the GSM user response SRES and the GSM cipher key Kc from the UMTS user response RES and the UMTS cipher/integrity keys CK, IK.

The execution of the UMTS (resp. GSM) AKA results in the establishment of a UMTS (resp. GSM) security context between the user and the serving network domain to which the VLR/SGSN belongs. The user needs to separately establish a security context with each serving network domain.

Figure 18 shows the different scenarios that can occur with UMTS subscribers using either R98- or ~~R99+ UE~~R99+ ME in a mixed network architecture.


Release 99+
HLR/AuC
CK, IK → Kc
RES → SRES
Quintets
Triplets
Release 99+ VLR/SGSN
CK, IK → Kc
CK, IK → Kc
RES → SRES
Release 98-
VLR/SGSN
CK
IK
[Kc]
[Kc]
[Kc]
UTRAN
GSM BSS
RAND
AUTN
RES
RAND
AUTN
RES
RAND
SRES
RAND
SRES
R99+ UE
R98- UE*
R99+ UE
or
R98- UE*
CK, IK
Kc
CK, IK
Kc
Kc
Kc
CK, IK → Kc
CK, IK → Kc
CK, IK → Kc
RES → SRES
CK, IK → Kc
RES → SRES
UICC (USIM/SIM)*
UMTS security context
GSM security context

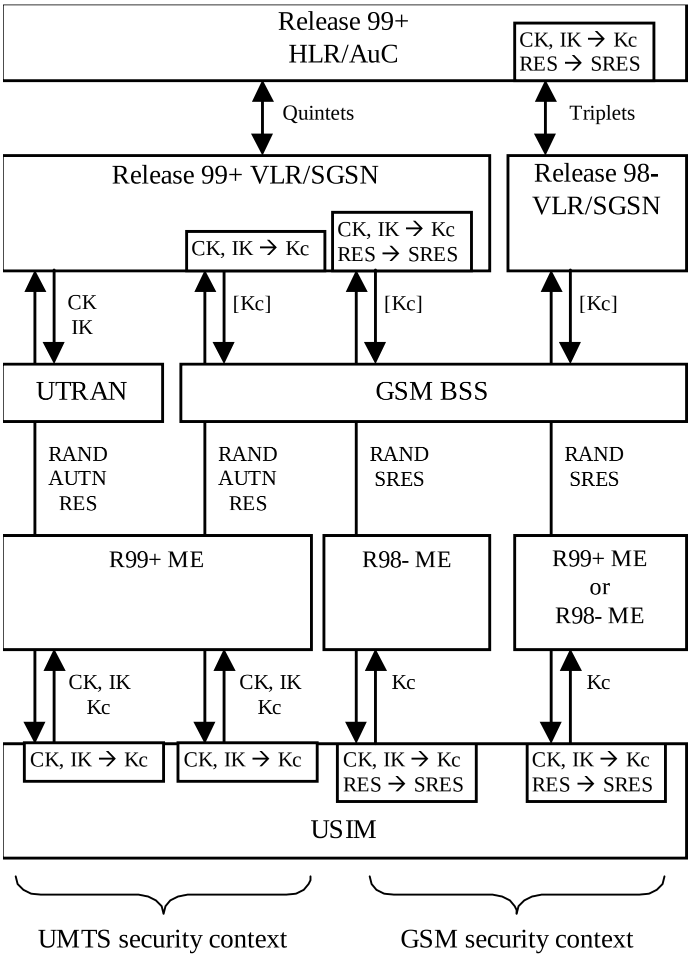


Figure 18: Authentication and key agreement of UMTS subscribers

Note that the UMTS parameters RAND, AUTN and RES are sent transparently through the UTRAN or GSM BSS and that the GSM parameters RAND and SRES are sent transparently through the GSM BSS.

In case of a GSM BSS, ciphering is applied in the GSM BSS for services delivered via the MSC/VLR, and by the SGSN for services delivered via the SGSN. In the latter case the GSM cipher key Kc is not sent to the GSM BSS.

In case of a UTRAN, ciphering and integrity are always applied in the RNC, and the UMTS cipher/integrity keys CK an IK are always sent to the RNC.

6.8.1.2 R99+ HLR/AuC

Upon receipt of an *authentication data request* from a R99+ VLR/SGSN for a UMTS subscriber, a R99+ HLR/AuC shall send quintuplets, generated as specified in 6.3.

Upon receipt of an *authentication data request* from a R98- VLR/SGSN for a UMTS subscriber, a R99+ HLR/AuC shall send triplets, derived from quintuplets using the following conversion functions:

a) c1: $\text{RAND}_{[\text{GSM}]} = \text{RAND}$

b) c2: $\text{SRES}_{[\text{GSM}]} = \text{XRES}_1$ [xor XRES_2 [xor XRES_3 [xor XRES_4]]]

c) c3: $\text{Kc}_{[\text{GSM}]} = \text{CK}_1$ xor CK_2 xor IK_1 xor IK_2

whereby XRES_i are all 32 bit long and XRES = XRES_1 [|| XRES_2 [|| XRES_3 [|| XRES_4]]] dependent on the length of XRES, and CK_i and IK_i are both 64 bits long and CK = CK_1 || CK_2 and IK = IK_1 || IK_2.

6.8.1.3 R99+ VLR/SGSN

The AKA procedure will depend on the terminal capabilities, as follows:

- **UMTS subscriber with ~~R99+ UE~~R99+ ME**

  When the user has ~~R99+ UE~~R99+ ME, UMTS AKA shall be performed using a quintuplet that is either:

  a) retrieved from the local database,

  b) provided by the HLR/AuC, or

  c) provided by the previously visited R99+ VLR/SGSN.

Note: Originally all quintuplets are provided by the HLR/AuC.

UMTS AKA results in the establishment of a UMTS security context; the UMTS cipher/integrity keys CK and IK and the key set identifier KSI are stored in theVLR/SGSN.

When the user is attached to a UTRAN, the UMTS cipher/integrity keys are sent to the RNC, where the cipher/integrity algorithms are allocated.

When the user is attached to a GSM BSS, UMTS AKA is followed by the derivation of the GSM cipher key from the UMTS cipher/integrity keys. When the user receives service from an MSC/VLR, the derived cipher key Kc is then sent to the BSC (and forwarded to the BTS). When the user receives service from an SGSN, the derived cipher key Kc is applied in the SGSN itself.

UMTS authentication and key freshness is always provided to UMTS subscribers with ~~R99+ UE~~R99+ ME independently of the radio access network.

- **UMTS subscriber with ~~R98- UE~~R98- ME**

When the user has ~~R98- UE~~R98- ME, the R99+ VLR/SGSN shall perform GSM AKA using a triplet that is either

a) derived by means of the conversion functions c2 and c3 in the R99+ VLR/SGSN from a quintuplet that is:

   i) retrieved from the local database,

   ii) provided by the HLR/AuC, or

   iii) provided by the previously visited R99+ VLR/SGSN, or

b) provided as a triplet by the previously visited MSC/VLR or SGSN.

NOTE: R99+ VLR/SGSN will always provide quintuplets for UMTS subscribers.

