3GPP TSG SA 3 Meeting #15
Washington, USA, 12-14 September 2000

***Document* S3-000552**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

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

33.102	CR		Current Version:	3.5.0

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

For submission to:	SA#9	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

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

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

Source: Siemens **Date:** 6 Sept. 2000

Subject: References

Work item: Security

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

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

Reason for change:
Clause 1: A reference to "Security Principles and Objectives" is added.
Clause 2: The reference list is updated. If and only if a reference occurs in the text it is included. No distinction is made between normative and informative references.
Clause 3: A reference to "Vocabulary for 3GPP Specifications" is added.
Clause 4: Reference to TS 23.121 is made uniform.
Clause 5.3: References to "Verify PIN" feature is updated to 3G specification.
Clause 5.4.1: Reference to (U)SIM Application Toolkit is updated to 3G specification.
Clause 6.1.1: References to GSM 03.20 and TS 23.060 are made uniform.
Clause 6.3.1: Reference to ISO/IEC 9798-4 is made uniform.
Clause 6.5.6: References to Kasumi specs are added.
Clause 6.6.6: References to Kasumi specs are added.

Clauses affected: 1, 2, 3, 4, 5.3, 5.4.1, 6.1.1, 6.3.1, 6.5.6, 6.6.6

Other specs Affected:

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

Other comments:
Reference 10 needs to be completed.
We might want to add tags "informative" / "normative".

help.doc

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

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" (TS 21.133 [1]) and implement the security objectives and principles described in TS 33.120 [2]. 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: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".

[2] 3G TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".

[3] 3G TR 21.905: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; Vocabulary for 3GPP Specifications (Release 1999)".

[4] 3G TS 23.121: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; Architecture Requirements for Release 99".

[5] 3G TS 31.101: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) T; UICC-terminal interface; Physical and logical characteristics".

[6] 3G TS 22.022: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; Personalisation of UMTS Mobile Equipment (ME); Mobile functionality specification".

[7] 3G TS 23.048: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; Security Mechanisms for the USIM application toolkit; Stage 2".

[8] ETSI GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[9] 3G TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

[10] ISO/IEC 9798-4: XXX.

[11] 3G TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications"

[12] 3G TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification"

[13] 3G TS 35.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementers' test data"

[14] 3G TS 35.204: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data"

~~[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: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Cryptographic Algorithm Requirements".

[13a] 3G TS 23.003: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) Core Network (CN); Numbering, addressing and identification".

[13b] 3G TS 23.060: "3rd Generation Partnership Project; Technical Specification Group and System Aspects; Digital cellular telecomunications 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

In addition to the definitions included in TR 21.905 [3], for ~~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

In addition to (and partly in overlap to) the abbreviations included in TR 21.905 [3], for ~~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_{HE}	Sequence number counter maintained in the HLR/AuC
SQN_{MS}	Sequence number counter maintained in the USIM
SGSN	Serving GPRS Support Node
SIM	(GSM) Subscriber Identity Module
SN	Serving Network
T	Triplet, GSM authentication vector
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.

