TSGS#3(99)144

3G TS 33.102 V2.0.0 (1999-04)

3rd Generation Partnership Project (3GPP);
Technical Specification Group (TSG) SA;
3G Security;
Security Architecture
3G TS 33.102 version 2.0.0

Reference
DTS/TSGS-03sec-a1U

Keywords
Security Architecture

3GPP

Postal address

Office address

Internet
http://www.3gpp.org

Contents

Intellectual Property Rights

To be added.

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects (TSG SA).

The contents of this TS may be subject to continuing work within the 3GPP and may change following formal TSG approval. Should the TSG modify the contents of this TS, it will be re-released with an identifying change of release date and an increase in version number as follows:

Version m.t.e

where:

m indicates [major version number]

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

y the third digit is incremented when editorial only changes have been incorporated into 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 capabilities 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.

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] 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".

2.2 Informative references

GSM documents:

[9] GSM 02.09 version 5.1.1: "Security Aspects"

[10] GSM 02.22 version 6.0.0: "Personalisation of GSM Mobile Equipment (ME); Mobile functionality specification."

[11] GSM 02.48, version 6.0.0: "Security Mechanisms for the SIM Application Toolkit; Stage 1"

[12] GSM 02.60, version 7.0.0: "GPRS; Service Description; Stage 1"

[13] GSM 03.20, version 6.0.1: "Security related network functions"

[14] GSM 03.48, version 6.1.0; "Security Mechanisms for the SIM application toolkit; Stage 2"

[15] GSM 03.60, version 7.0.0: "GPRS; Service Description; Stage 2"

[16] GSM 11.11, version 7.1.0: "Specification of SIM-terminal interface"

[17] GSM 11.14, version 7.1.0: "Specification of SIM Application Toolkit for SIM-terminal interface"

UMTS documents:

[18] UMTS 21.11, version 0.4.0: "IC-card aspects"

[19] UMTS 23.01, version 1.0.0: "UMTS Network architecture"

[20] 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.

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
f6	Encryption function used to encrypt the IMUI
f7	Decryption function used to decrypt the IMUI ($=f6^{-1}$)
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:

3GMS	Third Generation Mobile Communication System
AK	Anonymity Key
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key

CS	Circuit Switched
HE	Home Environment
HLR	Home Location Register
IK	Integrity Key
IMUI	International Mobile User Identity
KSI	Key Set Identifier
KSS	Key Stream Segment
LAI	Location Area Identity
MAC	Message Authentication Code
MAC	The message authentication code included in AUTN, computed using f1
MS	Mobile Station
MSC	Mobile Services Switching Centre
MT	Mobile Termination
PS	Packet Switched
TE	Terminal Equipment
TMUI	Temporary Mobile User Identity
RAND	Random challenge
SEQ	Sequence number
SN	Serving Network
TMUI	Temporary Mobile User Identity
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UN	User Name
USIM	User Services Identity Module
VLR	Visited Location Register
XRES	Expected Response
XUR	Expected User Response