NOTE: For a UMTS subscriber, all triplets are derived from quintuplets, be it in the HLR/AuC or in an VLR/SGSN.

GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the VLR/SGSN.

In this case the user is attached to a GSM BSS. When the user receives service from an MSC/VLR, the GSM cipher key is sent to the BSC (and forwarded to the BTS). When the user receives service from an SGSN, the derived cipher key Kc is applied in the SGSN itself.

UMTS authentication and key freshness cannot be provided to UMTS subscriber with ~~R98- UE~~R98- ME.

6.8.1.4 ~~R99+ UE~~R99+ ME

~~R99+ UE~~R99+ ME with a USIM inserted and attached to a UTRAN shall only participate in UMTS AKA and shall not participate in GSM AKA.

~~R99+ UE~~R99+ ME with a USIM inserted and attached to a GSM BSS shall participate in UMTS AKA and may participate in GSM AKA. Participation in GSM AKA is required to allow registration in a R98- VLR/SGSN.

The execution of UMTS AKA results in the establishment of a UMTS security context; the UMTS cipher/integrity keys CK and IK and the key set identifier KSI are passed to the ~~UE~~ME. If the USIM supports conversion function c3 and/or GSM AKA, the ~~The UE~~ME shall also receive a GSM cipher key Kc derived at the USIM.

The execution of GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the ~~UE~~ME.

6.8.1.5 ~~UICC (~~USIM~~/SIM)~~

The ~~UICC~~ USIM

shall support UMTS AKA ~~(UICC shall contain USIM application)~~ and

may support backwards compatibility with the GSM system, which consists of

Feature 1. GSM cipher key derivation (conversion function c3) to access GSM BSS attached to a R99+ VLR/SGSN using a dual-mode R99+ ME ~~and~~

Feature 2. GSM AKA ~~(UICC may contain a SIM application)~~ to access the GSM BSS attached to a R98- VLR/SGSN or when using R98- ME;

Feature 3. SIM-ME interface [GSM 11.11] to operate within R98- ME.

- ~~. Support of GSM AKA is required to allow access to GSM-BSS with a R98- VLR/SGSN and/or with a R98- UE.~~

When the ~~UE~~ME provides the ~~UICC~~ USIM with RAND and AUTN, UMTS AKA shall be executed. If the verification of AUTN is successful, the ~~UICC~~ USIM shall respond with the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The ~~UICC~~ USIM shall store CK and IK as current security context data. If the USIM supports access to GSM ~~BSS~~cipher key derivation (feature 1), ~~The~~ the ~~UICC~~ USIM shall also derive the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK using conversion function c3 and send the derived Kc to the ~~R99+ UE~~R99+ ME. In case the verification of AUTN is not successful, the ~~UICC~~ USIM shall respond with an appropriate error indication to the ~~R99+ UE~~R99+ ME.

When the ~~UE~~ME provides the ~~UICC~~ USIM with only RAND, and the USIM supports GSM AKA (Feature 2), GSM AKA shall be executed~~, if supported~~. The ~~UICC~~ USIM first computes the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The ~~UICC~~ USIM then derives the GSM user response SRES and the GSM cipher key Kc using the conversion functions c2 and c3. The ~~UICC~~ USIM then stores the GSM cipher key Kc as the current security context and sends the GSM user response SRES and the GSM cipher key Kc to the ~~UE~~ME.

In case the ~~UICC~~ USIM does not support GSM cipher key derivation (Feature 1) or GSM AKA (Feature 2) ~~(conversion function c3 is not available to derive Kc and pass it to the R99+ UER99+ ME)~~, the ~~R99+ UE~~R99+ ME shall be informed. A ~~UICC~~ USIM that does not support GSM cipher key derivation (Feature 1) cannot operate in any GSM BSS. A USIM that does not support GSM AKA (Feature 2) cannot operate under a R98- VLR/SGSN or in a ~~R98- UE~~R98- ME.

6.8.2 Authentication and key agreement for GSM subscribers

6.8.2.1 General

For GSM subscribers, GSM AKA shall always be used.

The execution of the GSM AKA results in the establishment of a GSM security context between the user and the serving network domain to which the VLR/SGSN belongs. The user needs to separately establish a security context with each serving network domain.

When in a UTRAN, the UMTS cipher/integrity keys CK and IK are derived from the GSM cipher key Kc by the ~~UE~~ME and the VLR/SGSN, both R99+ entities.

Figure 19 shows the different scenarios that can occur with GSM subscribers using either R98- or ~~R99+ UE~~R99+ ME in a mixed network architecture.

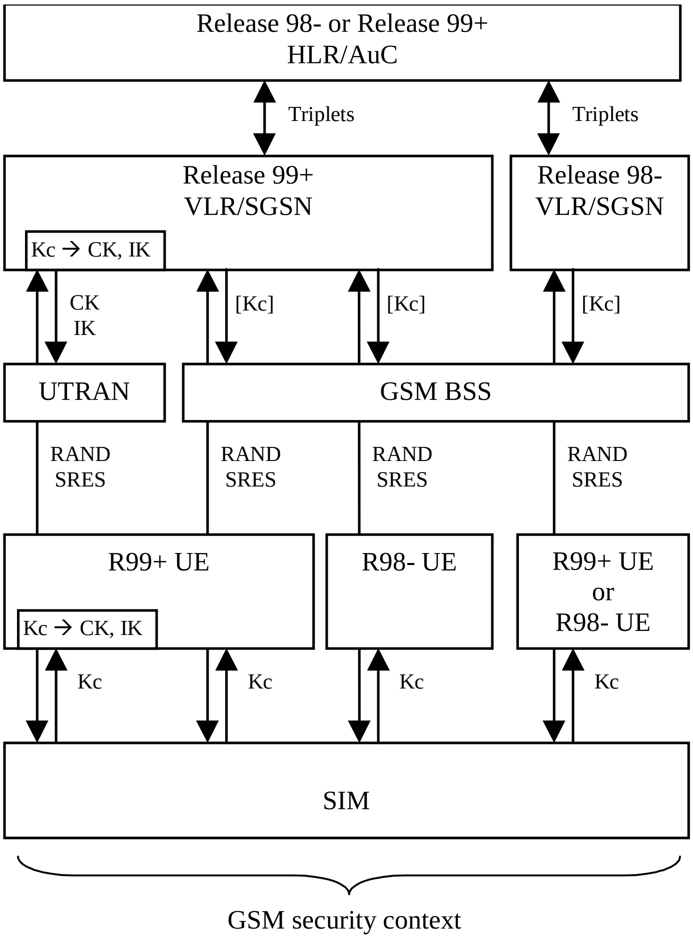


Figure 19: Authentication and key agreement for GSM subscribers

Note that the GSM parameters RAND and RES are sent transparently through the UTRAN or GSM BSS.

In case of a GSM BSS, ciphering is applied in the GSM BSS for services delivered via the MSC/VLR, and by the SGSN for services delivered via the SGSN. In the latter case the GSM cipher key Kc is not sent to the GSM BSS.

