

# ETSI TS 133 102 V3.5.0 (2000-07)

---

*Technical Specification*

## **Universal Mobile Telecommunications System (UMTS); 3G Security; Security Architecture (3G TS 33.102 version 3.5.0 Release 1999)**



---

**Reference**

RTS/TSGS-0333102UR2

---

**Keywords**

UMTS

**ETSI**

650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

---

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° 7803/88

---

**Important notice**

---

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF).

In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at <http://www.etsi.org/tb/status/>

If you find errors in the present document, send your comment to:

editor@etsi.fr

---

**Copyright Notification**

---

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2000.

All rights reserved.

---

## Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://www.etsi.org/ipr>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

---

## Foreword

This Technical Specification (TS) has been produced by the ETSI 3<sup>rd</sup> Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under [www.etsi.org/key](http://www.etsi.org/key) .

# Contents

Foreword .....	6
1 Scope.....	7
2 References.....	7
2.1 Normative references.....	7
2.2 Informative references .....	8
3 Definitions, symbols and abbreviations .....	8
3.1 Definitions .....	8
3.2 Symbols .....	9
3.3 Abbreviations.....	10
4 Overview of the security architecture .....	11
5 Security features .....	12
5.1 Network access security.....	12
5.1.1 User identity confidentiality.....	12
5.1.2 Entity authentication .....	13
5.1.3 Confidentiality.....	13
5.1.4 Data integrity.....	13
5.1.5 Mobile equipment identification .....	14
5.2 Network domain security.....	14
5.2.1 Void.....	14
5.2.2 Void.....	14
5.2.3 Void.....	14
5.2.4 Fraud information gathering system.....	14
5.3 User domain security .....	14
5.3.1 User-to-USIM authentication.....	14
5.3.2 USIM-Terminal Link .....	14
5.4 Application security.....	15
5.4.1 Secure messaging between the USIM and the network .....	15
5.4.2 Void.....	15
5.4.3 Access to user profile data .....	15
5.4.4 IP security .....	15
5.5 Security visibility and configurability.....	15
5.5.1 Visibility.....	15
5.5.2 Configurability .....	16
6 Network access security mechanisms .....	16
6.1 Identification by temporary identities.....	16
6.1.1 General .....	16
6.1.2 TMUI reallocation procedure.....	16
6.1.3 Unacknowledged allocation of a temporary identity.....	17
6.1.4 Location update.....	17
6.2 Identification by a permanent identity .....	17
6.3 Authentication and key agreement.....	18
6.3.1 General .....	18
6.3.2 Distribution of authentication data from HE to SN.....	20
6.3.3 Authentication and key agreement .....	22
6.3.4 Distribution of IMSI and temporary authentication data within one serving network domain .....	24
6.3.5 Re-synchronisation procedure.....	25
6.3.6 Reporting authentication failures from the SGSN/VLR to the HLR.....	26
6.3.7 Length of sequence numbers.....	26
6.4 Local authentication and connection establishment.....	26
6.4.1 Cipher key and integrity key setting.....	26
6.4.2 Ciphering and integrity mode negotiation.....	26
6.4.3 Cipher key and integrity key lifetime.....	27
6.4.4 Cipher key and integrity key identification.....	27

6.4.5	Security mode set-up procedure .....	28
6.4.6	Signalling procedures in the case of an unsuccessful integrity check .....	30
6.4.7	Signalling procedure for periodic local authentication.....	30
6.4.8	Initialisation of synchronisation for ciphering and integrity protection .....	31
6.5	Access link data integrity.....	32
6.5.1	General .....	32
6.5.2	Layer of integrity protection .....	32
6.5.3	Data integrity protection method.....	32
6.5.4	Input parameters to the integrity algorithm .....	33
6.5.4.1	COUNT-I.....	33
6.5.4.2	IK.....	33
6.5.4.3	FRESH.....	33
6.5.4.4	DIRECTION .....	34
6.5.4.5	MESSAGE .....	34
6.5.5	Integrity key selection .....	34
6.5.6	UIA identification .....	34
6.6	Access link data confidentiality .....	34
6.6.1	General .....	34
6.6.2	Layer of ciphering .....	35
6.6.3	Ciphering method.....	35
6.6.4	Input parameters to the cipher algorithm.....	35
6.6.4.1	COUNT-C .....	35
6.6.4.2	CK .....	36
6.6.4.3	BEARER .....	37
6.6.4.4	DIRECTION .....	37
6.6.4.5	LENGTH .....	37
6.6.5	Cipher key selection.....	37
6.6.6	UEA identification .....	37
6.7	Void .....	37
6.8	Interoperation and handover between UMTS and GSM.....	38
6.8.1	Authentication and key agreement of UMTS subscribers.....	38
6.8.1.1	General .....	38
6.8.1.2	R99+ HLR/AuC.....	39
6.8.1.3	R99+ VLR/SGSN.....	40
6.8.1.4	R99+ ME .....	40
6.8.1.5	USIM.....	41
6.8.2	Authentication and key agreement for GSM subscribers.....	41
6.8.2.1	General .....	41
6.8.2.2	R99+ HLR/AuC.....	42
6.8.2.3	VLR/SGSN.....	42
6.8.2.4	R99+ ME .....	43
6.8.3	Distribution and use of authentication data between VLRs/SGSNs.....	43
6.8.4	Intersystem handover for CS Services – from UTRAN to GSM BSS .....	44
6.8.4.1	UMTS security context.....	44
6.8.4.2	GSM security context .....	45
6.8.5	Intersystem handover for CS Services – from GSM BSS to UTRAN .....	45
6.8.5.1	UMTS security context.....	45
6.8.5.2	GSM security context .....	45
6.8.6	Intersystem change for PS Services – from UTRAN to GSM BSS .....	46
6.8.6.1	UMTS security context.....	46
6.8.6.2	GSM security context .....	46
6.8.7	Intersystem change for PS services – from GSM BSS to UTRAN.....	46
6.8.7.1	UMTS security context.....	46
6.8.7.2	GSM security context .....	47
7	Void .....	47
8	Application security mechanisms .....	47
8.1	Secure messaging between the USIM and the network .....	47
8.2	Void .....	48
8.3	Mobile IP security.....	48

<b>Annex A (informative):</b>	<b>Requirements analysis .....</b>	<b>49</b>
<b>Annex B:</b>	<b>Void.....</b>	<b>50</b>
<b>Annex C (informative):</b>	<b>Management of sequence numbers.....</b>	<b>51</b>
C.1	Generation of sequence numbers in the Authentication Centre.....	51
C.2	Handling of sequence numbers in the USIM.....	52
C.2.1	Protection against wrap around of counter in the USIM.....	52
C.2.2	Acceptance rule .....	52
C.2.3	List update .....	52
C.2.4	Notes.....	52
<b>Annex D:</b>	<b>Void.....</b>	<b>54</b>
<b>Annex E:</b>	<b>Void.....</b>	<b>55</b>
<b>Annex F (informative):</b>	<b>Example uses of AMF .....</b>	<b>56</b>
F.1	Support multiple authentication algorithms and keys.....	56
F.2	Changing list parameters .....	56
F.3	Setting threshold values to restrict the lifetime of cipher and integrity keys.....	56
<b>Annex G (informative):</b>	<b>Change history .....</b>	<b>57</b>

---

# 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:

- 3 the first digit:
  - 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

This specification defines the security architecture, i.e., the security features and the security mechanisms, for the third generation mobile telecommunication system.

A security feature is a service capability that meets one or several security requirements. The complete set of security features address the security requirements as they are defined in "3G Security: Threats and Requirements" (21.133 [1]). A security mechanism is an element that is used to realise a security feature. All security features and security requirements taken together form the security architecture.

An example of a security feature is user data confidentiality. A security mechanism that may be used to implement that feature is a stream cipher using a derived cipher key.

This specification defines 3G security procedures performed within 3G capable networks (R99+), i.e. intra-UMTS and UMTS-GSM. As an example, UMTS authentication is applicable to UMTS radio access as well as GSM radio access provided that the serving network node and the subscriber are UMTS capable. Interoperability with non-UMTS capable networks (R98-) is also covered.

---

# 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.

## 2.1 Normative references

- [1] 3G TS 21.133: "3<sup>rd</sup> Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".
- [2] 3G TS 33.120: "3<sup>rd</sup> Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".
- [3] UMTS 33.21, version 2.0.0: "Security requirements".
- [4] UMTS 33.22, version 1.0.0: "Security features".
- [5] UMTS 33.23, version 0.2.0: "Security architecture".
- [6] Proposed UMTS Authentication Mechanism based on a Temporary Authentication Key.
- [7] TTC Work Items for IMT-2000 – System Aspects.
- [8] Annex 8 of "Requirements and Objectives for 3G Mobile Services and systems" – "Security Design Principles".
- [9] ETSI GSM 09.02 Version 4.18.0: Mobile Application Part (MAP) Specification.
- [10] ISO/IEC 11770-3: *Key Management – Mechanisms using Asymmetric Techniques*.
- [11] ETSI SAGE: Specification of the BEANO encryption algorithm, Dec. 1995 (confidential).
- [12] ETSI SMG10 WPB: SS7 Signalling Protocols Threat Analysis , Input Document AP 99-28 to SMG10 Meeting#28, Stockholm, Sweden.



- [13] 3G TS 33.105: "3<sup>rd</sup> Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Cryptographic Algorithm Requirements".
- [13a] 3G TS 23.003: "3<sup>rd</sup> Generation Partnership Project (3GPP); Technical Specification Group (TSG) Core Network (CN); Numbering, addressing and identification".
- [13b] 3G TS 23.060: "3<sup>rd</sup> Generation Partnership Project; Technical Specification Group and System Aspects; Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

## 2.2 Informative references

### GSM documents:

- [14] GSM 02.09 version 5.1.1: "Security Aspects".
- [15] GSM 02.22 version 6.0.0: "Personalisation of GSM Mobile Equipment (ME); Mobile functionality specification".
- [16] GSM 02.48, version 6.0.0: "Security Mechanisms for the SIM Application Toolkit; Stage 1".
- [17] GSM 02.60, version 7.0.0: "GPRS; Service Description; Stage 1".
- [18] GSM 03.20, version 6.0.1: "Security related network functions".
- [19] GSM 03.48, version 6.1.0: "Security Mechanisms for the SIM application toolkit; Stage 2".
- [20] GSM 03.60, version 7.0.0: "GPRS; Service Description; Stage 2".
- [21] GSM 11.11, version 7.1.0: "Specification of SIM-terminal interface".
- [22] GSM 11.14, version 7.1.0: "Specification of SIM Application Toolkit for SIM-terminal interface".

### UMTS documents:

- [23] UMTS 21.11, version 0.4.0: "IC-card aspects".
- [24] UMTS 23.01, version 1.0.0: "UMTS Network architecture".
- [25] UMTS 23.20, version 1.4.0: "Evolution of the GSM platform towards UMTS".

---

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

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

**Confidentiality:** The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

**Data integrity:** The property that data has not been altered in an unauthorised manner.

**Data origin authentication:** The corroboration that the source of data received is as claimed.

**Entity authentication:** The provision of assurance of the claimed identity of an entity.

**Key freshness:** A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

**USIM – User Services Identity Module.** In a security context, this module is responsible for performing UMTS subscriber and network authentication and key agreement. It should also be capable of performing GSM authentication and key agreement to enable the subscriber to roam easily into a GSM Radio Access Network.

**SIM – GSM Subscriber Identity Module.** In a security context, this module is responsible for performing GSM subscriber authentication and key agreement. This module is **not** capable of handling UMTS authentication nor storing UMTS style keys.

**UMTS Entity authentication and key agreement:** Entity authentication according to this specification.

**GSM Entity authentication and key agreement:** Entity authentication according to TS ETSI GSM 03.20

**User access module:** either a USIM or a SIM

**Mobile station, user:** the combination of user equipment and a user access module.

**UMTS subscriber:** a mobile station that consists of user equipment with a USIM inserted.

**GSM subscriber:** a mobile station that consists of user equipment with a SIM inserted.

**UMTS security context:** a state that is established between a user and a serving network domain as a result of the execution of UMTS AKA. At both ends "UMTS security context data" is stored, that consists at least of the UMTS cipher/integrity keys CK and IK and the key set identifier KSI.

**GSM security context:** a state that is established between a user and a serving network domain usually as a result of the execution of GSM AKA. At both ends "GSM security context data" is stored, that consists at least of the GSM cipher key Kc and the cipher key sequence number CKSN.

**Quintet, UMTS authentication vector:** temporary authentication data that enables an MSC/VLR or SGSN to engage in UMTS AKA with a particular user. A quintet consists of five elements: a) a network challenge RAND, b) an expected user response XRES, c) a cipher key CK, d) an integrity key IK and e) a network authentication token AUTN.

**Triplet, GSM authentication vector:** temporary authentication data that enables an MSC/VLR or SGSN to engage in GSM AKA with a particular user. A triplet consists of three elements: a) a network challenge RAND, b) an expected user response SRES and c) a cipher key Kc.