4 Overview of the security architecture

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

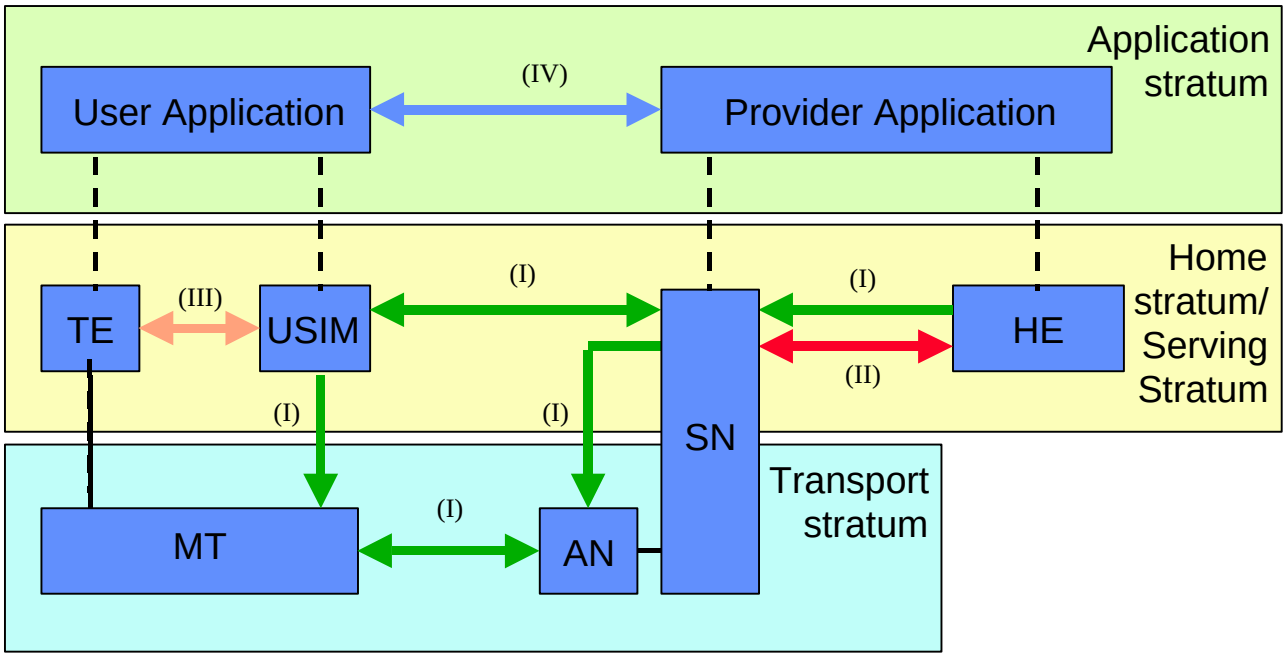

Figure 1 : Overview of the security architecture

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.

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.

Clause 6.2 describes a mechanism that allows a user to be identified on the radio path in case he is not known in the visited serving network by a temporary identity. It provides a transparent channel between the USIM and the user's HE that provides the user's HE with the option to implement a mechanism that allows identification by means of an encrypted permanent identity. The serving network then has to forward the encrypted permanent identity to the user's HE for decryption and receives the user's permanent identity from the user's HE. A possible mechanism that makes use of symmetric key encryption using group keys is included in Annex B. Alternatively, the user's HE environment has the option to let the user identify himself by means of its permanent identity in cleartext. Either of both mechanisms should be used to identify a user on the radio path, whenever the user is not known by a temporary identity in the serving network.

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 Entity authentication

The following features with respect to authentication of network elements are provided:

- **authentication mechanism agreement:** the property that two network entities can securely negotiate the mechanism for authentication that they shall use subsequently;

- **network element authentication:** the property that a network element corroborates the identity of another network element it wants to communicate with;

This feature ensures that no malicious operational or maintenance commands can be injected into a network domain by an intruder. It provides network elements, in particular network elements belonging to different network operators, with the possibility to corroborate each other’s identities before exchanging data.

This goal may be achieved either by an explicit or implicit entity authentication mechanism, to be performed each time data are exchanged between two network entities. Implicit authentication is realised by exchanging encrypted messages only, so that only an entity in possession of a certain shared key can make use of the data. The shared keys may be distributed among the network elements of a single operator in a manner outlined in Annex D.

Explicit authentication mechanisms can be achieved by asymmetrically based protocols (e.g. by using digital signatures) or by symmetric (e.g. challenge-response) protocols. Again, for explicit symmetric authentication, the necessary keys may be distributed as proposed in Annex E.

5.2.2 Data confidentiality

The following security features are provided with respect to confidentiality of data exchanged between network elements:

- **cipher algorithm agreement:** the property that two network elements can securely negotiate the algorithm that they shall use subsequently;

- **cipher key agreement:** the property that two network elements agree on a cipher key that they may use subsequently;

- **confidentiality of exchanged data:** the property that data exchanged between two network elements cannot be eavesdropped;

In case authentication data can be eavesdropped in the network domain, serious fraud problems will arise. Therefore, these features are needed to ensure the confidentiality of sensitive data, e.g. authentication or other subscriber data inside the network domain. The first two features may be realised in course of an authentication mechanism performed

by the network elements; the agreed cipher key is then used for securing signalling and user data by means of the agreed cipher algorithm.