In case of a UTRAN, ciphering is always applied in the RNC, and the UMTS cipher/integrity keys CK an IK are always sent to the RNC.

6.8.2.2 R99+ HLR/AuC

Upon receipt of an *authentication data request* for a GSM subscriber, a R99+ HLR/AuC shall send triplets generated as specified in GSM 03.20.

6.8.2.3 VLR/SGSN

The R99+ VLR/SGSN shall perform GSM AKA using a triplet that is either:

a) retrieved from the local database,

b) provided by the HLR/AuC, or

c) provided by the previously visited VLR/SGSN.

NOTE: All triplets are originally provided by the HLR/AuC.

GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the VLR/SGSN.

When the user is attached to a UTRAN, the R99+ VLR/SGSN derives the UMTS cipher/integrity keys from the GSM cipher key using the following conversion functions:

a) c4: $CK_{[UMTS]}$ = 0…0 || Kc;

b) c5: $IK_{[UMTS]}$ = Kc || Kc;

whereby in c4, Kc occupies the 64 least significant bits of CK.

The UMTS cipher/integrity keys are then sent to the RNC where the ciphering and integrity algorithms are allocated.

When the user is attached to a GSM BSS and the user receives service from an MSC/VLR, the cipher key Kc is sent to the BSC (and forwarded to the BTS). When the user receives service from an SGSN, the cipher key Kc is applied in the SGSN itself.

6.8.2.4 ~~R99+ UE~~R99+ ME

~~R99+ UE~~R99+ ME with a SIM inserted, shall participate only in GSM AKA.

GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the ~~UE~~ME.

When the user is attached to a UTRAN, ~~R99+ UE~~R99+ ME shall derive the UMTS cipher/integrity keys CK and IK from the GSM cipher key Kc using the conversion functions c4 and c5.

6.8.3 Distribution and use of authentication data between VLRs/SGSNs

The distribution of authentication data (unused authentication vectors and/or current security context data) between R99+ VLRs/SGSNs of the same service network domain is performed according to chapter 6.3.4. The following four cases are distinguished related to the distribution of authentication data between VLRs/SGSNs (of the same or different releases). Conditions for the distribution of such data and for its use when received at VLRn/SGSNn are indicated for each case:

a) R99+ VLR/SGSN to R99+ VLR/SGSN

UMTS and GSM authentication vectors can be distributed between R99+ VLRs/SGSNs. Note that originally all authentication vectors (quintuplets for UMTS subscribers and triplets for GSM subscribers) are provided by the HLR/AuC.

Current security context data can be distributed between R99+ VLRs/SGSNs. VLRn/SGSNn shall not use current security context data received from VLRo/SGSNo to authenticate the subscriber using local authentication in the following cases:

i) Security context to be established at VLRn/SGSNn requires a different set of keys than the one currently in use at VLRo/SGSNo. This change of security context is caused by a change of ~~UE~~ME release (R'99 ~~UE~~ME ←→ R'98 ~~UE~~ME) when the user registers at VLRn/SGSNn.

ii) Authentication data from VLRo includes Kc+CKSN but no unused AVs and the subscriber has a R'99 ~~UE~~ME (under GSM BSS or UTRAN). In this situation, VLRn have no indication of whether the subscriber is GSM or UMTS and it is not able to decide whether Kc received can be used (in case the subscriber were a GSM subscriber).

In these two cases, received current security context data shall be discarded and a new AKA procedure shall be performed.

b) R98- VLR/SGSN to R98- VLR/SGSN

Only triplets can be distributed between R98- VLRs/SGSNs. Note that originally for GSM subscribers, triplets are generated by HLR/AuC and for UMTS subscribers, they are derived from UMTS authentication vectors by R99+ HLR/AuC. UMTS AKA is not supported and only GSM security context can be established by a R98- VLR/SGSN.

R98- VLRs are not prepared to distribute current security context data.

Since only GSM security context can be established under R98- SGSNs, security context data can be distributed and used between R98- SGSNs.

c) R99+ VLR/SGSN to R98- VLR/SGSN

R99+ VLR/SGSN can distribute to a new R98- VLR/SGSN triplets originally provided by HLR/AuC for GSM subscribers or can derive triplets from stored quintuplets originally provided by R99+ HLR/AuC for UMTS subscribers. Note that R98- VLR/SGSN can only establish GSM security context.

R99+ VLRs shall not distribute current security context data to R98- VLRs.

Since R98- SGSNs are only prepared to handle GSM security context data, R99+ SGSNs shall only distribute GSM security context data (Kc, CKSN) to R98- SGSNs.

d) R98- VLR/SGSN to R99+ VLR/SGSN.

In order to not establish a GSM security context for a UMTS subscriber, triplets provided by a R98- VLR/SGSN can only be used by a R99+ VLR/SGSN to establish a GSM security context under GSM-BSS with a ~~R98- UE~~R98- ME.

In all other cases, R99+ VLR/SGSN shall request fresh AVs (either triplets or quintuplets) to HE. In the event, the R99+ VLR/SGSN receives quintuplets, it shall discard the triplets provided by the R98- VLR/SGSN.

R98- VLRs are not prepared to distribute current security context data.

R98- SGSNs can distribute GSM security context data only. The use of this information at R99+ SGSNn shall be performed according to the conditions stated in a).

6.8.4 Intersystem handover for CS Services – from UTRAN to GSM BSS

If ciphering has been started when an intersystem handover occurs from UTRAN to GSM BSS, the necessary information (e.g. Kc, supported/allowed GSM ciphering algorithms) is transmitted within the system infrastructure before the actual handover is executed to enable the communication to proceed from the old RNC to the new GSM BSS, and to continue the communication in ciphered mode.

6.8.4.1 UMTS security context

A UMTS security context in UTRAN is only established for a UMTS subscriber with a ~~R99+ UE~~R99+ ME. At the network side, three cases are distinguished:

a) In case of a handover to a GSM BSS controlled by the same MSC/VLR, the MSC/VLR derives the GSM cipher key Kc from the stored UMTS cipher/integrity keys CK and IK (using the conversion function c3) and sends Kc to the target BSC (which forwards it to the BTS).

b) In case of a handover to a GSM BSS controlled by other R98- MSC/VLR, the initial MSC/VLR derives the GSM cipher key from the stored UMTS cipher/integrity keys (using the conversion function c3) and sends it to the target BSC via the new MSC/VLR controlling the BSC. The initial MSC/VLR remains the anchor point throughout the service.

c) In case of a handover to a GSM BSS controlled by another R99+ MSC/VLR, the initial MSC/VLR sends the stored UMTS cipher/integrity keys CK and IK to the new MSC/VLR. The initial MSC/VLR also derives Kc and sends it to the new MSC/VLR. The new MSC/VLR store the keys and sends the received GSM cipher key Kc to the target BSC (which forwards it to the BTS). The initial MSC/VLR remains the anchor point throughout the service.

At the user side, in either case, the ~~UE~~ME applies the derived GSM cipher key Kc received from the USIM during the last UMTS AKA procedure.