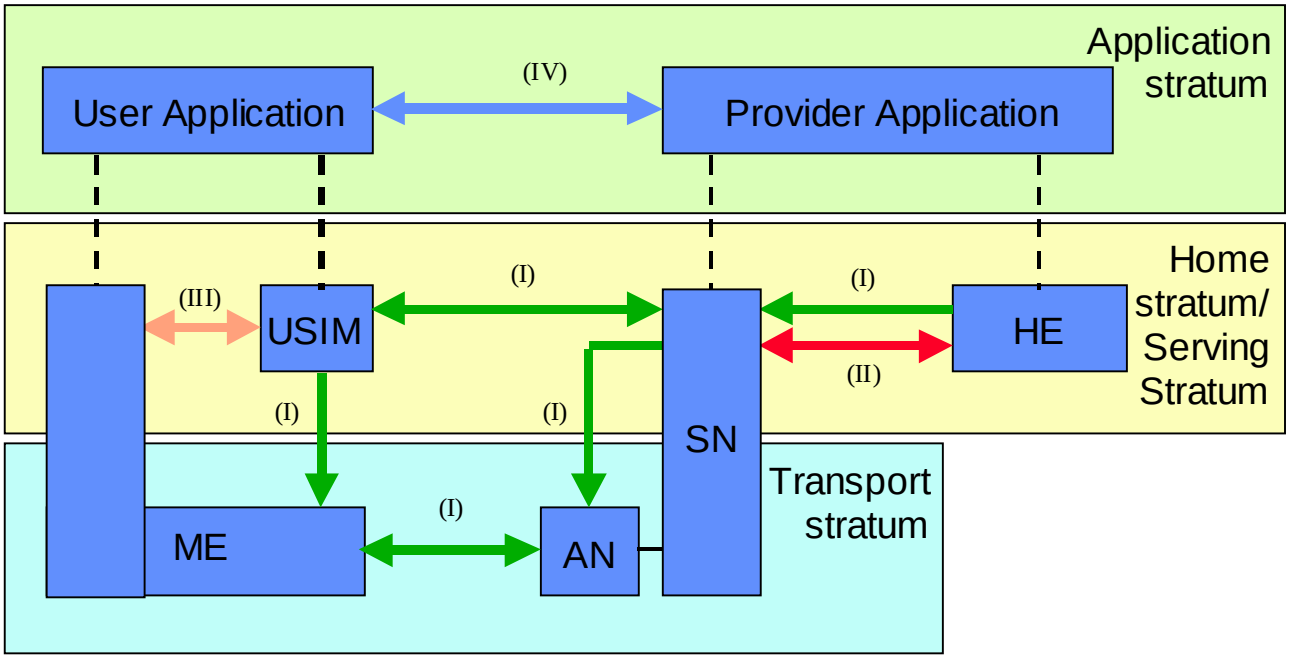

Figure 1: Overview of the security architecture

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.

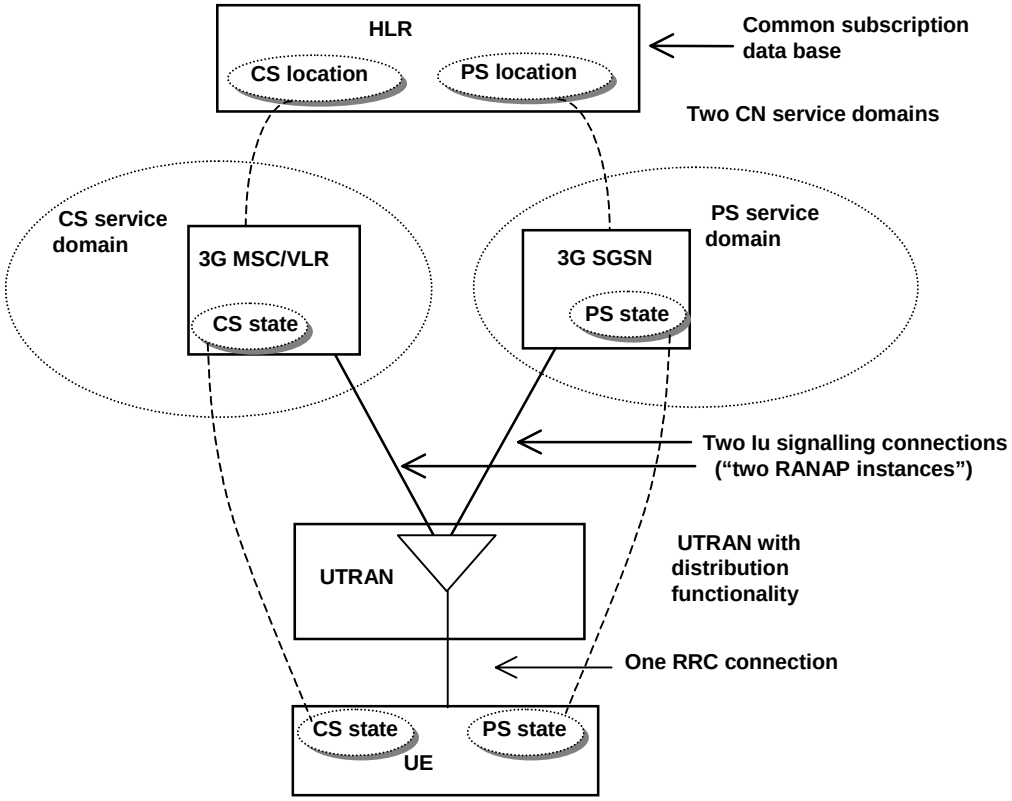

Figure 2: Overview of the ME registration and connection principles within UMTS for the separate CN architecture case when the CN consists of both a CS service domain with evolved MSC/VLR, 3G_MSC/VLR, as the main serving node and an PS service domain with evolved SGSN/GGSN, 3G_SGSN and 3G GGSN, as the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

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 TS 31.101[5]~~[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 TS 22.022 [6]~~[15]~~.

5.4.1 Secure messaging between the USIM and the network

~~It is expected that 3GMS will~~ This feature provide~~s~~ 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.

This security feature is implemented by means of the mechanism described in TS 23.048 [7].

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.

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 a 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 [8] and TS 23.060 [9]. The following subclauses contain a summary of this feature.

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 [10] (section 5.1.1).