5.2.3 Data integrity

The following security features are provided with respect to integrity of data exchanged between two network elements:

- **integrity algorithm agreement:** the property that two network elements can securely negotiate the integrity algorithm that they shall use subsequently;
- **integrity key agreement:** the property that two network elements agree on an integrity key that they may use subsequently;
- **data integrity and data origin authentication of signalling data:** the property that the receiving network element is able to verify that signalling data has not been modified in an unauthorised way since it was sent by the sending element and that the data origin of the signalling data received is indeed the one claimed;

The feature data integrity of signalling data ensures that operation and maintenance commands or user data exchanged between two network elements cannot be modified by an intruder without being detected, while the third feature ensures that no malicious operational or maintenance commands can be injected into a network domain by an intruder

The first two features may be realised in course of an authentication mechanism performed by the network entities involved; the agreed integrity key is then used for securing integrity of the exchanged data by means of the agreed integrity algorithm.

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.

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.

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 Network-wide user traffic confidentiality

This feature provides users with the assurance that their traffic is protected against eavesdropping across the entire network, not just on the radio links in the access network.

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 network-wide encryption: the property that the user is informed whether the confidentiality of user data is protected along the entire communication path;
- 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 user identity (TMUI). A TMUI has local significance only in the location area in which the user is registered. Outside that area it should be a accompanied by an appropriate Location Area Identification (LAI) in order to avoid ambiguities. The association between the permanent and temporary user identities is kept by the Visited Location Register (VLR) in which the user is registered.

The TMUI, 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.

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 2.

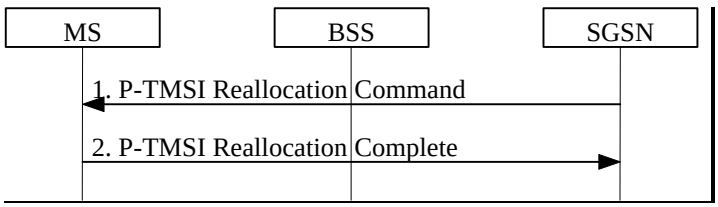

Figure 2: TMUI Allocation

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

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

Upon receipt the user stores TMUIn 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 TMUIn and the IMUI and between the old temporary identity TMUIo (if there is any) and the IMUI.

For an user-originated transaction, the network shall allow the user to identify itself by either the old temporary identity TMUIo or the new temporary identity TMUIn. 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 user identity (IMUI).

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 network, or when the serving network cannot retrieve the IMUI from the TMUI by which the user identifies itself on the radio path.

The mechanism is illustrated in Figure 3.

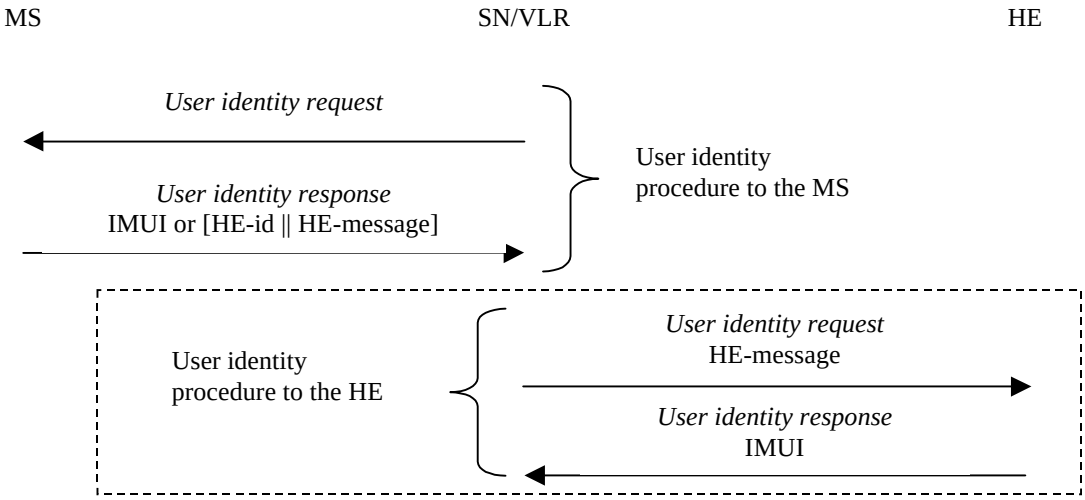

Figure 3: Identification by the permanent identity

The mechanism is initiated by the visited SN/VLR that requests the user to send its permanent identity. According to the user's preferences, his response may contain either 1) the IMUI in cleartext, or 2) the user's HE-identity in cleartext and an HE-message that contains an encrypted IMUI.