6.8.4.2 GSM security context

A GSM security context in UTRAN is only established for a GSM subscribers with a ~~R99+ UE~~R99+ ME. At the network side, two cases are distinguished:

a) In case of a handover to a GSM BSS controlled by the same MSC/VLR, the MSC/VLR sends the stored GSM cipher key Kc to the target BSC (which forwards it to the BTS).

b) In case of a handover to a GSM BSS controlled by another MSC/VLR (R99+ or R98-), the initial MSC/VLR sends the stored GSM cipher key Kc to the BSC via the new MSC/VLR controlling the target BSC. The initial MSC/VLR remains the anchor point throughout the service.

If the non-anchor MSC/VLR is R99+, then the anchor MSC/VLR also derives and sends to the non-anchor MSC/VLR the UMTS cipher/integrity keys CK and IK. The non-anchor MSC/VLR stores all keys. This is done to allow subsequent handovers in a non-anchor R99+ MSC/VLR.

At the user side, in either case, the ~~UE~~ME applies the stored GSM cipher key Kc.

6.8.5 Intersystem handover for CS Services – from GSM BSS to UTRAN

If ciphering has been started when an intersystem handover occurs from GSM BSS to UTRAN, the necessary information (e.g. CK, IK, initial HFN value information, supported/allowed UMTS algorithms) is transmitted within the system infrastructure before the actual handover is executed to enable the communication to proceed from the old GSM BSS to the new RNC, and to continue the communication in ciphered mode.

The integrity protection of signalling messages shall be started immediately after that the intersystem handover from GSM BSS to UTRAN is completed.

6.8.5.1 UMTS security context

A UMTS security context in GSM BSS is only established for UMTS subscribers with ~~R99+ UE~~R99+ ME under GSM BSS controlled by a R99+ VLR/SGSN. At the network side, two cases are distinguished:

a) In case of a handover to a UTRAN controlled by the same MSC/VLR, the stored UMTS cipher/integrity keys CK and IK are sent to the target RNC.

b) In case of a handover to a UTRAN controlled by another MSC/VLR, the initial MSC/VLR sends the stored UMTS cipher/integrity keys CK and IK to the new RNC via the new MSC/VLR that controls the target RNC. The initial MSC/VLR remains the anchor point for throughout the service.

   The anchor MSC/VLR also derives and sends to the non-anchor MSC/VLR the GSM cipher key Kc. The non-anchor MSC/VLR stores all keys. This is done to allow subsequent handovers in a non-anchor R99+ MSC/VLR.

At the user side, in either case, the ~~UE~~ME applies the stored UMTS cipher/integrity keys CK and IK.

6.8.5.2 GSM security context

Handover from GSM BSS to UTRAN with a GSM security context is only possible for a GSM subscriber with a ~~R99+ UE~~R99+ ME. At the network side, two cases are distinguished:

a) In case of a handover to a UTRAN controlled by the same MSC/VLR, UMTS cipher/integrity keys CK and IK are derived from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and sent to the target RNC.

b) In case of a handover to a UTRAN controlled by another MSC/VLR, the initial MSC/VLR (R99+ or R98-) sends the stored GSM cipher key Kc to the new MSC/VLR controlling the target RNC. That MSC/VLR derives UMTS cipher/integrity keys CK and IK which are then forwarded to the target RNC. The initial MSC/VLR remains the anchor point for throughout the service.

At the user side, in either case, the ~~UE~~ME derives the UMTS cipher/integrity keys CK and IK from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and applies them.

6.8.6 Intersystem change for PS Services – from UTRAN to GSM BSS

6.8.6.1 UMTS security context

A UMTS security context in UTRAN is only established for UMTS subscribers. At the network side, three cases are distinguished:

a) In case of an intersystem change to a GSM BSS controlled by the same SGSN, the SGSN derives the GSM cipher key Kc from the stored UMTS cipher/integrity keys CK and IK (using the conversion function c3) and applies it.

b) In case of an intersystem change to a GSM BSS controlled by another R99+ SGSN, the initial SGSN sends the stored UMTS cipher/integrity keys CK and IK to the new SGSN. The new SGSN stores the keys, derives the GSM cipher key Kc and applies the latter. The new SGSN becomes the new anchor point for the service.

c) In case of an intersystem change to a GSM BSS controlled by a R98- SGSN, the initial SGSN derives the GSM cipher key Kc and sends the GSM cipher key Kc to the new SGSN. The new SGSN stores the GSM cipher key Kc and applies it. The new SGSN becomes the new anchor point for the service.

At the user side, in all cases, the ~~UE~~ME applies the derived GSM cipher key Kc received from the USIM during the last UMTS AKA procedure.

6.8.6.2 GSM security context

A GSM security context in UTRAN is only established for GSM subscribers. At the network side, two cases are distinguished:

a) In case of an intersystem change to a GSM BSS controlled by the same SGSN, the SGSN starts to apply the stored GSM cipher key Kc.

b) In case of an intersystem change to a GSM BSS controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the BSC. The new SGSN stores the key and applies it. The new SGSN becomes the new anchor point for the service.

At the user side, in both cases, the ~~UE~~ME applies the GSM cipher key Kc that is stored.

6.8.7 Intersystem change for PS services – from GSM BSS to UTRAN

6.8.7.1 UMTS security context

A UMTS security context in GSM BSS is only established for UMTS subscribers with ~~R99+ UE~~R99+ ME connected to a R99+ VLR/SGSN. At the network side, two cases are distinguished:

a) In case of an intersystem change to a UTRAN controlled by the same SGSN, the stored UMTS cipher/integrity keys CK and IK are sent to the target RNC.

b) In case of an intersystem change to a UTRAN controlled by another SGSN, the initial SGSN sends the stored UMTS cipher/integrity keys CK and IK to the (new) SGSN controlling the target RNC. The new SGSN becomes the new anchor point for the service. The new SGSN then stores the UMTS cipher/integrity keys CK and IK and sends them to the target RNC.

At the user side, in both cases, the ~~UE~~ME applies the stored UMTS cipher/integrity keys CK and IK.

6.8.7.2 GSM security context

A GSM security context in GSM BSS can be either:

- **Established for a UMTS subscriber**

  A GSM security context for a UMTS subscriber is established in case the user has a ~~R98- UE~~R98- ME, where intersystem change to UTRAN is not possible, or in case the user has a R99+~~UE~~ME but the SGSN is R98-, where intersystem change to UTRAN implies a change to a R99+ SGSN.

  As result, in case of intersystem change to a UTRAN controlled by another R99+ SGSN, the initial R98- SGSN sends the stored GSM cipher key Kc to the new SGSN controlling the target RNC.

  Since the new R99+ SGSN has no indication of whether the subscriber is GSM or UMTS, a R99+ SGSN shall perform a new UMTS AKA when receiving Kc from a R98- SGSN. A UMTS security context using fresh quintuplets is then established between the R99+ SGSN and the USIM. The new SGSN becomes the new anchor point for the service.

  At the user side, new keys shall be agreed during the new UMTS AKA initiated by the R99+ SGSN.