**Authentication vector:** either a quintet or a triplet.

**Temporary authentication data:** either UMTS or GSM security context data or UMTS or GSM authentication vectors.

## 3.2 Symbols

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

	Concatenation
⊕	Exclusive or
f1	Message authentication function used to compute MAC
f2	Message authentication function used to compute RES and XRES
f3	Key generating function used to compute CK
f4	Key generating function used to compute IK
f5	Key generating function used to compute AK
K	Long-term secret key shared between the USIM and the AuC

### 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
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAC	Message Authentication Code
MAC-A	The message authentication code included in AUTN, computed using f1
ME	Mobile Equipment
MS	Mobile Station
MSC	Mobile Services Switching Centre
PS	Packet Switched
P-TMSI	Packet-TMSI
Q	Quintet, UMTS authentication vector
RAI	Routing Area Identifier
RAND	Random challenge
SQN	Sequence number
SQN <sub>HE</sub>	Sequence number counter maintained in the HLR/AuC
SQN <sub>MS</sub>	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
TMSI	Temporary Mobile Subscriber Identity
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	UMTS IC Card
USIM	User Services Identity Module
VLR	Visitor Location Register
XRES	Expected Response

## 4 Overview of the security architecture

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

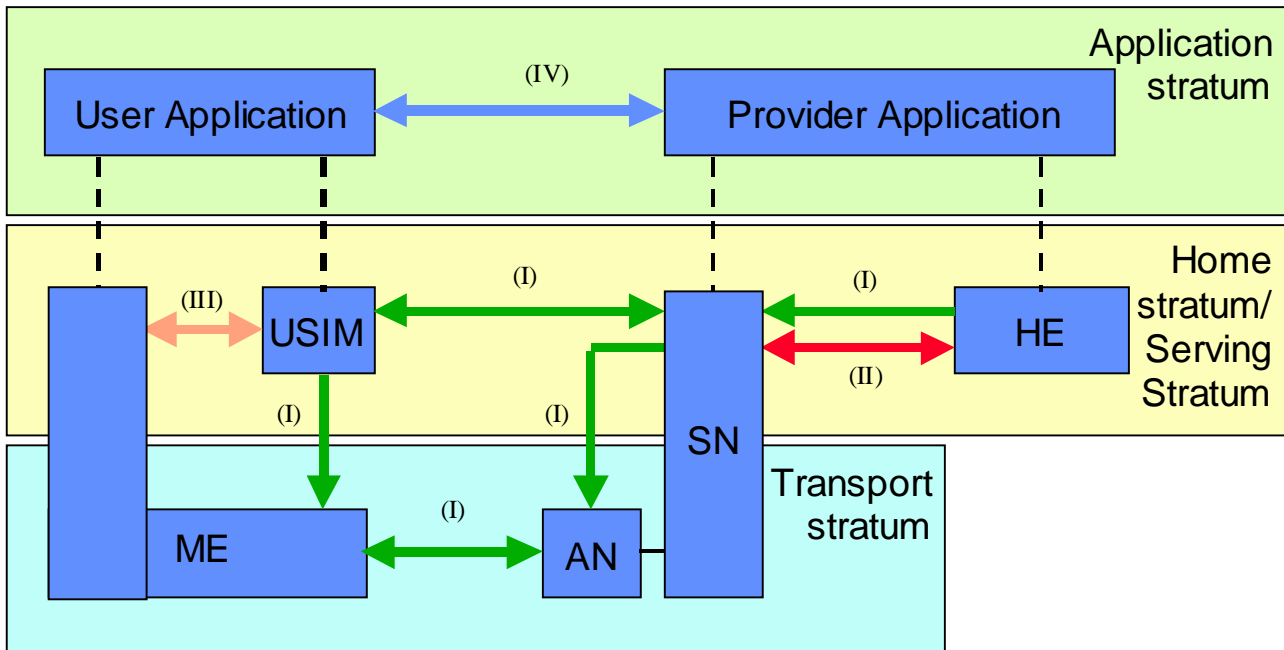


Figure 1: Overview of the security architecture

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 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.

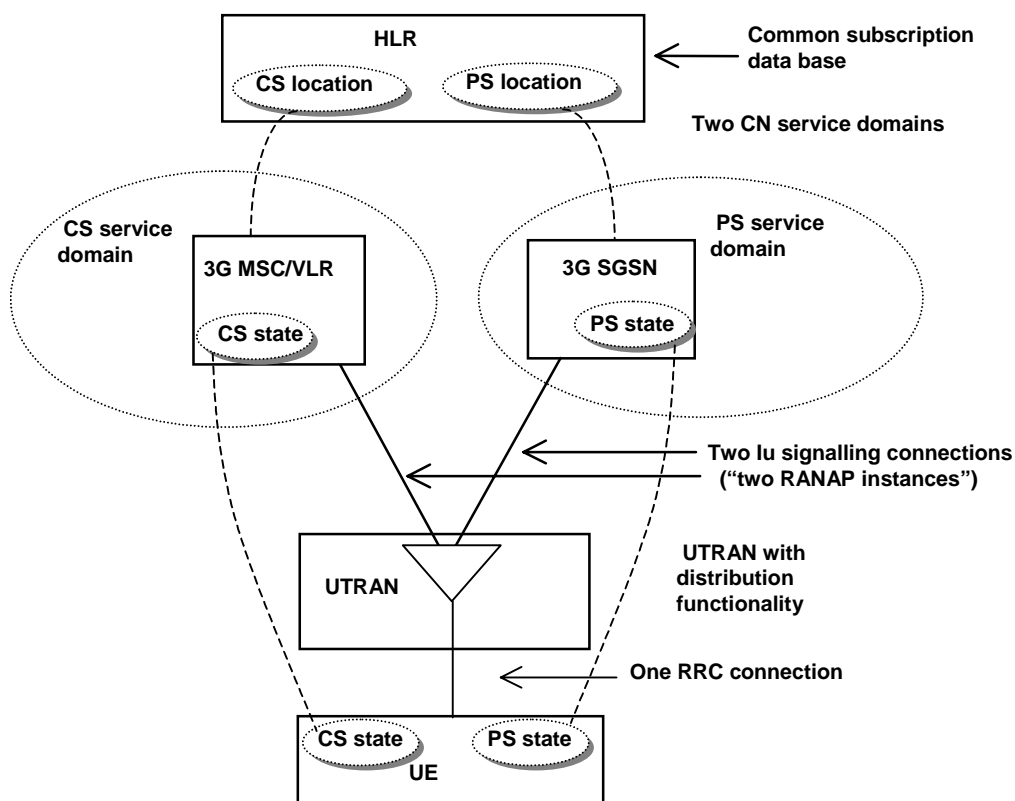


Figure 2: Overview of the ME registration and connection principles within UMTS for the separate CN architecture case when the CN consists of both a CS service domain with evolved MSC/VLR, 3G\_MSC/VLR, as the main serving node and an PS service domain with evolved SGSN/GGSN, 3G\_SGSN and 3G GGSN, as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

## 5 Security features

### 5.1 Network access security

#### 5.1.1 User identity confidentiality

The following security features related to user identity confidentiality are provided:

- **user identity confidentiality:** the property that the permanent user identity (IMUI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link;
- **user location confidentiality:** the property that the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link;
- **user untraceability:** the property that an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.

To achieve these objectives, the user is normally identified by a temporary identity by which he is known by the visited serving network, or by an encrypted permanent identity. To avoid user traceability, which may lead to the compromise of user identity confidentiality, the user should not be identified for a long period by means of the same temporary or encrypted identity. To achieve these security features, in addition it is required that any signalling or user data that might reveal the user's identity is ciphered on the radio access link.

Clause 6.1 describes a mechanism that allows a user to be identified on the radio path by means of a temporary identity by which he is known in the visited serving network. This mechanism should normally be used to identify a user on the

radio path in location update requests, service requests, detach requests, connection re-establishment requests, etc..

## 5.1.2 Entity authentication

The following security features related to entity authentication are provided:

- **authentication mechanism agreement:** the property that the user and the serving network can securely negotiate the mechanism for authentication and key agreement that they shall use subsequently;
- **user authentication:** the property that the serving network corroborates the user identity of the user;
- **network authentication:** the property that the user corroborates that he is connected to a serving network that is authorised by the user's HE to provide him services; this includes the guarantee that this authorisation is recent.

To achieve these objectives, it is assumed that entity authentication should occur at each connection set-up between the user and the network. Two mechanisms have been included: an authentication mechanism using an authentication vector delivered by the user's HE to the serving network, and a local authentication mechanism using the integrity key established between the user and serving network during the previous execution of the authentication and key establishment procedure.

Clause 6.3 describes an authentication and key establishment mechanism that achieves the security features listed above and in addition establishes a secret cipher key (see 5.1.3) and integrity key (see 5.1.4) between the user and the serving network. This mechanism should be invoked by the serving network after a first registration of a user in a serving network and after a service request, location update request, attach request, detach request or connection re-establishment request, when the maximum number of local authentications using the derived integrity key have been conducted.

Clause 6.5 describes the local authentication mechanism. The local authentication mechanism achieves the security features user authentication and network authentication and uses an integrity key established between user and serving network during the previous execution of the authentication and key establishment procedure. This mechanism should be invoked by the serving network after a service request, location update request, attach request, detach request or connection re-establishment request, provided that the maximum number of local authentications using the same derived integrity key has not been reached yet.

## 5.1.3 Confidentiality

The following security features are provided with respect to confidentiality of data on the network access link:

- **cipher algorithm agreement:** the property that the MS and the SN can securely negotiate the algorithm that they shall use subsequently;
- **cipher key agreement:** the property that the MS and the SN agree on a cipher key that they may use subsequently;
- **confidentiality of user data:** the property that user data cannot be overheard on the radio access interface;
- **confidentiality of signalling data:** the property that signalling data cannot be overheard on the radio access interface;

Cipher key agreement is realised in the course of the execution of the mechanism for authentication and key agreement (see 6.3). Cipher algorithm agreement is realised by means of a mechanism for security mode negotiation between the user and the network (see 6.6.9). This mechanism also enables the selected ciphering algorithm and the agreed cipher key to be applied in the way described in 6.6.

## 5.1.4 Data integrity

The following security features are provided with respect to integrity of data on the network access link:

- **integrity algorithm agreement:** the property that the MS and the SN can securely negotiate the integrity algorithm that they shall use subsequently;
- **integrity key agreement:** the property that the MS and the SN agree on an integrity key that they may use subsequently;

- **data integrity and origin authentication of signalling data:** the property that the receiving entity (MS or SN) is able to verify that signalling data has not been modified in an unauthorised way since it was sent by the sending entity (SN or MS) and that the data origin of the signalling data received is indeed the one claimed;

Integrity key agreement is realised in the course of the execution of the mechanism for authentication and key agreement (see 6.3). Integrity algorithm agreement is realised by means of a mechanism for security mode negotiation between the user and the network (see 6.6.9). This mechanism also enables the selected integrity algorithm and the agreed integrity key to be applied in the way described in 6.4.

### 5.1.5 Mobile equipment identification

NOTE: In certain cases, SN may request the MS to send it the mobile equipment identity of the terminal. The mobile equipment identity shall only be sent after authentication of SN with exception of emergency calls. The IMEI should be securely stored in the terminal. However, the presentation of this identity to the network is not a security feature and the transmission of the IMEI is not protected. Although it is not a security feature, it should not be deleted from UMTS however, as it is useful for other purposes.

## 5.2 Network domain security

### 5.2.1 Void

### 5.2.2 Void

### 5.2.3 Void

### 5.2.4 Fraud information gathering system

NOTE: Some feature will be provided which will allow fraud information to be exchanged between 3GMS providers according to time constraints that yet have to be defined.

## 5.3 User domain security

### 5.3.1 User-to-USIM authentication

This feature provides the property that access to the USIM is restricted until the USIM has authenticated the user. Thereby, it is ensured that access to the USIM can be restricted to an authorised user or to a number of authorised users. To accomplish this feature, user and USIM must share a secret (e.g. a PIN) that is stored securely in the USIM. The user gets access to the USIM only if he/she proves knowledge of the secret.

This security feature is implemented by means of the mechanism described in [21].

### 5.3.2 USIM-Terminal Link

This feature ensures that access to a terminal or other user equipment can be restricted to an authorised USIM. To this end, the USIM and the terminal must share a secret that is stored securely in the USIM and the terminal. If a USIM fails to prove its knowledge of the secret, it will be denied access to the terminal.

This security feature is implemented by means of the mechanism described in [15].

## 5.4 Application security

### 5.4.1 Secure messaging between the USIM and the network

It is expected that 3GMS will provide the capability for operators or third party providers to create applications which are resident on the USIM (similar to SIM Application Toolkit in GSM). There exists a need to secure messages which are transferred over the 3GMS network to applications on the USIM, with the level of security chosen by the network operator or the application provider.