Note: The term HE-id denotes 3G equivalent of the information contained in MCC || MNC.

In case the response contains the IMUI in cleartext, the procedure is ended successfully. This variant represents a breach in the provision of user identity confidentiality.

In case the response contains an encrypted IMUI, the visited SN/VLR forwards the HE message to the user's HE in a request to send the user's IMUI. The user's HE then derives the IMUI from the HE-message and sends the IMUI back to the SN/VLR. Annex B describes an example mechanism that makes use of group keys to encrypt the IMUI.

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 SQN_{MS} and SQN_{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.

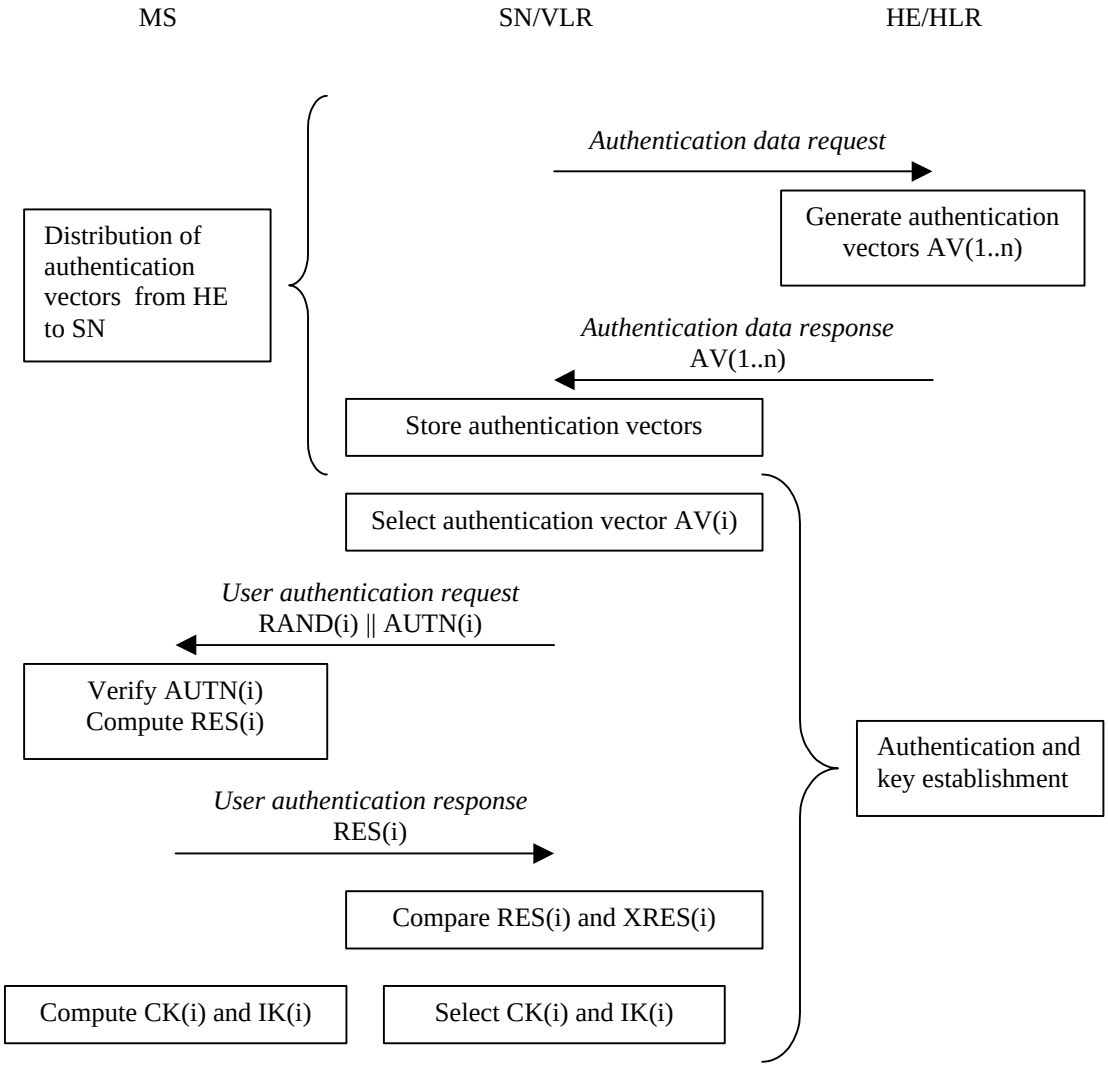

Figure 4: Authentication and key agreement

Upon receipt of a request from the SN/VLR, the HE/AuC sends an ordered array of *n* authentication vectors (the equivalent of a GSM "triplet") to the SN/VLR. 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 SN/VLR and the USIM.

When the SN/VLR 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 SN/VLR. The USIM also computes CK and IK. The SN/VLR compares the received RES with XRES. If they match the SN/VLR 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 SN/VLR to the entities which perform ciphering and integrity functions.

SN/VLRs 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).

Note: It is ffs. whether a separate mechanism for authentication based on a shared integrity key is required, or whether entity authentication is implicitly provided by means of the data integrity protection of signalling messages. If a separate mechanism is required, it is described in 6.5.