- **Established for a GSM subscriber**

Handover from GSM BSS to UTRAN for GSM subscriber is only possible with ~~R99+ UE~~R99+ ME. At the network side, three cases are distinguished:

a) In case of an intersystem change to a UTRAN controlled by the same SGSN, the SGSN derives UMTS cipher/integrity keys CK and IK from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and sends them to the target RNC.

b) In case of an intersystem change from a R99+ SGSN to a UTRAN controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the target RNC. The new SGSN becomes the new anchor point for the service. The new SGSN stores the GSM cipher key Kc and derives the UMTS cipher/integrity keys CK and IK which are then forwarded to the target RNC.

c) In case of an intersystem change from an R98-SGSN to a UTRAN controlled by another SGSN, the initial SGSN sends the stored GSM cipher key Kc to the (new) SGSN controlling the target RNC. The new SGSN becomes the new anchor point for the service. To ensure use of UMTS keys for a possible UMTS subscriber (superfluous in this case), a R99+ SGSN will perform a new AKA when a R99+~~UE~~ME is coming from a R98-SGSN.

At the user side, in all cases, the ~~UE~~ME derives the UMTS cipher/integrity keys CK and IK from the stored GSM cipher key Kc (using the conversion functions c4 and c5) and applies them. In case c) these keys will be over-written with a new CK, IK pair due to the new AKA.

7.6 Distribution of security parameters to UTRAN

Confidentiality and integrity between the user and the network is handled by the ~~UE~~ME/USIM and the RNC.

The security parameters for the confidentiality and integrity algorithms must be distributed from the core network to the RNC over the Iu-interface in a secure manner. The actual mechanism for securing these parameters has not yet been identified.

3GPP TSG SA WG 3 (Security) meeting #13
Yokohama (Japan), 24—26 May, 2000

Document **S3-000337**
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.

33.103 CR 009 Current Version: 3.2.0

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

For submission to:	SA #8	for approval	☒	strategic	□	*(for SMG*
list expected approval meeting # here ↑		for information	□	non-strategic	□	*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: (U)SIM □ ME □ UTRAN / Radio □ Core Network ☒
(at least one should be marked with an X)

Source: SA WG3 **Date:** 2000-05-19

Subject: SQN length

Work item: Security

Category:	F	Correction	☒	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	□		Release 98	□
with an X)	D	Editorial modification	□		Release 99	☒
					Release 00	□

Reason for change: S3 decision to fix the length of SQN to 48 bits must be reflected in TS 33.103. The length of “AUTN”, “AUTS” and “UMTS AV” is also aligned accordingly.

Clauses affected: 4.2.2, 4.5.3, 4.6.1

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: This CR considers that EUIC and MAP Security features are not part of R99 and therefore these chapters are not updated and proposed to be removed instead.

help.doc

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

4.2.2 Authentication and key agreement (AKA$_{USIM}$)

The USIM shall support the UMTS mechanism for authentication and key agreement described in 6.3 of 3G TS 33.102.

The following data elements need to be stored on the USIM:

a) K: a permanent secret key;

b) SQN$_{MS}$: a counter that is equal to the highest sequence number SQN in an AUTN parameter accepted by the user;

c) RAND$_{MS}$: the random challenge which was received together with the last AUTN parameter accepted by the user. It is used to calculate the re-synchronisation message together with the highest accepted sequence number (SQN$_{MS}$);

d) KSI: key set identifier;

e) THRESHOLD$_{C}$: a threshold defined by the HE to trigger re-authentication and to control the cipher key lifetime;

f) CK The access link cipher key established as part of authentication;

g) IK The access link integrity key established as part of authentication;

h) HFN$_{MS:}$ Stored Hyper Frame Number provides the Initialisation value for most significant part of COUNT-C and COUNT-I. The least significant part is obtained from the RRC sequence number;

i) AMF: A 16-bit field used Authentication Management. The use and format are unspecified in the architecture but examples are given in an informative annex;

j) The GSM authentication parameter and GSM cipher key derived from the UMTS to GSM conversion functions.

Table 3 provides an overview of the data elements stored on the USIM to support authentication and key agreement.

Table 3: USIM – Authentication and key agreement – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
K	Permanent secret key	1 (note 1)	Permanent	128 bits	Mandatory
SQN$_{MS}$	Sequence number counter	1	Updated when AKA protocol is executed	~~32-64~~48 bits	Mandatory
WINDOW (option 1)	Accepted sequence number array	1	Updated when AKA protocol is executed	10 to 100 bits	Optional
LIST (option 2)	Ordered list of sequence numbers received	1	Updated when AKA protocol is executed	32-64 bits	Optional
RAND$_{MS}$	Random challenge received by the user.	1	Updated when AKA protocol is executed	128 bits	Mandatory
KSI	Key set identifier	1	Updated when AKA protocol is executed	3 bits	Mandatory
THRESHOLD$_{C}$	Threshold value for ciphering	1	Permanent	32 bits	Optional
CK	Cipher key	1	Updated when AKA protocol is executed	128 bits	Mandatory
IK	Integrity key	1	Updated when AKA protocol is executed	128 bits	Mandatory
HFN$_{MS:}$	Initialisation value for most significant part for COUNT-C and for COUNT-I	1	Updated when connection is released	25 bits	Mandatory
AMF	Authentication Management Field (indicates the algorithm and key in use)	1	Updated when AKA protocol is executed	16 bits	Mandatory
RAND$_{G}$	GSM authentication parameter from conversion function	1	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional
SRES	GSM authentication parameter from conversion function	1	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional
Kc	GSM cipher Key	1	Updated when GSM AKA or UMTS AKA protocol is executed	As for GSM	Optional

NOTE 1: HE policy may dictate more than one, the active key signalled using the AMF function.

The following cryptographic functions need to be implemented on the USIM:

- f1: a message authentication function for network authentication;
- f1*: a message authentication function for support to re-synchronisation;
- f2: a message authentication function for user authentication;
- f3: a key generating function to derive the cipher key;
- f4: a key generating function to derive the integrity key;

- f5: a key generating function to derive the anonymity key;
- c2: Conversion function for interoperation with GSM from XRES (UMTS) to SRES (GSM);
- c3: Conversion function for interoperation with GSM from Ck and IK (UMTS) to Kc (GSM).

Figure 2 provides an overview of the data integrity, data origin authentication and verification of the freshness by the USIM of the RAND and AUTN parameters received from the VLR/SGSN, and the derivation of the response RES, the cipher key CK and the integrity key IK. Note that the anonymity Key (AK) is optional.