The following security features are provided with respect to protecting messages transferred to applications on the USIM over the 3GMS network:

- **Entity authentication of applications:** the property that two applications are able to corroborate each other's identity.
- **Data origin authentication of application data:** the property that the receiving application is able to verify the claimed data origin of the application data received;
- **Data integrity of application data:** the property that the receiving application is able to verify that application data has not been modified since it was sent by the sending application;
- **Replay detection of application data:** the property that an application is able to detect that the application data that it receives is replayed;
- **Sequence integrity of application data:** the property that an application is able to detect that the application data that it receives is received in sequence;
- **Proof of receipt:** the property that the sending application can proof that the receiving application has received the application data sent.
- **Confidentiality of application data:** the property that application data is not disclosed to unauthorised parties.

NOTE: It is assumed that these security features will be based on GSM SIM Application Toolkit security features. Further work is required to identify what enhancements need to be made to SIM Application Toolkit security. Possible areas of enhancement may include: key management support, enhancement of security mechanisms/features, increased flexibility in algorithm choice and security parameter size. A joint 3GPP TSG-SA 'Security'/3GPP TSG-T 'USIM' working group may be required to progress this issue.

### 5.4.2 Void

### 5.4.3 Access to user profile data

[ffs]

### 5.4.4 IP security

[ffs]

## 5.5 Security visibility and configurability

### 5.5.1 Visibility

Although in general the security features should be transparent to the user, for certain events and according to the user's concern, greater user visibility of the operation of security features should be provided. This yields to a number of features that inform the user of security-related events, such as:

- indication of access network encryption: the property that the user is informed whether the confidentiality of user



data is protected on the radio access link, in particular when non-ciphered calls are set-up;

- indication of the level of security: the property that the user is informed on the level of security that is provided by the visited network, in particular when a user is handed over or roams into a network with lower security level (3G → 2G).

## 5.5.2 Configurability

Configurability is the property that that the user and the user's HE can configure whether the use or the provision of a service should depend on whether a security feature is in operation. A service can only be used if all security features, which are relevant to that service and which are required by the configurations of the user or of the user's HE, are in operation. The following configurability features are suggested:

- Enabling/disabling user-USIM authentication: the user and/or user's HE should be able to control the operation of user-USIM authentication, e.g., for some events, services or use.
- Accepting/Rejecting incoming non-ciphered calls: the user and/or user's HE should be able to control whether the user accepts or rejects incoming non-ciphered calls;
- Setting up or not setting-up non-ciphered calls: the user and/or user's HE should be able to control whether the user sets up connections when ciphering is not enabled by the network;
- Accepting/rejecting the use of certain ciphering algorithms: the user and/or user's HE should be able to control which ciphering algorithms are acceptable for use.

---

# 6 Network access security mechanisms

## 6.1 Identification by temporary identities

### 6.1.1 General

This mechanism allows the identification of a user on the radio access link by means of a temporary mobile subscriber identity (TMSI/P-TMSI). A TMSI /P-TMSI has local significance only in the location area or routing area in which the user is registered. Outside that area it should be accompanied by an appropriate Location Area Identification (LAI) or Routing Area Identification (RAI) in order to avoid ambiguities. The association between the permanent and temporary user identities is kept by the Visited Location Register (VLR/SGSN) in which the user is registered.

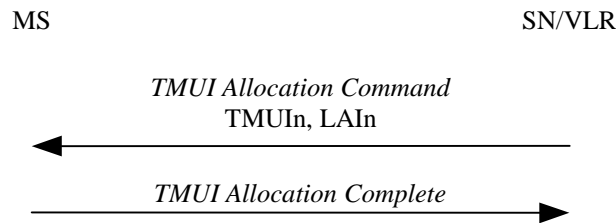
The TMSI/P-TMSI, when available, is normally used to identify the user on the radio access path, for instance in paging requests, location update requests, attach requests, service requests, connection re-establishment requests and detach requests.

The procedures and mechanisms are described in GSM 03.20 and TS 23.060. The following subclauses contain a summary of this feature.

### 6.1.2 TMUI reallocation procedure

The purpose of the mechanism described in this subsection is to allocate a new TMUI/LAI pair to a user by which he may subsequently be identified on the radio access link.

The procedure should be performed after the initiation of ciphering. The ciphering of communication over the radio path is specified in clause 6.6. The allocation of a temporary identity is illustrated in Figure 3.



**Figure 3: TMSI allocation**

The allocation of a temporary identity is initiated by the VLR.

The VLR generates a new temporary identity (TMUIIn) and stores the association of TMUIIn and the permanent identity IMUI in its database. The TMUI should be unpredictable. The VLR then sends the TMUIIn and (if necessary) the new location area identity LAIn to the user.

Upon receipt the user stores TMUIIn and automatically removes the association with any previously allocated TMUI. The user sends an acknowledgement back to the VLR.

Upon receipt of the acknowledgement the VLR removes the association with the old temporary identity TMUIo and the IMUI (if there was any) from its database.

### 6.1.3 Unacknowledged allocation of a temporary identity

If the serving network does not receive an acknowledgement of the successful allocation of a temporary identity from the user, the network shall maintain the association between the new temporary identity TMUIIn and the IMUI and between the old temporary identity TMUIo (if there is any) and the IMUI.

For a user-originated transaction, the network shall allow the user to identify itself by either the old temporary identity TMUIo or the new temporary identity TMUIIn. This allows the network to determine the temporary identity stored in the mobile station. The network shall subsequently delete the association between the other temporary identity and the IMUI, to allow the temporary identity to be allocated to another user.

For a network-originated transaction, the network shall identify the user by its permanent identity (IMUI). When radio contact has been established, the network shall instruct the user to delete any stored TMUI. When the network receives an acknowledgement from the user, the network shall delete the association between the IMUI and any TMUI to allow the released temporary identities to be allocated to other users.

Subsequently, in either of the cases above, the network may initiate the normal TMUI reallocation procedure.

Repeated failure of TMUI reallocation (passing a limit set by the operator) may be reported for O&M action.

### 6.1.4 Location update

In case a user identifies itself using a TMUIo/LAIo pair that was assigned by the visited VLRn the IMUI can normally be retrieved from the database. If this is not the case, the visited VLRn should request the user to identify itself by means of its permanent user identity. This mechanism is described in 6.2.

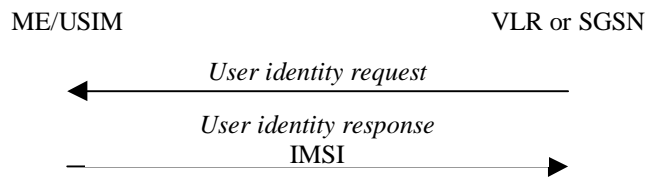
In case a user identifies itself using a TMUIo/LAIo pair that was not assigned by the visited VLRn and the visited VLRn and the previously visited VLRO exchange authentication data, the visited VLRn should request the previously visited VLRO to send the permanent user identity. This mechanism is described in 6.3.4, it is integrated in the mechanism for distribution of authentication data between VLRs. If the previously visited VLRO cannot be contacted or cannot retrieve the user identity, the visited VLRn should request the user to identify itself by means of its permanent user identity. This mechanism is described in 6.2.

## 6.2 Identification by a permanent identity

The mechanism described in here allows the identification of a user on the radio path by means of the permanent subscriber identity (IMSI).

The mechanism should be invoked by the serving network whenever the user cannot be identified by means of a temporary identity. In particular, it should be used when the user registers for the first time in a serving network, or when the serving network cannot retrieve the IMSI from the TMSI by which the user identifies itself on the radio path.

The mechanism is illustrated in Figure 4.



**Figure 4: Identification by the permanent identity**

The mechanism is initiated by the visited VLR or SGSN that requests the user to send its permanent identity. The user's response contains the IMSI in cleartext. This represents a breach in the provision of user identity confidentiality.

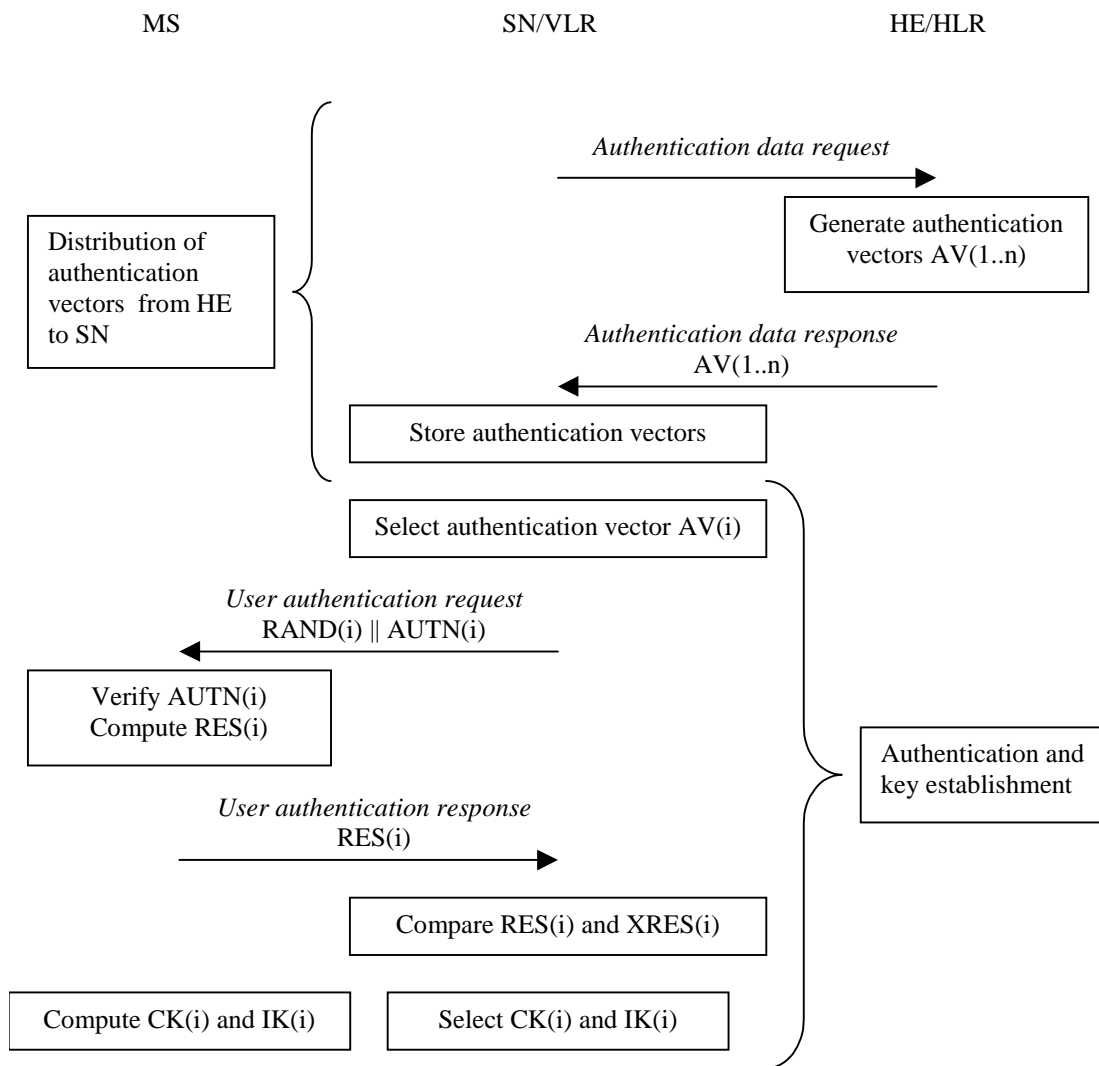
## 6.3 Authentication and key agreement

### 6.3.1 General

The mechanism described here achieves mutual authentication by the user and the network showing knowledge of a secret key  $K$  which is shared between and available only to the USIM and the AuC in the user's HE. In addition the USIM and the HE keep track of counters  $SEQ_{MS}$  and  $SEQ_{HE}$  respectively to support network authentication.

The method was chosen in such a way as to achieve maximum compatibility with the current GSM security architecture and facilitate migration from GSM to UMTS. The method is composed of a challenge/response protocol identical to the GSM subscriber authentication and key establishment protocol combined with a sequence number-based one-pass protocol for network authentication derived from the ISO standard ISO/IEC 9798-4 (section 5.1.1).

An overview of the mechanism is shown in Figure 5.



**Figure 5: Authentication and key agreement**

Upon receipt of a request from the VLR/SGSN, the HE/AuC sends an ordered array of  $n$  authentication vectors (the equivalent of a GSM "triplet") to the VLR/SGSN. Each authentication vector consists of the following components: a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each authentication vector is good for one authentication and key agreement between the VLR/SGSN and the USIM.