An overview of the mechanism is shown in Figure 5.

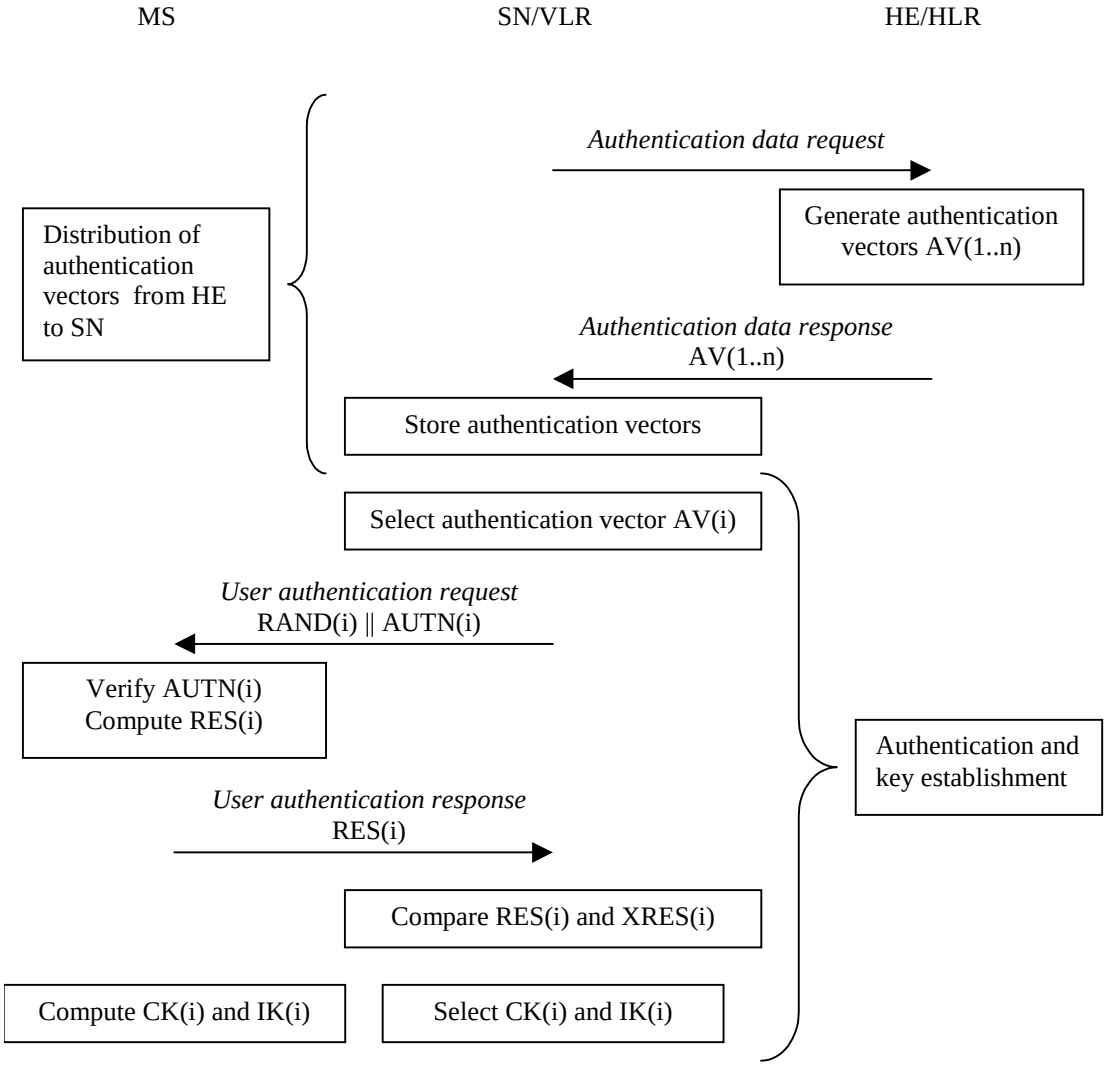

Figure 5: Authentication and key agreement

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.

6.5.6 UIA identification

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

"0001_2" : UIA1, Kasumi.

The remaining values are not defined.

The use of Kasumi for the integrity protection function f9 is specified in TS 35.201 [11] and TS 35.202 [12]. Implementers' test data and design conformance data is provided in TS 35.203 [13] and TS 35.202 [14].

6.6.6 UEA identification

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

"0000_2" : UEA0, no encryption.

"0001_2" : UEA1, Kasumi.

The remaining values are not defined.

The use of Kasumi for the ciphering function f8 is specified in TS 35.201 [11] and TS 35.202 [12]. Implementers' test data and design conformance data is provided in TS 35.203 [13] and TS 35.202 [14].