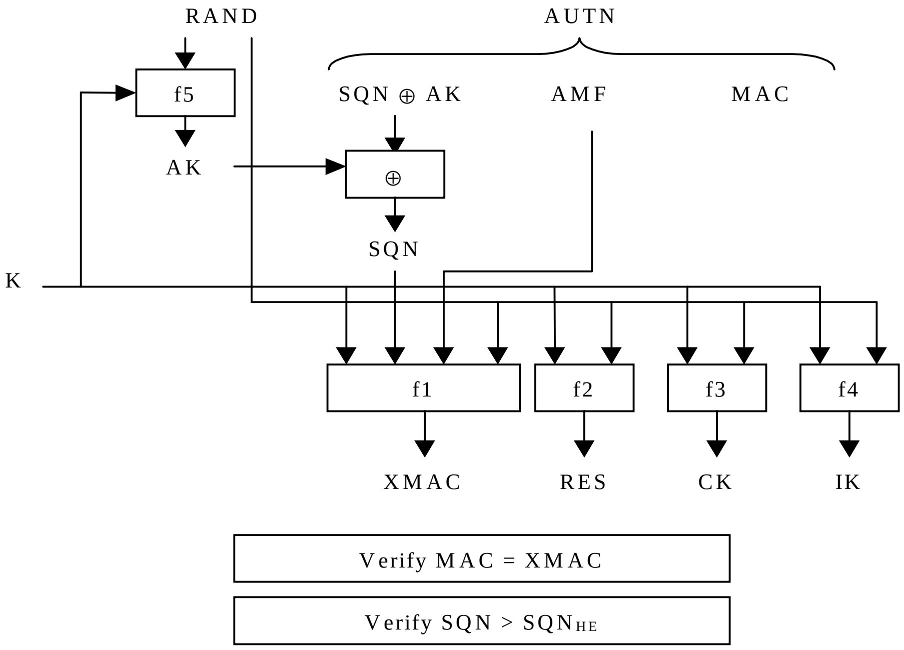


Figure 1: User authentication function in the USIM

Figure 3 provides an overview of the generation in the USIM of a token for re-synchronisation AUTS.

a) The USIM computes MAC-S = $f1^*_K(SQN_{MS} \| RAND \| AMF^*)$, whereby AMF* is a default value for AMF used in re-synchronisation.

b) If SQN_{MS} is to be concealed with an anonymity key AK, the USIM computes AK = $f5_K$(MAC-S || 0…0), whereby MAC-S forms the 12 most significant octets and 32 zeros form the 4 least significant octets of the required 16 octet input parameter, and the concealed counter value is then computed as $SQN_{MS} \oplus AK$.

c) The re-synchronisation token is constructed as AUTS = SQN_{MS} [⊕ AK] || MAC-S.

Upon receipt of an indication of synchronisation failure and a (AUTS, RAND) pair, the HLR/AuC may perform the following cryptographic functions:

a) If SQN_{MS} is concealed with an anonymity key AK, the HLR/AuC computes AK = $f5_K$(MAC-S || 0…0), whereby MAC-S forms the 12 most significant octets and 32 zeros form the 4 least significant octets of the required 16 octet input parameter and retrieves the unconcealed counter value as $SQN_{MS} = (SQN_{MS} \oplus AK)$ xor AK.

b) If SQN generated from SQN_{HE} would not be acceptable, then the HLR/AuC computes XMAC-S = $f1^*_K(SQN_{MS} \|$ RAND || AMF*), whereby AMF* is a default value for AMF used in re-synchronisation.

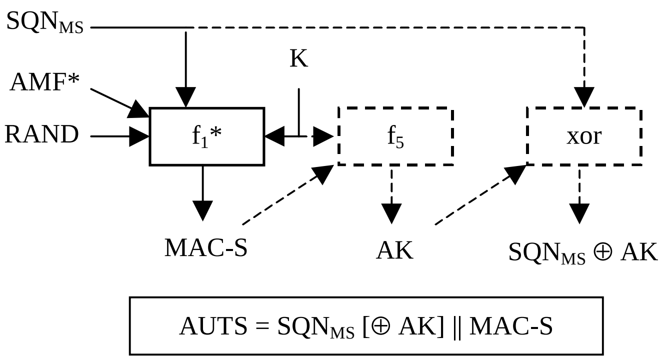


Figure 2: Generation of a token for re-synchronisation AUTS (note 1)

NOTE 1: The lengths of AUTS and MAC-S are specified in table 20~~2~~.

Table 4 provides a summary of the cryptographic functions implemented on the USIM to support authentication and key agreement.

Table 4: USIM – Authentication and key agreement – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f1	Network authentication function	1	Permanent	Proprietary	Mandatory
f1*	Message authentication function for synchronisation	1	Permanent	Proprietary	Mandatory
f2	User authentication function	1	Permanent	Proprietary	Mandatory
f3	Cipher key generating function	1	Permanent	Proprietary	Mandatory
f4	Integrity key generating function	1	Permanent	Proprietary	Mandatory
f5	Anonymity key generating function	1	Permanent	Proprietary	Optional
c2 and c3	Conversion functions for interoperation with GSM	1 of each	Permanent	Standard	Optional

4.5.3 Authentication and key agreement (AKA_{SN})

The VLR (equivalently the SGSN) shall support the UMTS mechanism for authentication and key agreement described in 6.3 of 3G TS 33.102.

The following data elements need to be stored in the VLR (and SGSN):

a) AV: Authentication vectors;

Table 16 provides an overview of the composition of an authentication vector

Table 16: Composition of an authentication vector

Symbol	Description	Multiplicity	Length
RAND	Network challenge	1	128
XRES	Expected response	1	32-128
CK	Cipher key	1	128
IK	Integrity key	1	128
AUTN	Authentication token	1 that consists of:	128~~112-144~~
SQN or SQN ⊕ AK	Sequence number or Concealed sequence number	1 per AUTN	48~~32-64~~
AMF	Authentication Management Field	1 per AUTN	16
MAC-A	Message authentication code for network authentication	1 per AUTN	64

b) KSI: Key set identifier;

c) CK: Cipher key;

d) IK: Integrity key;

e) GSM AV: Authentication vectors for GSM.

Table 17 provides an overview of the data elements stored in the VLR/SGSN to support authentication and key agreement.

Table 17: VLR/SGSN – Authentication and key agreement – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
UMTS AV	UMTS Authentication vectors	several per user, SN dependent	Depends on many things	528-640~~656~~	Mandatory
KSI	Key set identifier	1 per user	Updated when AKA protocol is executed	3 bits	Mandatory
CK	Cipher key	1 per user	Updated when AKA protocol is executed	128 bits	Mandatory
IK	Integrity key	1 per user	Updated when AKA protocol is executed	128 bits	Mandatory
GSM AV	GSM Authentication vectors	As for GSM	As for GSM	As for GSM	Optional

The following cryptographic functions shall be implemented in the VLR/SGSN:

- c4: Conversion function for interoperation with GSM from Kc (GSM) to CK (UMTS);
- c5: Conversion function for interoperation with GSM from Kc (GSM) to IK (UMTS).

Table 18 provides an overview of the cryptographic functions implemented on the UE to support the mechanism for data confidentiality.

Table 18: VLR/SGSN Authentication and Key Agreement – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
c4	Conversion function for interoperation with GSM	1	Permanent	Standardised	Optional
c5	Conversion function for interoperation with GSM	1	Permanent	Standardised	Optional

4.6.1 Authentication and key agreement (AKA_{he})

The HLR/AuC shall support the UMTS mechanism for authentication and key agreement described in 6.3 of 3G TS 33.102.