When the VLR/SGSN initiates an authentication and key agreement, it selects the next authentication vector from the array and sends the parameters RAND and AUTN to the user. The USIM checks whether AUTN can be accepted and, if so, produces a response RES which is sent back to the VLR/SGSN. The USIM also computes CK and IK. The VLR/SGSN compares the received RES with XRES. If they match the VLR/SGSN considers the authentication and key agreement exchange to be successfully completed. The established keys CK and IK will then be transferred by the USIM and the VLR/SGSN to the entities which perform ciphering and integrity functions.

VLR/SGSNs can offer secure service even when HE/AuC links are unavailable by allowing them to use previously derived cipher and integrity keys for a user so that a secure connection can still be set up without the need for an authentication and key agreement. Authentication is in that case based on a shared integrity key, by means of data integrity protection of signalling messages (see 6.4).

The authenticating parties shall be the AuC of the user's HE (HE/AuC) and the USIM in the user's mobile station. The mechanism consists of the following procedures:

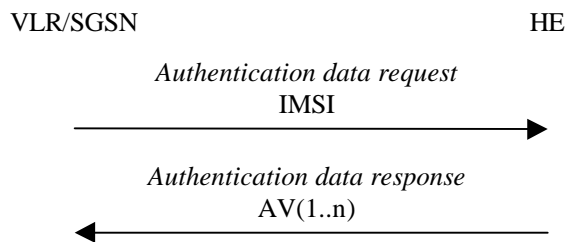
A procedure to distribute authentication information from the HE/AuC to the VLR/SGSN. This procedure is described in 6.3.2. The VLR/SGSN is assumed to be trusted by the user's HE to handle authentication information securely. It is also assumed that the intra-system links between the VLR/SGSN to the HE/AuC are adequately secure. It is further assumed that the user trusts the HE.

A procedure to mutually authenticate and establish new cipher and integrity keys between the VLR/SGSN and the MS. This procedure is described in 6.3.3.

A procedure to distribute authentication data from a previously visited VLR to the newly visited VLR. This procedure is described in 6.3.4. It is also assumed that the links between VLR/SGSNs are adequately secure.

### 6.3.2 Distribution of authentication data from HE to SN

The purpose of this procedure is to provide the VLR/SGSN with an array of fresh authentication vectors from the user's HE to perform a number of user authentications.



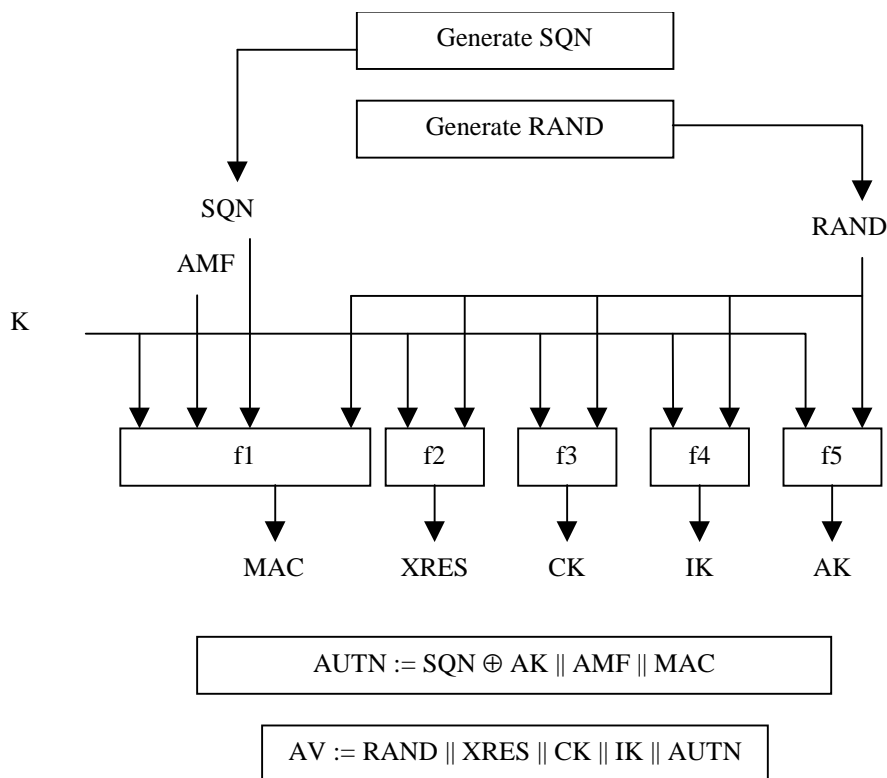
**Figure 6: Distribution of authentication data from HE to VLR/SGSN**

The VLR/SGSN invokes the procedures by requesting authentication vectors to the HE/AuC.

The *authentication data request* shall include the IMSI.

Upon the receipt of the *authentication data request* from the VLR/SGSN, the HE may have pre-computed the required number of authentication vectors and retrieve them from the HLR database or may compute them on demand. The HE/AuC sends an authentication response back to the VLR/SGSN that contains an ordered array of n authentication vectors AV(1..n).

Figure 7 shows the generation of an authentication vector AV by the HE/AuC.



**Figure 7: Generation of authentication vectors**

The HE/AuC starts with generating a fresh sequence number SQN and an unpredictable challenge RAND.

For each user the HE/AuC keeps track of a counter:  $SQN_{HE}$

The HE has some flexibility in the management of sequence numbers, but some requirements need to be fulfilled by the mechanism used:

- a) The generation mechanism shall allow a re-synchronisation procedure in the HE described in section 6.3.5
- b) In case the SQN exposes the identity and location of the user, the AK may be used as an anonymity key to conceal it.
- c) The generation mechanism shall allow protection against wrap around the counter in the USIM.  
A method how to achieve this is given in informative Annex C.2.

The mechanisms for verifying the freshness of sequence numbers in the USIM shall to some extent allow the out-of-order use of sequence numbers. This is to ensure that the authentication failure rate due to synchronisation failures is sufficiently low. This requires the capability of the USIM to store information on past successful authentication events (e.g. sequence numbers or relevant parts thereof). The mechanism shall ensure that a sequence number can still be accepted if it is among the last  $x = 50$  sequence numbers generated. This shall not preclude that a sequence number is rejected for other reasons such as a limit on the age for time-based sequence numbers.

The same minimum number  $x$  needs to be used across the systems to guarantee that the synchronisation failure rate is sufficiently low under various usage scenarios, in particular simultaneous registration in the CS- and the PS-service domains, user movement between VLRs/SGSNs which do not exchange authentication information, super-charged networks.

The use of  $SEQ_{HE}$  is specific to the method of generation sequence numbers. A method is specified in Annex C.1 how to generate a fresh sequence number. A method is specified in Annex C.2 how to verify the freshness of a sequence number.

An authentication and key management field AMF is included in the authentication token of each authentication vector. Example uses of this field are included in Annex F.

Subsequently the following values are computed:

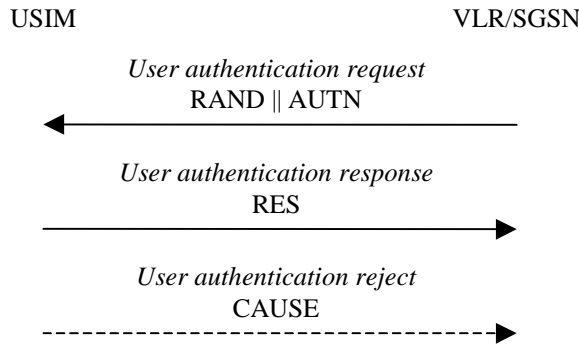
- a message authentication code  $MAC = f1_K(SQN \parallel RAND \parallel AMF)$  where  $f1$  is a message authentication function;
- an expected response  $XRES = f2_K(RAND)$  where  $f2$  is a (possibly truncated) message authentication function;
- a cipher key  $CK = f3_K(RAND)$  where  $f3$  is a key generating function;
- an integrity key  $IK = f4_K(RAND)$  where  $f4$  is a key generating function;
- an anonymity key  $AK = f5_K(RAND)$  where  $f5$  is a key generating function or  $f5 \equiv 0$ .

Finally the authentication token  $AUTN = SQN \oplus AK \parallel AMF \parallel MAC$  is constructed.

Here, AK is an anonymity key used to conceal the sequence number as the latter may expose the identity and location of the user. The concealment of the sequence number is to protect against passive attacks only. If no concealment is needed then  $f5 \equiv 0$  ( $AK = 0$ ).

### 6.3.3 Authentication and key agreement

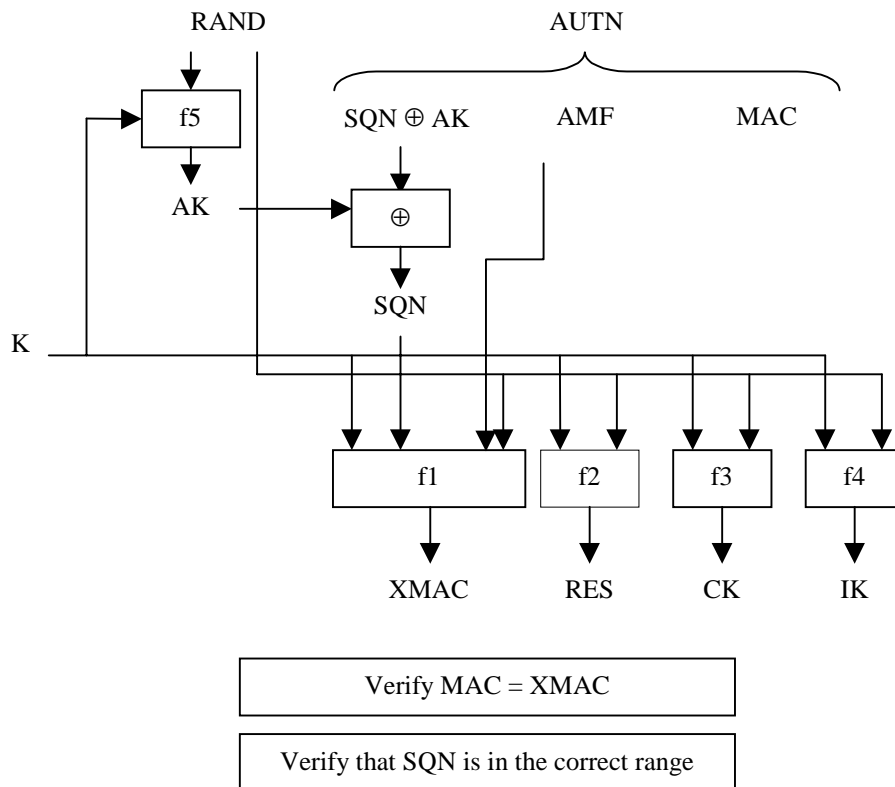
The purpose of this procedure is to authenticate the user and establish a new pair of cipher and integrity keys between the VLR/SGSN and the USIM. During the authentication, the USIM verifies the freshness of the authentication vector that is used.



**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  $SQN = (SQN \oplus AK) \oplus AK$ .

Next the USIM computes  $XMAC = f1_K (SQN \parallel RAND \parallel AMF)$  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.

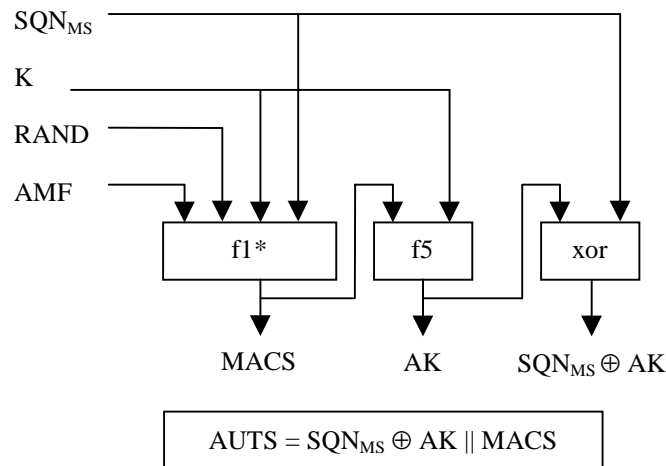
Next the USIM verifies that the received sequence number SQN is in the correct range.

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  $AUTS = Conc(SQN_{MS}) \parallel MAC-S$ .  $Conc(SQN_{MS}) = SQN_{MS} \oplus f5_K(MAC-S \parallel 0\dots0)$  is the concealed value of the counter  $SEQ_{MS}$  in the MS, and  $MAC-S = f1^*_K(SEQ_{MS} \parallel RAND \parallel AMF)$  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  $f1, \dots, f5$  and vice versa.

The AMF used to calculate MAC-S 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 is 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 conversion function c3, it shall derive the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK. 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.

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.