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 SN/VLR. This procedure is described in 6.3.2. The SN/VLR 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 SN/VLR to the HE/AuC are adequately secure. Mechanisms to secure these links are described in clause 7. It is further assumed that the user trusts the HE.

A procedure to mutually authenticate and establish new cipher and integrity keys between the SN/VLR 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 SN/VLRs are adequately secure. Mechanisms to secure these links are described in clause 7.

6.3.2 Distribution of authentication data from HE to SN

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

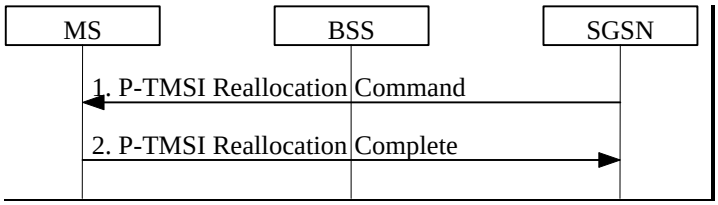

Figure 5: Distribution of authentication data from HE to SN/VLR

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

The *authentication data request* shall include a user identity and a parameter MODE that indicates whether the requesting node is a PS node or a CS node. If the user is known in the SN/VLR by means of the IMUI, the *authentication data request* shall include the IMUI. However, if the user is identified by means of an encrypted permanent identity (see 6.2), the HLR-message from which the HE can derive the IMUI is included instead. In that case, this procedure and the procedure *user identity request to the HLR* are integrated.

Upon the receipt of the *authentication data request* from the SN/VLR, 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 SN/VLR that contains an ordered array of n authentication vectors AV(1..n).

Figure 6 shows the generation of an authentication vector AV by the HE/AuC.