The following data elements need to be stored in the HLR/AuC:

a) K: a permanent secret key;

b) SQN_{HE}: a counter used to generate SQN from;

c) AV: authentication vectors computed in advance;

Table 19 provides an overview of the data elements stored on the HLR/AuC to support authentication and key agreement.

Table 19: HLR/AuC – Authentication and key agreement – Data elements

Symbol	Description	Multiplicity	Lifetime	Length	Mandatory / Optional
K	Permanent secret key	1	Permanent	128 bits	Mandatory
SQN_{HE}	Sequence number counter	1	Updated when AVs are generated	48~~32-64~~ bits	Mandatory
UMTS AV	UMTS Authentication vectors	HE option	Updated when AVs are generated	544-640 bits	Optional
GSM AV	GSM Authentication vectors	HE option that consists of:	Updated when AVs are generated	As GSM	Optional
RAND	GSM Random challenge			128 bits	Optional
SRES	GSM Expected response			32 bits	Optional
Kc	GSM cipher key			64 bits	Optional

Table 20 shows how the construction of authentication token for synchronisation failure messages used to support authentication and key agreement.

Table 20: Composition of an authentication token for synchronisation failure messages

Symbol	Description	Multiplicity	Length
AUTS	Synchronisation Failure authentication token	that consists of:	112~~96 – 128~~
SQN	Sequence number	1 per AUTS	48~~32-64~~
MAC-S	Message authentication code for Synchronisation Failure messages	1 per AUTS	64

Figure 4 provides an overview of how authentication vectors are generated in the HLR/AuC.

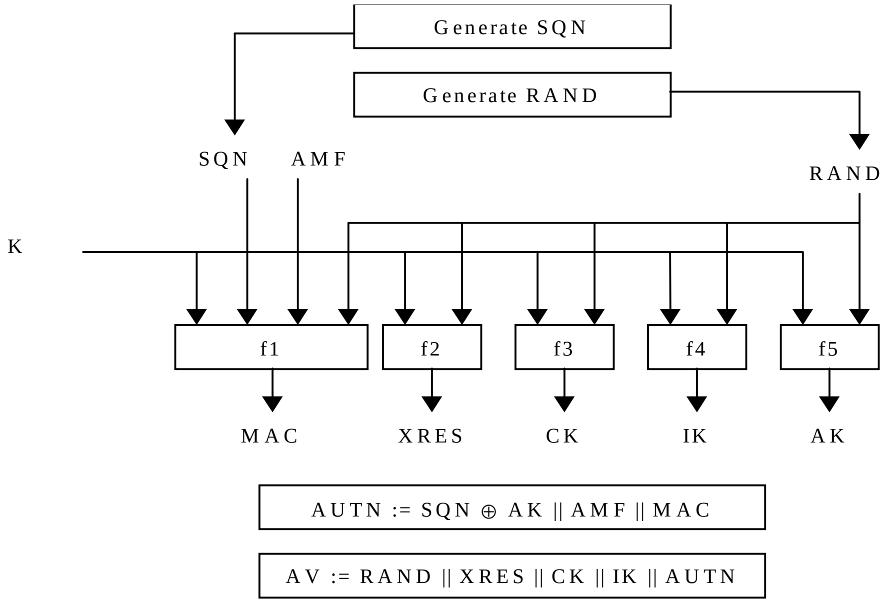

Generate SQN
Generate RAND
SQN
AMF
RAND
K
f1
f2
f3
f4
f5
MAC
XRES
CK
IK
AK
AUTN := SQN ⊕ AK || AMF || MAC
AV := RAND || XRES || CK || IK || AUTN

Figure 3: Generation of an authentication vector

The following cryptographic functions need to be implemented in the HLR/AuC:

- f1: a message authentication function for network authentication;
- f1*: a message authentication function for support to re-synchronisation;
- f2: a message authentication function for user authentication;
- f3: a key generating function to derive the cipher key;
- f4: a key generating function to derive the integrity key;
- f5: a key generating function to derive the anonymity key;
- c1: Conversion function for interoperation with GSM from RAND (UMTS) > RAND (GSM);
- c2: Conversion function for interoperation with GSM from XRES (UMTS) to SRES (GSM);
- c3: Conversion function for interoperation with GSM from CK and IK (UMTS) to Kc (GSM).

Table 21 provides a summary of the cryptographic functions implemented on the USIM to support authentication and key agreement.

Table 21: HLR/AuC – Authentication and key agreement – Cryptographic functions

Symbol	Description	Multiplicity	Lifetime	Standardised / Proprietary	Mandatory / Optional
f1	Network authentication function	1	Permanent	Proprietary	Mandatory
f1*	Message authentication function for synchronisation	1	Permanent	Proprietary	Mandatory
f2	User authentication function	1	Permanent	Proprietary	Mandatory
f3	Cipher key generating function	1	Permanent	Proprietary	Mandatory
f4	Integrity key generating function	1	Permanent	Proprietary	Mandatory
f5	Anonymity key generating function	1	Permanent	Proprietary	Optional
A3/A8	GSM user authentication functions	1	Permanent	Proprietary	Optional
c1, c2 and c3	Functions for converting UMTS AV's to GSM AV's	1 for each	Permanent	Standard	Optional

3GPP TSG SA WG3#13
Yokohama, Japan, 24-26 May 2000

Document S3-000342_att
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.

33.105 CR 011 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:	TSG SA#8	for approval	☒	strategic	□	*(for SMG use only)*
list expected approval meeting # here ↑		for information	□	non-strategic	□	

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 □
(at least one should be marked with an X)

Source: SA WG3 (Security) **Date:** 22 May 2000

Subject: Clarification of BEARER and DIRECTION parameters

Work item: Security

Category:	F	Correction	☒	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	□		Release 98	□
with an X)	D	Editorial modification	□		Release 99	☒
					Release 00	□

Reason for change: To get 33.105 in line with 33.102. The BEARER parameter cannot be the logical channel identity because that is not unique for one UE; instead the radio bearer identity must be used. Values for the DIRECTION bit have to be defined.

Clauses affected:

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:

help.doc

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

5.2.7 Interfaces to the algorithm

5.2.7.1 CK

CK: the cipher key

CK[0], CK[1], …, CK[127]

The length of CK is 128 bits. In case the effective key length k is smaller than 128 bits, the most significant bits of CK shall carry the effective key information, whereas the remaining, least significant bits shall repeat the effective key information:

CK[n] = CK[n mod k], for all n, such that k ≤ n < 128.

5.2.7.2 COUNT-C

COUNT-C: the cipher sequence number.

COUNT-C[0], COUNT-C[1], …, COUNT-C[31]

The length of the COUNT-C parameter is 32 bits.

Sychronisation of the keystream is based on the use of a physical layer (Layer 1) frame counter combined with a hyperframe counter introduced to avoid re-use of the keystream. This allows the keystream to be synchronised every 10ms physical layer frame. The exact structure of the COUNT-C is specified in TS 33.102.

5.2.7.3 BEARER

BEARER: the radio bearer identifier.

BEARER[0], BEARER[1], …, BEARER[4~~3~~]

The length of BEARER is 5~~4~~ bits.