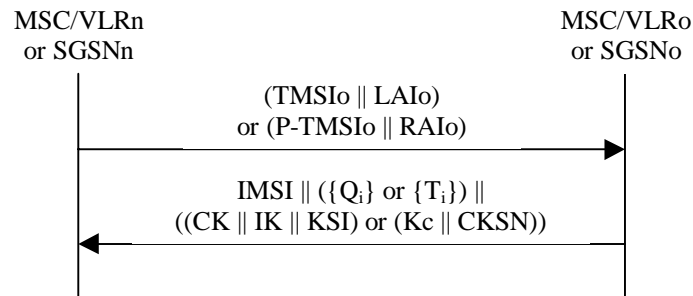
**Conditions on the use of authentication information by the VLR/SGSN:** The VLR/SGSN shall use a UMTS authentication vector (i.e. a quintuplet) only once and, hence, shall send out each user authentication request *RAND // AUTN* only once no matter whether the authentication attempt was successful or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



### 6.3.4 Distribution of IMSI and temporary authentication data within one serving network domain

The purpose of this procedure is to provide a newly visited MSC/VLR or SGSN with temporary authentication data from a previously visited MSC/VLR or SGSN within the same serving network domain.

The procedure is shown in Figure 11.



**Figure 11: Distribution of IMSI and temporary authentication data within one serving network domain**

The procedure shall be invoked by the newly visited MSC/VLRn (resp. SGSNn) after the receipt of a location update request (resp. routing area update request) from the user wherein the user is identified by means of a temporary user identity TMSIo (resp. P-TMSIo) and the location area identity LAIo (resp. routing area identity RAIo) under the jurisdiction of a previously visited MSC/VLRo or SGSNo that belongs to the same serving network domain as the newly visited MSC/VLRn or SGSNn.

The protocol steps are as follows:

- a) The MSC/VLRn (resp. SGSNn) sends a *user identity request* to the MSC/VLRo (or SGSNo), this message contains TMSIo and LAIo (resp. P-TMSIo and RAIo).
- b) The MSC/VLRo (resp. SGSNo) searches the user data in the database.

If the user is found, the MSC/VLRo (resp. SGSNo) shall send a *user identity response* back that

- i) shall include the IMSI,
- ii) may include a number of unused authentication vectors (quintets or triplets) and
- iii) may include the current security context data: CK, IK and KSI (UMTS) or Kc and CKSN (GSM).

The MSC/VLRo or SGSNo subsequently deletes the authentication vectors which have been sent and the data elements on the current security context.

If the user cannot be identified the MSC/VLRo or SGSNo shall send a *user identity response* indicating that the user identity cannot be retrieved.

- c) If the MSC/VLRn or SGSNn receives a *user identity response* with an IMSI, it creates an entry and stores any authentication vectors and any data on the current security context that may be included.

If the MSC/VLRn or SGSNn receives a *user identity response* indicating that the user could not be identified, it shall initiate the user identification procedure described in 6.2.



### 6.3.5 Re-synchronisation procedure

A VLR/SGSN may send two types of *authentication data requests* to the HE/AuC, the (regular) one described in subsection 6.3.2 and one used in case of synchronisation failures, described in this subsection.

Upon receiving a *synchronisation failure* message from the user, the VLR/SGSN sends an *authentication data request* with a "*synchronisation failure indication*" to the HE/AuC, together with the parameters

- *RAND* sent to the MS in the preceding user authentication request and
- *AUTS* received by the VLR/SGSN in the response to that request, as described in subsection 6.3.3.

An VLR/SGSN will not react to unsolicited "*synchronisation failure indication*" messages from the MS.

The VLR/SGSN does not send new user authentication requests to the user before having received the response to its authentication data request from the HE/AuC (or before it is timed out).

When the HE/AuC receives an *authentication data request* with a "*synchronisation failure indication*" it acts as follows:

1. The HE/AuC retrieves  $SEQ_{MS}$  from  $Conc(SEQ_{MS})$  by computing  $f5_k(MAC-S // 0...0)$ .
2. The HE/AuC checks if  $SEQ_{HE}$  is in the correct range, i.e. if the next sequence number generated  $SEQ_{HE}$  using would be accepted by the USIM.
3. If  $SEQ_{HE}$  is in the correct range then the HE/AuC continues with step (6), otherwise it continues with step (4).
4. The HE/AuC verifies *AUTS* (cf. subsection 6.3.3.).
5. If the verification is successful the HE/AuC resets the value of the counter  $SEQ_{HE}$  to  $SEQ_{MS}$ .
6. The HE/AuC sends an *authentication data response* with a new batch of authentication vectors to the VLR/SGSN. If the counter  $SEQ_{HE}$  was not reset then these authentication vectors can be taken from storage, otherwise they are newly generated after resetting  $SEQ_{HE}$ . In order to reduce the real-time computation burden on the HE/AuC, the HE/AuC may also send only a single authentication vector in the latter case.

Whenever the VLR/SGSN receives a new batch of authentication vectors from the HE/AuC in an authentication data response to an authentication data request with synchronisation failure indication it deletes the old ones for that user in the VLR/SGSN.

The user may now be authenticated based on a new authentication vector from the HE/AuC. Figure 12 shows how re-synchronisation is achieved by combining a *user authentication request* answered by a *synchronisation failure* message (as described in subclause 6.3.3) with an *authentication data request* with *synchronisation failure* indication answered by an *authentication data response* (as described in this subclause).

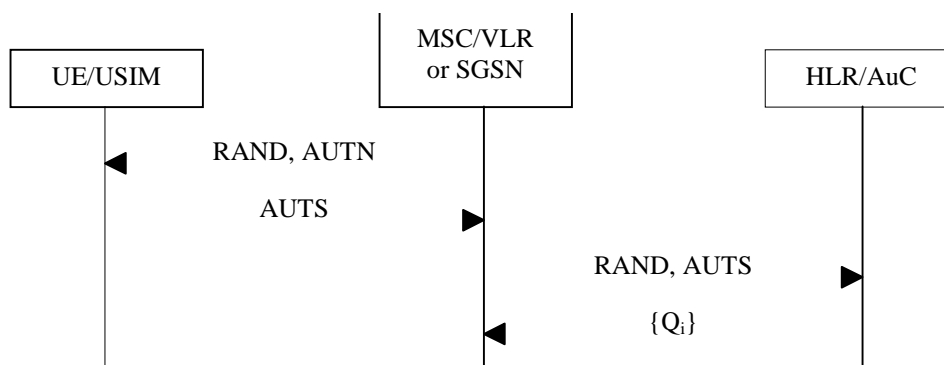
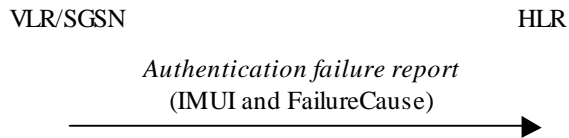


Figure 12: Resynchronization mechanism

### 6.3.6 Reporting authentication failures from the SGSN/VLR to the HLR

The purpose of this procedure is to provide a mechanism for reporting authentication failures from the serving environment back to the home environment.

The procedure is shown in Figure 13.



**Figure 13: Reporting authentication failure from VLR/SGSN to HLR**

The procedure is invoked by the serving network VLR/SGSN when the authentication procedure fails. The *authentication failure report* shall contain the subscriber identity and a failure cause code. The possible failure causes are either that the network signature was wrong or that the user response was wrong.

The HE may decide to cancel the location of the user after receiving an *authentication failure report*.

### 6.3.7 Length of sequence numbers

Sequence numbers shall have a length of 6 octets.

## 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 ME as part of the security mode set-up procedure (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 network have no versions of the UIA algorithm in common, then the connection shall be released.
- 2) If the MS and the network 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 no versions of the UEA algorithm in common and the user (respectively the user's HE) and the network are willing to use an unciphered connection, then an unciphered connection shall be used.
- 3) 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.

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 values  $START_{CS}$  and  $START_{PS}$  of the bearers that were protected in that RRC connection are stored in the USIM. When the next RRC connection is established that values are read from the USIM.

The ME shall trigger the generation of a new access link key set (a cipher key and an integrity key) if  $START_{CS}$  or  $START_{PS}$  reach 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

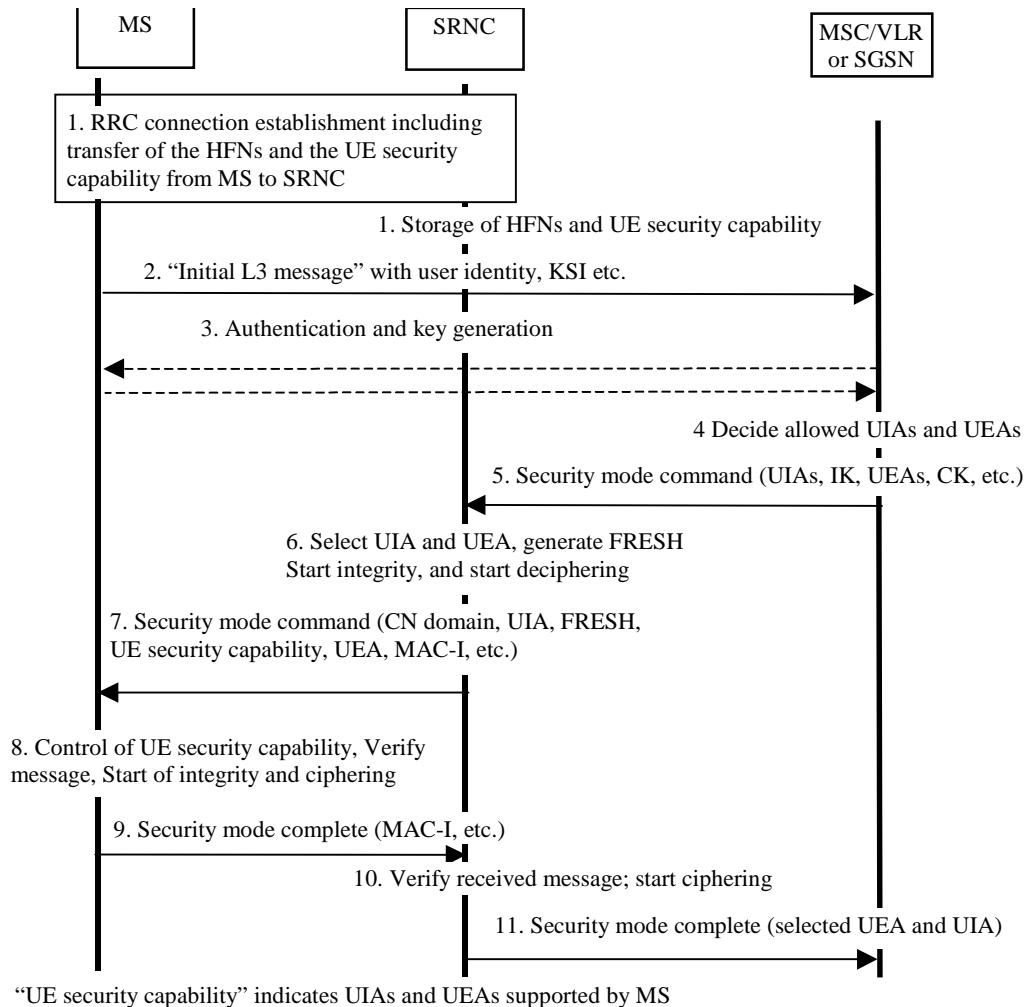
This section describes one common procedure for both ciphering and integrity protection set-up. It is mandatory to start integrity protection of signalling messages by use of this procedure at each new signalling connection establishment between MS and MSC/VLR respective SGSN. The three exceptions when 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.



**Figure 14: Local authentication and connection set-up**

NOTE 1: The network must have the "ME security capability" information before the integrity protection can start, i.e. the "ME security capability" must be sent to the network in an unprotected message. Returning the "ME security capability" later on to the ME in a protected message will give ME the possibility to verify that it was the correct "ME security capability" that reached the network.

Detailed description of the flow above:

1. RRC connection establishment includes the transfer from MS to RNC of the ME security capability and the initial hyperframe numbers (HFN) for the CS service domain respective the PS service domain. The UE security capability information includes the ciphering capabilities (UEAs) and the integrity capabilities (UIAs) of the MS. The initial HFN is used to initialise the HFN to be used as part of one of the input parameters COUNT-I for the integrity algorithm and COUNT-C, for the ciphering algorithm. The initial HFNs and the UE security capability information are 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 MSC/VLR or SGSN. This message contains e.g. the user identity and the KSI. The included KSI (Key Set Identifier) is the KSI allocated by the CS service domain or PS service domain at the last authentication for this CN domain.
3. User identity request may be performed (see 6.2). Authentication of the user and generation of new security keys (IK and CK) may be performed (see 6.3.3). A new KSI will then also be allocated.
4. The MSC/VLR or SGSN determines which UIAs and UEAs that are allowed to be used.
5. The MSC/VLR or SGSN initiates integrity and 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. If ciphering shall be started, it contains the allowed UEAs and the CK to be used. If a new authentication and security key generation

has been performed (see 3 above), this shall be indicated in the message sent to the SRNC. The indication of new generated keys implies that the initial HFN to be used shall be reset (i.e. set to zero) at start use of the new keys. Otherwise, it is the HFN already available in the SRNC that shall be used (see 1. above).