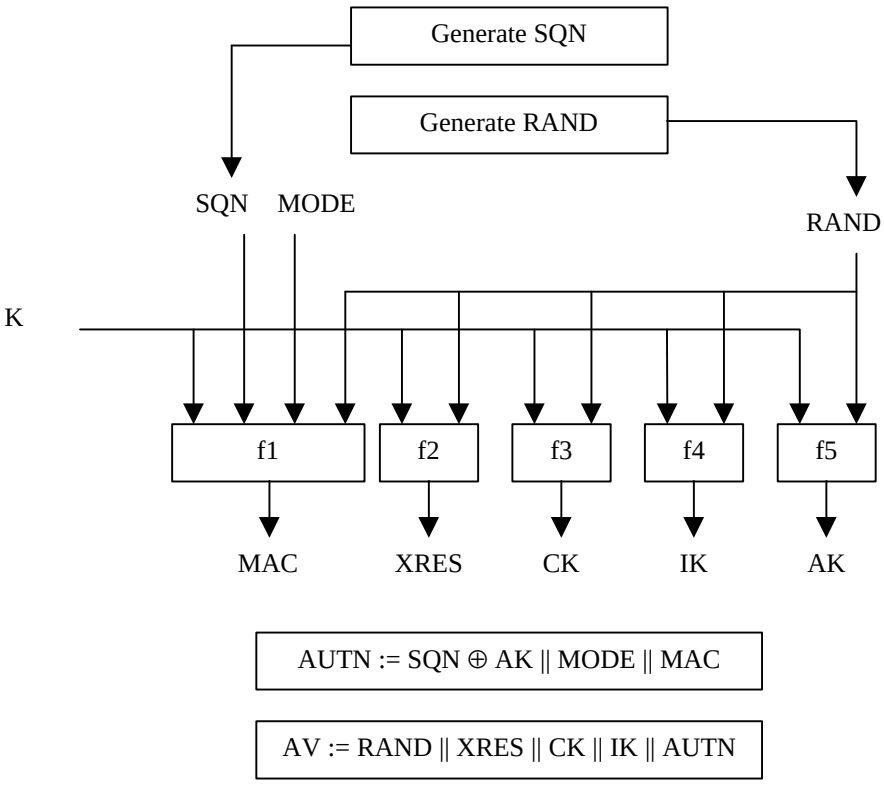

Figure 6: Generation of an authentication vector

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 two counters: $SQN_{HE/CS}$ for authentications initiated by the CS CN nodes, and $SQN_{HE/PS}$ for authentications initiated by the PS CN nodes.

To generate a fresh sequence number, the counter of the appropriate mode is incremented and subsequently the SQN is set to the new counter value.

Note 1: The HE has some flexibility in the management of sequence numbers. Annex C contains alternative methods for the generation and verification of sequence numbers.

Note 2: The solution in the main body uses the parameter MODE to distinguish between the CS and the PS core network nodes such that each node can simultaneously and independently support mobility management for the mobile user. Consequently two counters are required both in the AuC and in the USIM. If a single counter would be used, we would run into the following problem: Suppose that a CS node would order the SQNs 1–5, and use SQN 1 and a PS node would order the SQNs 6–10 and uses 6. Then the CS node would like to use 2, but that SQN is rejected. He orders new authentication vectors, with SQNs 11–15, and authenticates with SQN 11. Then the PS node runs into problems. The separate counters for CS and PS mode provide a solution for this problem.

Subsequently the following values are computed:

- a message authentication code $MAC = f1_K(SQN \| RAND \| MODE)$ 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.

Finally the authentication token $AUTN = SQN \oplus AK \| MODE \| MAC$ 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.

Note 1: The need for f5 to use a long-term key different from K is ffs.

Note 2: The requirements on f3, f4 and f5 are ffs.

Note 3: It is also ffs in how far the functions f1, ..., f5 need to differ and how they may be suitably combined.

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 SN/VLR and the MS. During the authentication, the user verifies the freshness of the authentication vector that is used.

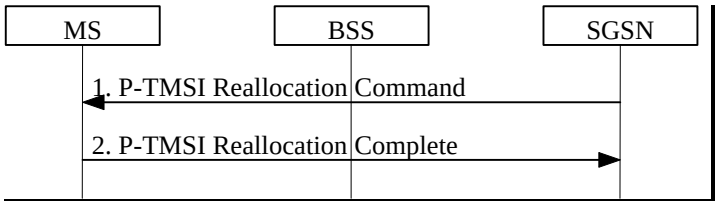

Figure 7: Authentication and key establishment

The SN/VLR invokes the procedure by selecting the next unused authentication vector from the ordered array of authentication vectors in the VLR database. The SN/VLR sends to the user 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 8.