The same cipher key may be used for different radio bearers simultaneously associated with a single user which are multiplexed onto a single 10ms physical layer frame. To avoid using the same keystream to encrypt more than one bearer, the algorithm shall generate the keystream based on the identity of the radio bearer.

5.2.7.4 DIRECTION

DIRECTION: the direction of transmission of the bearer to be encrypted.

DIRECTION[0]

The length of DIRECTION is 1 bit.

The same cipher key may be used for uplink and downlink channels simultaneously associated with a UE, which are multiplexed onto a single 10ms physical layer frame. To avoid using the same keystream to encrypt both uplink and downlink transmissions, the algorithm shall generate the keystream based on the direction of transmission.

The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

An explicit direction value is required in preference to splitting the keystream segment into uplink and downlink portions to allow for asymmetric bearer services.

5.2.7.5 LENGTH

LENGTH: the required length of keystream.

LENGTH[0], LENGTH[1], …, LENGTH[15]

The length of LENGTH is 16 bits.

For a given bearer and transmission direction the length of the plaintext block that is transmitted during a single physical layer frame may vary. The algorithm shall generate a keystream block of variable length based on the value of the length parameter.

The input parameter LENGTH shall affect only the length of the KEYSTREAM BLOCK, not the actual bits in it.

The format of LENGTH cannot be specified at present since the number and sizes of RLC PDUs / MAC SDUs in each 10ms physical layer frame have not yet been fully specified. However, a maximum RLC PDU / MAC SDU size in the region of 1000 bits has been informally indicated by 3GPP TSG RAN2. The range of values of the length parameter will depend not only on the RLC PDU / MAC SDU size but also the number of RLC PDUs / MAC SDUs which may be sent in a single physical layer 10ms frame for a given bearer and transmission direction.

Not all values between the maximum and minimum values shall be required but it is expected that the ability to produce length values of whole numbers of octets between a minimum and a maximum value will be required.

5.2.7.6 KEYSTREAM

KEYSTREAM: the output keystream.

KS [0], KS [1], …, KS [LENGTH-1]

The length of a keystream block equals the value of the input parameter LENGTH.

5.2.7.7 PLAINTEXT

PLAINTEXT: the plaintext.

PT[0], PT[1], …, PT[LENGTH-1]

The length of a keystream block equals the value of the input parameter LENGTH.

This plaintext block consists of the payload of the particular RLC PDUs / MAC SDUs to be encrypted in a single 10ms physical layer frame for a given bearer and transmission direction. It may consist of user traffic or signalling data. The structure of the plaintext block cannot be specified at present.

5.2.7.8 CIPHERTEXT

CIPHERTEXT: the ciphertext.

CT[0], CT[1], …, CT[LENGTH-1]

The length of a keystream block equals the value of the input parameter LENGTH.

5.3 Data integrity

5.3.1 Overview

The mechanism for data integrity of signalling data that is described in 6.6 of [1] requires the following cryptographic function:

f9 UMTS integrity algorithm.

Figure 3 illustrates the use of the function f9 to derive a MAC-I from a signalling message.

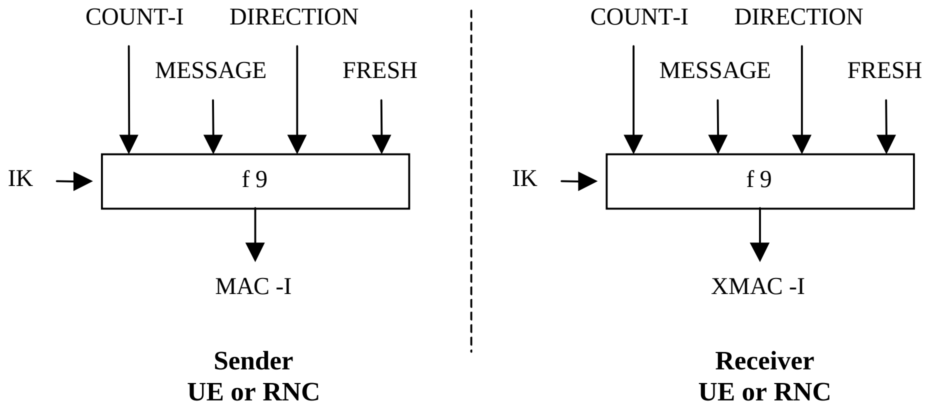


Figure 1: Derivation of MAC-I (or XMAC-I) on a signalling message

The input parameters to the algorithm are the Integrity Key (IK), a time dependent input (COUNT-I), a random value generated by the network side (FRESH), the direction bit (DIRECTION) and the signalling data (MESSAGE). Based on these input parameters the user computes with the function f9 the message authentication code for data integrity (MAC-I) which is appended to the message when sent over the radio access link. The receiver computes XMAC-I on the messages received in the same way as the sender computed MAC-I on the message sent.

5.3.2 Use

The MAC function f9 shall be used to authenticate the data integrity and data origin of signalling data transmitted between UE and RNC.

5.3.3 Allocation

The MAC function f9 is allocated to the UE and the RNC.

Integrity protection shall be applied at the RRC layer.

5.3.4 Extent of standardisation

The function f9 is fully standardized.

5.3.5 Implementation and operational considerations

The algorithm should be designed to accommodate a range of implementation options including hardware and software implementations.

5.3.6 Type of algorithm

The function f9 shall be a MAC function.

5.3.7 Interface

5.3.7.1 IK

IK: the integrity key

IK[0], IK[1], …, IK[127]

The length of IK is 128 bits.

5.3.7.2 COUNT-I

COUNT-I: a frame dependent input.

COUNT-I[0], COUNT-I[1], …, COUNT-I[31]

The length of COUNT-I is 32 bits.

The input parameter COUNT-I protects against replay during a connection. It is a value incremented by one for each integrity protected message. COUNT-I consists of two parts: the HYPERFRAME NUMBER (HFN) as the most significant part and a RRC Sequence Number as the least significant part. The initial value of the hyperframe number is sent by the user to the network at connection set-up. The user stores the greatest used hyperframe number from the previous connection and increments it by one. In this way the user is assured that no COUNT-I value is re-used (by the network) with the same integrity key.

5.3.7.3 FRESH

FRESH: a random number generated by the RNC.

FRESH[0], FRESH[1], …, FRESH[31]

The length of FRESH is 32 bits.

The same integrity key may be used for several consecutive connections. This FRESH value is an input to the algorithm in order to assure the network side that the user is not replaying old MAC-Is.

5.3.7.4 MESSAGE

MESSAGE: the signalling data.

MESSAGE[0], MESSAGE[1], …, MESSAGE[X19-1]

The maximum length of MESSAGE is X19.

5.3.7.5 DIRECTION

DIRECTION: the direction of transmission of signalling messages (user to network or network to users).

DIRECTION[0]

The length of DIRECTION is 1 bit.

The same integrity key may be used for uplink and downlink channels simultaneously associated with a UE.

The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

5.3.7.6 MAC-I (and equivalently XMAC-I)

MAC-I: the message authentication code for data integrity authentication

MAC-I[0], MAC-I[1], …, MAC-I[31]

The length of MAC-I is 32 bits.