6. The SRNC decides which algorithms to use by selecting from the list of allowed algorithms, and the list of algorithms supported by the MS (see 6.4.2). The SRNC generates a random value FRESH and initiates the downlink integrity protection. If the requirements received in the Security mode command can not be fulfilled, the SRNC sends a SECURITY MODE REJECT message to the requesting MSC/VLR or SGSN. The further actions are described in 6.4.2.
7. The SRNC generates the RRC message Security mode command. The message includes the ME security capability, the UIA and FRESH to be used and if ciphering shall be started also the UEA to be used. Additional information (start of ciphering) may also be included. Because of that the MS can have two ciphering and integrity key sets, the network must indicate which key set to use. This is obtained by including a CN type indicator information in the Security mode command message. 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 mode command message, the MS controls that the ME security capability received is equal to the 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 mode complete and generates the MAC-I for this message. If any control is not successful, the procedure ends in 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 MSC/VLR or SGSN ends the procedure.

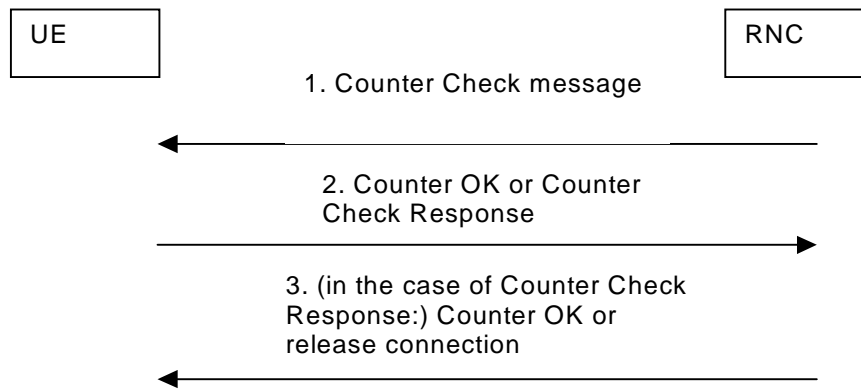
The Security mode command to MS starts the downlink integrity protection, i.e. also all following downlink messages sent to the MS are integrity protected and possibly ciphered. The Security mode complete from MS starts the uplink integrity protection and possible ciphering, i.e. also all following messages 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 ME. The RNC is monitoring the COUNT-C and COUNT-I 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.



**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 ME and if they agree with the current status in the ME, a 'Counter OK' message is returned to the RNC. If there is a difference between the counter values in the ME and the values indicated in the Counter Check message, the 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.

## 6.4.8 Initialisation of synchronisation for ciphering and integrity protection

The ciphering and integrity protection algorithms are driven by counters (COUNT-C and COUNT-I) that at connection establishment need to be initialised. For that purpose the ME and the USIM have the ability to store a START value. The ME and the USIM store a START<sub>CS</sub> value for the CS cipher/integrity keys and a START<sub>PS</sub> value for the PS cipher/integrity keys. The length of START is 20 bits.

The ME only contains (valid) START values when it is powered-on and a USIM is inserted. When the ME is powered-off or the USIM is removed, the ME deletes its START values. After power-on or insertion of a USIM, the USIM sends its START values to the ME, and the ME stores them. During idle mode, the START values in the ME and in the USIM are identical and static.

At radio connection establishment for a particular serving network domain (CS or PS) the ME sends the START<sub>CS</sub> and the START<sub>PS</sub> value to the RNC in the *RRC connection setup complete* message. The ME marks the START values in the USIM as invalid by setting START<sub>CS</sub> and START<sub>PS</sub> to THRESHOLD.

The ME and the RNC initialise the 20 most significant bits of the RRC HFN (for integrity protection), the RLC HFN (for ciphering) and the MAC-d HFN (for ciphering) to the START value of the corresponding service domain; the remaining bits are initialised to 0. Also the RRC SN (for integrity protection), the RLC SN (for ciphering) and the MAC-d HFN (for ciphering) are initialised to 0.

During an ongoing radio connection, the START<sub>CS</sub> value in the ME is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling and CS user data logical channels protected using CK<sub>CS</sub> and/or IK<sub>CS</sub>, incremented by 1, i.e.:

$$\text{START}_{\text{CS}} = \text{MSB}_{20} (\text{MAX} \{ \text{COUNT-C}, \text{COUNT-I} \mid \text{all logical channels protected with CK}_{\text{CS}} \text{ and IK}_{\text{CS}} \}) + 1.$$

Likewise, during an ongoing radio connection, the START<sub>PS</sub> value in the ME is defined as the 20 most significant bits of the maximum of all current COUNT-C and COUNT-I values for all signalling and PS user data logical channels protected using CK<sub>PS</sub> and/or IK<sub>PS</sub>, incremented by 1, i.e.:



$$\text{START}_{\text{PS}} = \text{MSB}_{20} (\text{MAX} \{ \text{COUNT-C}, \text{COUNT-I} \mid \text{all logical channels protected with CK}_{\text{PS}} \text{ and IK}_{\text{PS}} \}) + 1.$$

Upon radio connection release and when a set of cipher/integrity keys is no longer used, the ME updates  $\text{START}_{\text{CS}}$  and  $\text{START}_{\text{PS}}$  in the USIM with the current values.

During authentication and key agreement the ME sets the  $\text{START}$  values of the corresponding service domain to 0 in the USIM and in the ME itself.

## 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 ME and the RNC.

After the RRC connection establishment and execution of the security mode set-up procedure, all dedicated MS  $\leftrightarrow$  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)
- Handover to UTRAN complete.

### 6.5.2 Layer of integrity protection

The UIA shall be implemented in the 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.

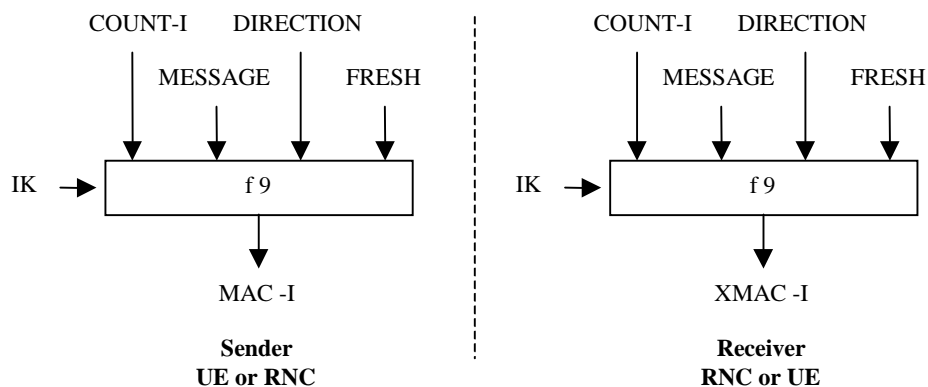


Figure 16: Derivation of MAC-I (or XMAC-I) on a signalling message

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.

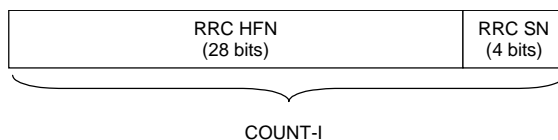
## 6.5.4 Input parameters to the integrity algorithm

### 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 ME to RNC during *RRC connection establishment*. The ME and the RNC then initialise the 20 most significant bits of the RRC HFN to START; the remaining bits of the RRC HFN are initialised to 0. The RRC HFN are incremented independently for each logical channel used for signalling.

### 6.5.4.2 IK

The integrity key IK is 128 bits long.

There may be one IK for CS connections (IK<sub>CS</sub>), established between the CS service domain and the user and one IK for PS connections (IK<sub>PS</sub>) 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 ME. IK is sent from the USIM to the ME upon request of the 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 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*.

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

#### 6.5.4.5 MESSAGE

The signalling message itself with the radio bearer identity. The latter is appended in front of the message. Note that the radio bearer identity is not transmitted with the message but it is needed to avoid that for different instances of message authentication codes the same set of input parameters is used.

### 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 follows 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<sub>2</sub>" : 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 identity (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 ME and the RNC.

## 6.6.2 Layer of ciphering

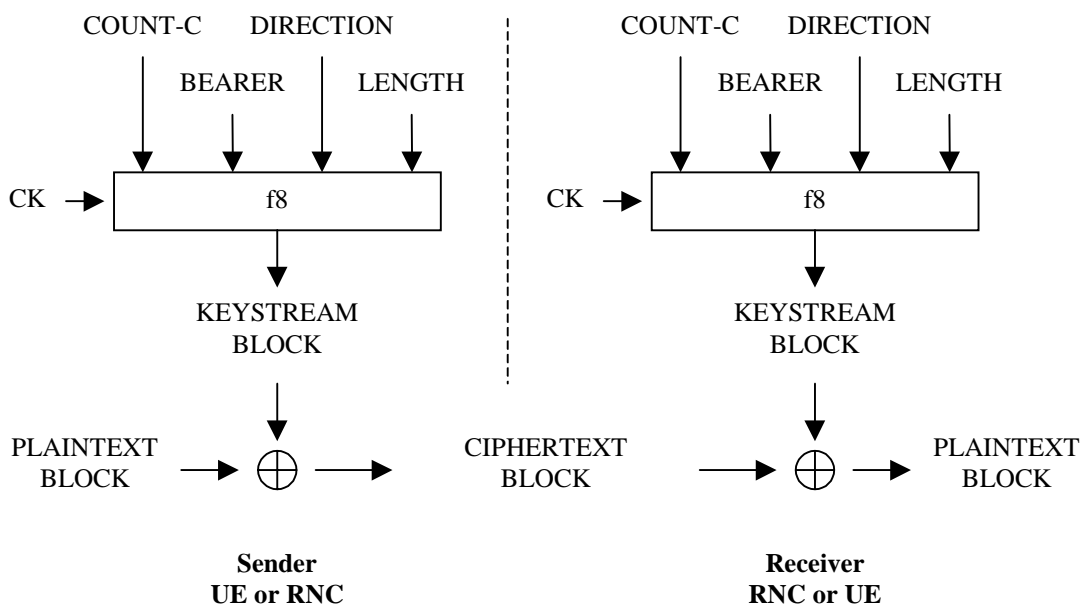
The ciphering function is performed either in the RLC sub-layer or in the MAC sub-layer, according to the following rules:

- 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 ME and the context needed for ciphering (CK, HFN, etc.) is only known in S-RNC and the 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.

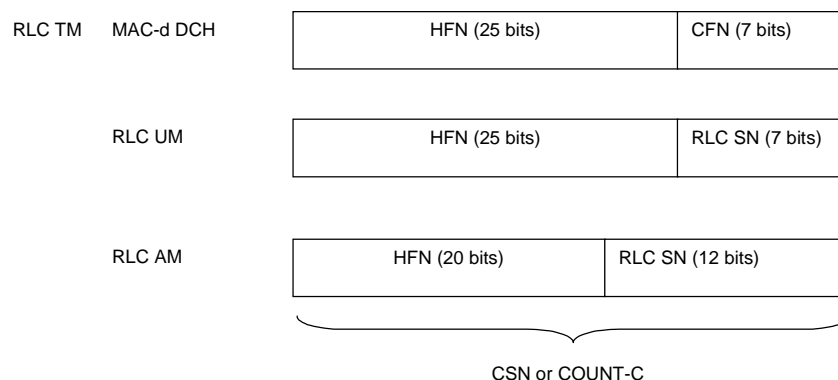
## 6.6.4 Input parameters to the cipher algorithm

### 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 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 ME to RNC in *RRC connection establishment*. The ME and the RNC then initialise the 20 most significant bits of the RLC HFN and MAC HFN to *START*; the remaining bits of the RLC HFN and MAC HFN are initialised to 0. The RRC HFN are incremented independently for each logical channel.

#### 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  $f_3$ , 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  $K_c$ , as described in 8.2.

CK is stored in the USIM and a copy is stored in the ME. CK is sent from the USIM to the ME upon request of the 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 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.

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 radio bearer identifier BEARER is 5 bits long.

There is one BEARER parameter per radio bearer associated with the same user and multiplexed on a single 10ms physical layer frame. The radio bearer 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. The value of the DIRECTION is 0 for messages from UE to RNC and 1 for messages from RNC to UE.

### 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 and 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<sub>2</sub>" : UEA0, no encryption.

"0001<sub>2</sub>" : UEA1, Kasumi.

The remaining values are not defined.

## 6.7 Void

## 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:

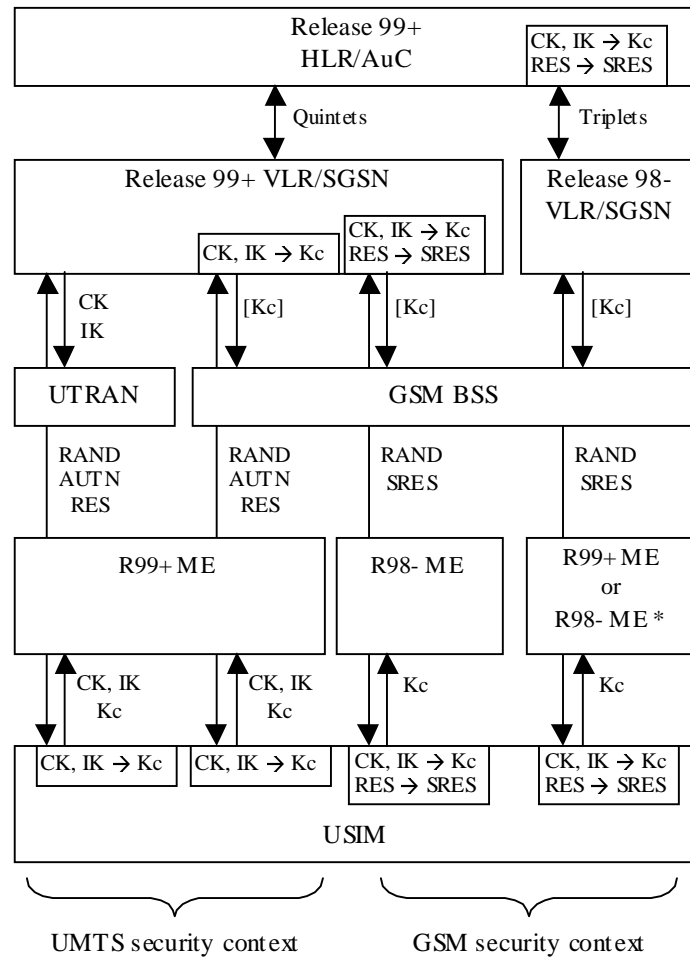
- UMTS AKA shall be applied when the user is attached to a UTRAN.
- UMTS AKA shall be applied when the user is attached to a GSM BSS, in case the user has R99+ ME and also the VLR/SGSN is R99+. In this case, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys CK and IK, by the VLR/SGSN 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- 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 operate within a R98- ME, the USIM may support the SIM-ME interface as defined in GSM 11.11, and support GSM AKA 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+ ME 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 and 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)  $c1: RAND_{[GSM]} = RAND$
- b)  $c2: SRES_{[GSM]} = XRES_1 [xor XRES_2 [xor XRES_3 [xor XRES_4]]]$
- c)  $c3: Kc_{[GSM]} = CK_1 xor CK_2 xor IK_1 xor IK_2$

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+ ME**

When the user has 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 the VLR/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+ ME independently of the radio access network.

- **UMTS subscriber with R98- ME**

When the user has 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- ME.

### 6.8.1.4 R99+ ME

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+ 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 ME. If the USIM supports conversion function c3 and/or GSM AKA, the 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 ME.

### 6.8.1.5 USIM

The USIM shall support UMTS AKA 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;
- Feature 2: GSM AKA 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.

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

When the ME provides the USIM with only RAND, and the USIM supports GSM AKA (Feature 2), GSM AKA shall be executed. The USIM first computes the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The USIM then derives the GSM user response SRES and the GSM cipher key Kc using the conversion functions c2 and c3. The 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 ME.

In case the USIM does not support GSM cipher key derivation (Feature 1) or GSM AKA (Feature 2), the R99+ ME shall be informed. A 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- 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 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+ ME in a mixed network architecture.



cipher key using the following conversion functions:

- a) c4:  $CK_{[UMTS]} = Kc \parallel Kc$ ;
- b) c5:  $IK_{[UMTS]} = Kc_1 \text{ xor } Kc_2 \parallel Kc \parallel Kc_1 \text{ xor } Kc_2$ ;

whereby in c5,  $Kc_i$  are both 32 bits long and  $Kc = Kc_1 \parallel Kc_2$ .

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+ ME

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 ME.

When the user is attached to a UTRAN, 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 ME release ( $R'99 \text{ ME} \leftarrow \rightarrow R'98 \text{ ME}$ ) when the user registers at VLRn/SGSNn.
- ii) Authentication data from VLRo includes  $Kc+CKSN$  but no unused AVs and the subscriber has a  $R'99 \text{ ME}$  (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- 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+ SGSNs 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. The RNC requests the MS to send the MS Classmark, which includes information on the GSM ciphering algorithm capabilities of the MS. The intersystem handover will imply a change of ciphering algorithm from a UEA to a GSM A5. The GSM BSS includes the selected GSM ciphering mode in the handover command message sent to the MS via the RNC.

The integrity protection of signalling messages is stopped at handover to GSM BSS.

The highest hyperframe number value reached for all signalling and user data bearers during the RRC connection shall be stored in the ME/USIM at handover to GSM BSS.

### 6.8.4.1 UMTS security context

A UMTS security context in UTRAN is only established for a UMTS subscriber with a 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 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+ 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 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 GSM BSS requests the MS to send the UMTS capability information, which includes information on the initial HFN and UMTS security capabilities of the MS. The intersystem handover will imply a change of ciphering algorithm from a GSM A5 to a UEA. The target UMTS RNC includes the selected UMTS ciphering mode in the handover to UTRAN command message sent to the MS via the GSM BSS.

The integrity protection of signalling messages shall be started immediately after that the intersystem handover from GSM BSS to UTRAN is completed. The Serving RNC will do this by initiating the RRC security mode control procedure when the first RRC message (i.e. the Handover to UTRAN complete message) has been received from the MS. The UE security capability information, that has been sent from MS to RNC via the GSM radio access and the system infrastructure before the actual handover execution, will then be included in the RRC Security mode command message sent to MS and then verified by the MS (i.e. verified that it is equal to the UE security capability information stored in the MS)

### 6.8.5.1 UMTS security context

A UMTS security context in GSM BSS is only established for UMTS subscribers with 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 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+ 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 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 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 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+ 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 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- ME, where intersystem change to UTRAN is not possible, or in case the user has a R99+ 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+ 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+ ME is coming from a R98-SGSN.

At the user side, in all cases, the 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 overwritten with a new CK, IK pair due to the new AKA.

---

## 7 Void

## 8 Application security mechanisms

### 8.1 Secure messaging between the USIM and the network

This clause will specify the structure of the secured messages in a general format so that they can be used over a variety of transport channels between an entity in a 3GMS network and an entity in the USIM. The sending/receiving entity in the 3GMS network and in the USIM are responsible for applying the security mechanisms to application messages as defined to provide the security features identified in 5.4.1.

Note: A joint 3GPP TSG-SA 'Security'/3GPP TSG-T 'USIM' working group may be required to progress this issue.



## 8.2 Void

## 8.3 Mobile IP security

The introduction of Mobile IP functionality for end users in 3G has no influence on the security architecture for 3G.

Mobile IP terminals may be equipped with security functionality independent of the 3G network access security in order to allow security functions outside the 3G network.

3G networks, supporting Mobile IP services, should support its inherent security functionality.

On the other hand, 3G network access security architecture can not be influenced or reduced by the Mobile IP option.

The Mobile IP security functionality must thus be separate from the 3G network access security and it is developed in an other forum, IETF.

## Annex A (informative): Requirements analysis

[In this part of the document we will address the question "do the features meet the requirements?"]

Annex B:  
Void

## Annex C (informative): Management of sequence numbers

This annex is devoted to the management of sequence numbers for the authentication and key agreement protocol.

### C.1 Generation of sequence numbers in the Authentication Centre

According to section 6.3 of this specification, authentication vectors are generated in the authentication centre (AuC) using sequence numbers. This section specifies how these sequence numbers are generated. It is taken into account that authentication vectors may be generated and sent by the AuC in batches such that all authentication vectors in one batch are sent to the same SN/VLR.

- (1) In its binary representation, the sequence number consists of two concatenated parts  $SN = SEQ \parallel IND$ .  $SEQ$  is the batch number, and  $IND$  is an index numbering the authentication vectors within one batch.  $SEQ$  in its turn consists of two concatenated parts  $SEQ = SEQ1 \parallel SEQ2$ .  $SEQ1$  represents the most significant bits of  $SEQ$ , and  $SEQ2$  represents the least significant bits of  $SEQ$ .  $IND$  represents the least significant bits of  $SN$ . If the concept of batches is not supported then  $IND$  is void and  $SN = SEQ$ .
- (2) There is a counter  $SEQ_{HE}$  in the HE.  $SEQ = SEQ1 \parallel SEQ2$  is stored by this counter.  $SEQ_{HE}$  is an individual counter, i.e. there is one per user.
- (3) There is a global counter, e.g. a clock giving universal time. For short we call the value of this global counter at any one time  $GLC$ . If  $GLC$  is taken from a clock it is computed mod  $p$ , where  $p = 2^n$  and  $n$  is the length of  $GLC$  and of  $SEQ2$  in bits.
- (4) If  $GLC$  is taken from a clock then there is a number  $D > 0$  such that the following holds:
  - (i) the time interval between two consecutive increases of the clock (the clock unit) shall be chosen such that, for each user, at most  $D$  batches are generated at the AuC during any  $D$  clock units;
  - (ii) the clock rate shall be significantly higher than the average rate at which batches are generated for any user;
  - (iii)  $D \ll 2^n$ .
- (5) When the HE needs new sequence numbers  $SN$  to create a new batch of authentication vectors, HE retrieves the (user-specific) value of  $SEQ_{HE} = SEQ1_{HE} \parallel SEQ2_{HE}$  from the database.
  - (i) If  $SEQ2_{HE} < GLC < SEQ2_{HE} + p - D + 1$  then HE sets  $SEQ = SEQ1_{HE} \parallel GLC$ ;
  - (ii) if  $GLC \leq SEQ2_{HE} \leq GLC + D - 1$  or  $SEQ2_{HE} + p - D + 1 \leq GLC$  then HE sets  $SEQ = SEQ_{HE} + 1$ ;
  - (iii) if  $GLC + D - 1 < SEQ2_{HE}$  then HE sets  $SEQ = (SEQ1_{HE} + 1) \parallel GLC$ .
  - (iv) The  $i$ -th authentication vector in the batch receives the sequence number  $SN = SEQ \parallel i$ .
  - (v) After the generation of the first authentication vector in the batch has been completed  $SEQ_{HE}$  is reset to  $SEQ$ .

#### NOTES

1. The clock unit and the value  $D$  have to be chosen with care so that condition (4)(i) is satisfied for every user at all times. Otherwise, user identity confidentiality may be compromised. When the parameters are chosen appropriately sequence numbers for a particular user do not reveal significant information about the user's identity. In particular,  $IND$  is to be sufficiently short so that no unacceptably long contiguous strings of sequence numbers are generated.  
If authentication vectors for the CS and the PS domains are not separated by other means it is recommended to choose  $D > 1$  as requests from the two different domains may arrive completely independently.
2. The use of  $IND$  is only for the benefit of the USIM (see note 4 in Annex C.2). When  $D$  is chosen sufficiently large then several authentication vectors can be generated at the same time by (5)(ii) even when  $IND$  is not present.

Another variant of the sequence number generation mechanism is described below.

The part  $SEQ$  is not divided into two parts. The global counter  $GLC$  is thus as long as  $SEQ$ . Instead of storing the individual counter  $SEQ_{HE}$  in the HE there is a value  $DIF$  stored in the HE which is individual for each user. The  $DIF$

value represents the current difference between generated  $SEQ$  values for that user and the  $GLC$ .

When the HE needs new sequence numbers  $SQN$  to create a new batch of authentication vectors, HE retrieves the (user-specific) value of  $DIF$  from the data base and calculates  $SEQ$  values as  $SEQ = GLC + DIF$ .

The  $DIF$  value needs to be updated in the HE only during the re-synchronization procedure.

## C.2 Handling of sequence numbers in the USIM

This section assumes that sequence numbers are generated according to Annex C.1. If the concept of batches is not supported then batch numbers and sequence numbers coincide and the parameter  $IND$  is not used.

The USIM keeps track of an ordered **list** of the  $b$  highest batch number values it has accepted. In addition, for each batch number  $SEQ$  in the list, the USIM stores the highest  $IND$  value  $IND(SEQ)$  it has accepted associated with that batch number. Let  $SEQ_{LO}$  denote the lowest and  $SEQ_{MS}$  denote the highest batch number in the list.

### C.2.1 Protection against wrap around of counter in the USIM

The USIM will not accept arbitrary jumps in batch numbers, but only increases by a value of at most  $\Delta$ .

Conditions on the choice of  $\Delta$  :

- (1)  $\Delta$  shall be sufficiently large so that the MS will not receive any batch number  $SEQ$  with  $SEQ - SEQ_{MS} \geq \Delta$  if the HE/AuC functions correctly.
- (2) In order to prevent that  $SEQ_{MS}$  ever reaches the maximum batch number value  $SEQ_{max}$  during the lifetime of the USIM the minimum number of steps  $SEQ_{max} / \Delta$  required to reach  $SEQ_{max}$  shall be sufficiently large.

### C.2.2 Acceptance rule

When a user authentication request arrives the USIM checks whether the sequence number is acceptable. The sequence number  $SQN = SEQ \parallel IND$  is accepted by the USIM if and only if (i) and either (ii) or (iii) hold:

- (i)  $SEQ - SEQ_{MS} < \Delta$ ;
- (ii)  $SEQ$  is in the list and  $IND > IND(SEQ)$ ;
- (iii)  $SEQ$  is not in the list and  $SEQ > SEQ_{LO}$ .

The USIM shall also be able to put a limit  $L$  on the difference between  $SEQ_{MS}$  and an accepted batch number  $SEQ$ . If such a limit is applied then, in addition to the above conditions, the sequence number shall only be accepted by the USIM if  $SEQ_{MS} - SEQ < L$ .

### C.2.3 List update

After a sequence number  $SQN = SEQ \parallel IND$  received in a user authentication request has been accepted by the USIM the USIM proceeds as follows:

- (i) Case 1: the batch number  $SEQ$  is not in the list.  
Then the list entry corresponding to  $SEQ_{LO}$  is deleted,  $SEQ$  is included in the list,  $IND(SEQ)$  is set to  $IND$  and  $SEQ_{LO}$  and  $SEQ_{MS}$  are updated;
- (ii) Case 2: the batch number  $SEQ$  is in the list.  
Then  $IND(SEQ)$  is set to  $IND$ .

If a sequence number received in a user authentication request is rejected the list remains unaltered.

### C.2.4 Notes

1. Using the above list mechanism, it is not required that a previously visited SN/VLR deletes the unused authentication vectors when a user de-registers from the serving network. Retaining the authentication vectors for use when the user returns later may be more efficient as regards signalling when a user abroad switches a lot between two serving networks.

2. The list mechanism may also be used to avoid unjustified rejection of user authentication requests when authentication vectors in two SN/VLRs from different mobility management domains (circuit and packet) are used in an interleaving fashion.
3. When a VLR uses fresh authentication vectors obtained during a previous visit of the user, the USIM can reject them although they have not been used before (because the list size  $b$  and the limit  $L$  are finite). Rejection of a sequence number can therefore occur in normal operation, i.e., it is not necessarily caused by (malicious) replay or a database failure.
4. The mechanism presented in this section allows the USIM to exploit knowledge about which authentication vectors belong to the same batch. It may be assumed that authentication vectors in the same batch are always used in the correct order as they are handled by the same SN/VLR. Consequently, only one sequence number per batch has to be stored.
5. With the exception of  $SEQ_{MS}$ , the batch numbers in the list need not be stored in full length if a limit  $L$  on the difference between  $SEQ_{MS}$  and an accepted batch number is applied and if those entries in the list which would cause the limit  $L$  to be exceeded are removed from the list after a new sequence number has been accepted.
6. Condition (2) on  $\Delta$  means that  $SEQ_{MS}$  can reach its maximum value only after a minimum of  $SEQ_{max}/\Delta$  successful authentications have taken place.
7. There is a dependency of the choice of  $\Delta$  and the size  $n$  of global counter GLC in Annex C.1:  $\Delta$  shall be chosen larger than  $2^n$ .

Annex D:  
Void

Annex E:  
Void



---

## Annex F (informative): Example uses of AMF

### F.1 Support multiple authentication algorithms and keys

A mechanism to support the use of multiple authentication and key agreement algorithms is useful for disaster recovery purposes. AMF may be used to indicate the algorithm and key used to generate a particular authentication vector.

The USIM keeps track of the authentication algorithm and key identifier and updates it according to the value received in an accepted network authentication token.

---

### F.2 Changing list parameters

This mechanism is used in conjunction with the window and list mechanisms described in C.2.

Parameters which may be used to manage a list are the number of entries in a list (the list size) and an upper list on the admissible  $SEQ_{MS} - SEQ$  between the highest batch number  $SEQ_{MS}$  in the list and an accepted batch number  $SEQ$ . A mechanism to change these parameters dynamically is useful since the optimum for these parameters may change over time. AMF is used to indicate the maximum admissible list size or maximum admissible difference  $SEQ_{MS} - SEQ$  to be used by the user when verifying the authentication token and deciding whether it is still accepted.

The USIM keeps track of the maximum admissible list size and maximum admissible difference  $SEQ_{MS} - SEQ$  and updates them according to the received value providing that  $SEQ > SEQ_{MS}$ .

---

### F.3 Setting threshold values to restrict the lifetime of cipher and integrity keys

According to section 6.4.3, the USIM contains a mechanism to limit the amount of data that is protected by an access link key set. The AMF field may be used by the operator to set or adjust this limit in the USIM. For instance, there could be two threshold values and the AMF field instructs the USIM to switch between them.

The USIM keeps track of the limit to the key set life time and updates it according to the value received in an accepted network authentication token.

## Annex G (informative): Change history

Change history					
TSG SA #	Version	CR	Tdoc SA	New Version	Subject/Comment
S_03	2.0.0	-	-	3.0.0	Approved at SA#3 and placed under TSG SA Change Control
S_04	3.0.0	001	SP-99308	3.1.0	Mechanism for data integrity of signalling messages
S_04	3.0.0	002	SP-99308	3.1.0	Description of layer on which ciphering takes place
S_04	3.0.0	003	SP-99308	3.1.0	Conditions on use of authentication information
S_04	3.0.0	004	SP-99308	3.1.0	Modified re-synchronisation procedure for AKA protocol
S_04	3.0.0	005	SP-99308	3.1.0	Sequence number management scheme protecting against USIM lockout
S_04	3.0.0	006	SP-99308	3.1.0	Criteria for Replacing the Authentication "Working Assumption"
S_04	3.0.0	007	SP-99308	3.1.0	Functional modification of Network domain security mechanisms
S_04	3.0.0	008	SP-99308	3.1.0	Cipher key lifetime
S_04	3.0.0	009	SP-99308	3.1.0	Mechanism for user domain security
S_04	3.0.0	010	SP-99308	3.1.0	Replacement of incorrect diagrams
S_04	3.0.0	011	SP-99308	3.1.0	Precision of the status of annex B
S_05	3.1.0	012	SP-99417	3.2.0	Re-organisation of clause 6
S_05	3.1.0	013	SP-99417	3.2.0	Integrity protection procedures
S_05	3.1.0	014	SP-99417	3.2.0	Security of MAP-Based Transmissions
S_05	3.1.0	015	SP-99417	3.2.0	Secure UMTS-GSM Interoperation
S_05	3.1.0	016	SP-99417	3.2.0	Network-wide confidentiality
S_05	3.1.0	017	SP-99417	3.2.0	Authentication management field
S_05	3.1.0	018	SP-99417	3.2.0	Support for window and list mechanisms for sequence number management in authentication scheme
S_05	3.1.0	019	SP-99417	3.2.0	Modification of text for window and list mechanisms
S_05	3.1.0	020	SP-99485	3.2.0	Cipher/integrity key setting
S_05	3.1.0	021	SP99-496	3.2.0	A generalised scheme for sequence number management
S_06	3.2.0	022r1	SP-99584	3.3.0	Refinement of Enhanced User Identity Confidentiality
S_06	3.2.0	025	SP-99584	3.3.0	Length of KSI
S_06	3.2.0	026r1	SP-99584	3.3.0	Mobile IP security
S_06	3.2.0	027r1	SP-99584	3.3.0	Clarification of re-authentication during PS connections
S_06	3.2.0	030	SP-99584	3.3.0	Handling of the MS UEA and UIA capability information
S_06	3.2.0	031	SP-99585	3.3.0	Removal of alternative authentication mechanism described in annex D
S_06	3.2.0	032	SP-99584	3.3.0	Removal of network-wide encryption mechanism from application security section
S_06	3.2.0	033	SP-99584	3.3.0	Interoperation and intersystem handover/change between UTRAN and GSM BSS
S_06	3.2.0	034	SP-99584	3.3.0	Distribution of authentication data within one serving network domain
S_06	3.2.0	035	SP-99584	3.3.0	Authentication and key agreement
S_06	3.2.0	036	SP-99584	3.3.0	Sequence number management
S_06	3.2.0	037r1	SP-99584	3.3.0	Authentication and key agreement
S_06	3.2.0	038	SP-99584	3.3.0	Clarification on system architecture
S_06	3.2.0	039	SP-99584	3.3.0	Updated definitions and abbreviations
S_06	3.2.0	040	SP-99584	3.3.0	An authentication failure report mechanism from SN to HE
-	3.3.0	-	-	3.3.1	Editorial clean-up by MCC
S_07	3.3.1	043	SP-000112	3.4.0	Clarification on cipher key and integrity key lifetime
S_07	3.3.1	044	SP-000112	3.4.0	local Authentication and connection establishment
S_07	3.3.1	045r3	SP-000075	3.4.0	Refinement EUIC
S_07	3.3.1	047r2	SP-000077	3.4.0	Interoperation and intersystem handover/change between UTRAN and GSM BSS
S_07	3.3.1	048	SP-000112	3.4.0	Clarification on the reuse of Avs
S_07	3.3.1	049	SP-000112	3.4.0	Authentication failure reporting
S_07	3.3.1	050	SP-000112	3.4.0	Refinement of Cipher key and integrity key lifetime
S_07	3.3.1	051r1	SP-000112	3.4.0	Conversion function c3 at USIM
S_07	3.3.1	052r1	SP-000112	3.4.0	Trigger points of AFR during AKA
S_07	3.3.1	053r1	SP-000112	3.4.0	Removal of EUIC from 'Authentication Data Request' procedure
S_07	3.3.1	054r1	SP-000112	3.4.0	Clarification of the scope
S_07	3.3.1	055	SP-000112	3.4.0	SQN Generation Requirements
S_07	3.3.1	056r1	SP-000112	3.4.0	Identification of temporary identities
S_07	3.3.1	057	SP-000112	3.4.0	Cipher key and integrity key selection
S_07	3.3.1	058r1	SP-000112	3.4.0	Clarification on ciphering and integrity mode setting
S_07	3.3.1	059	SP-000112	3.4.0	Clarification on when integrity protection is started
S_07	3.3.1	061r1	SP-000112	3.4.0	Unsuccessful integrity check
S_07	3.3.1	062r1	SP-000112	3.4.0	Clarification on signalling messages to be integrity protected

Change history					
TSG SA #	Version	CR	Tdoc SA	New Version	Subject/Comment
S_07	3.3.1	063r1	SP-000112	3.4.0	Clarification of the HFN handling
S_07	3.3.1	064r2	SP-000077	3.4.0	Distribution and Use of Authentication Data between VLRs/SGSNs
S_07	3.3.1	066r1	SP-000077	3.4.0	Ciphering
S_07	3.3.1	067r1	SP-000077	3.4.0	Data integrity
S_07	3.3.1	072	SP-000112	3.4.0	Clarification on ciphering and integrity protection at intersystem handover
S_07	3.3.1	073r1	SP-000044	3.4.0	MAP Security
S_07	3.3.1	074	SP-000112	3.4.0	Clarification about CK and IK which are transmitted in clear over the lu-interface
S_07	3.3.1	076	SP-000112	3.4.0	Cipher key and integrity key lifetime
S_07	3.3.1	077	SP-000112	3.4.0	Cipher key and integrity key setting
S_07	3.3.1	079r1	SP-000112	3.4.0	Local Authentication and connection establishment
S_08	3.4.0	080	SP-000272	3.5.0	Clarification on ciphering and integrity protection at intersystem handover
S_08	3.4.0	083	SP-000272	3.5.0	Authentication and key agreement (minimal)
S_08	3.4.0	084	SP-000272	3.5.0	Conversion functions for GSM-UMTS interoperation
S_08	3.4.0	088r2	SP-000272	3.5.0	Initialisation of synchronisation for ciphering and integrity protection
S_08	3.4.0	089	SP-000274	3.5.0	Addition of another variant of sequence number generation
S_08	3.4.0	090	SP-000272	3.5.0	Clarification of BEARER and DIRECTION parameters
S_08	3.4.0	091	SP-000274	3.5.0	Inclusion of the radio bearer identity to the integrity mechanism
S_08	3.4.0	092	SP-000273	3.5.0	Removal of enhanced user identity confidentiality
S_08	3.4.0	093	SP-000272	3.5.0	Removal of network domain security
S_08	3.4.0	094	SP-000272	3.5.0	Cipher and integrity key update once every 24 hours
S_08	3.4.0	096	SP-000272	3.5.0	Clarification on the HFN handling
S_08	3.4.0	097r1	SP-000271	3.5.0	Align of note and star in figure 18
S_08	3.4.0	098	SP-000272	3.5.0	Security mode set-up procedure
S_08	3.4.0	100	SP-000272	3.5.0	Replace COUNT by STARTCS and STARTPS
S_08	3.4.0	102	SP-000273	3.5.0	Removal of NW Wide Encryption
S_08	3.4.0	103r2	SP-000271	3.5.0	Clarification on terminology in user domain

---

# History

<b>Document history</b>		
V3.3.1	January 2000	Publication
V3.4.0	March 2000	Publication
V3.5.0	July 2000	Publication