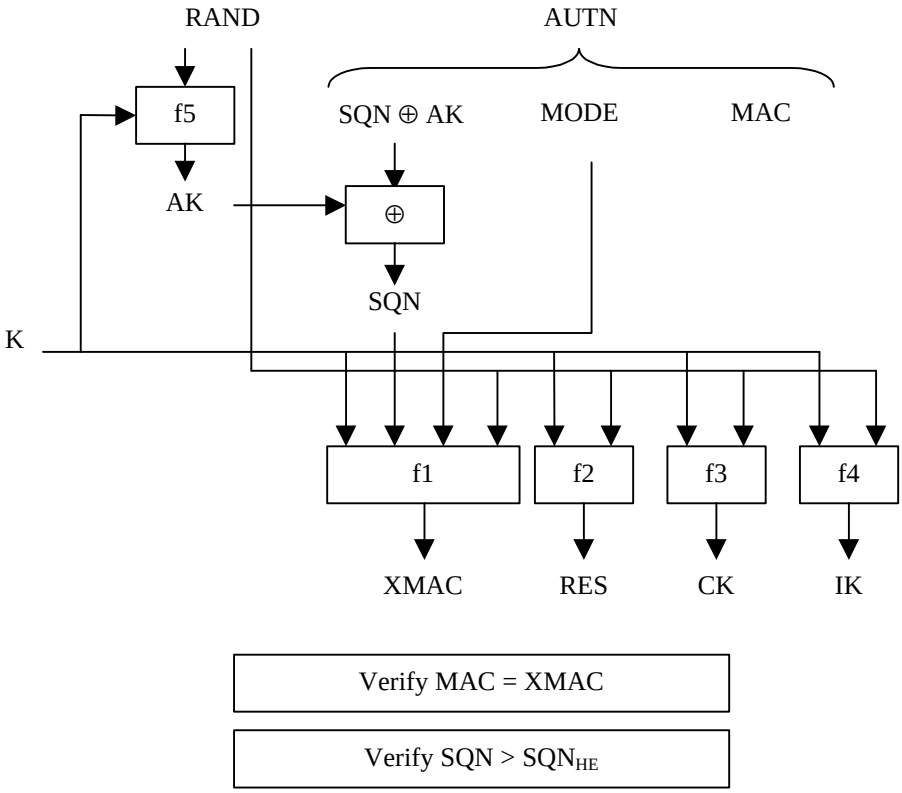

Figure 8: User authentication function in the USIM

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

Next the user computes XMAC = $f1_K$ (SQN || RAND || MODE) and compares this with MAC which is included in AUTN. If they are different, the user sends *user authentication reject* back to the SN/VLR with an indication of the cause and the user abandons the procedure.

Next the user verifies the freshness of the received sequence number SQN.

For each mode the USIM keeps track of one counter: $SQN_{MS/CS}$ for authentications initiated by the CS CN nodes, and $SQN_{MS/PS}$ for authentications initiated by the PS CN nodes.

To verify the freshness of the sequence number SQN, the USIM compares SQN with $SQN_{MS/MODE}$. If SQN > $SQN_{MS/MODE}$ the MS considers the sequence number as fresh and subsequently sets $SQN_{MS/MODE}$ to SQN.

Note: The HE has some flexibility in the management of sequence numbers. Annex C contains alternative method for the generation and verification of sequence numbers.

If the user considers the sequence numbers not fresh, he sends *user authentication reject* back to the SN/VLR with an indication of the cause and the user abandons the procedure.

If the sequence number is consider fresh however, the user computes RES = $f2_K$ (RAND) and includes this parameter in a *user authentication response* back to the SN/VLR. Finally the user 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.

Upon receipt of *user authentication response* the SN/VLR 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 SN/VLR also selects the appropriate cipher key CK and integrity key IK from the selected authentication vector.

6.3.4 Distribution of authentication vectors between VLRs

The purpose of this procedure is to provide a newly visited VLR with unused authentication vectors from a previously visited VLR. The procedure is shown in Figure 9.

The procedure is initiated by the visited VLR and illustrated in the following figure:

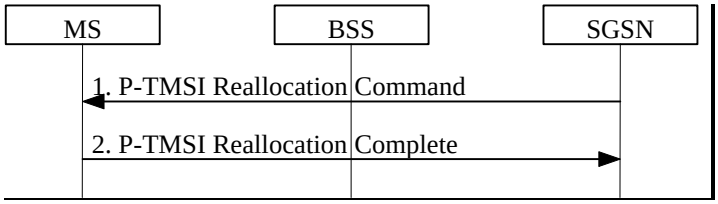

Figure 9: Distribution of authentication data between SN/VLR

The procedure is invoked by the newly visited SN/VLRn after a *location update request* sent by the user. Typically the user identifies himself using a temporary user identity TMUIo and the location area identity LAIo of a location area under the jurisdiction of SN/VLRo. In that case this procedure is integrated with the procedure described in 6.1.4. In addition, the SN/VLRn indicates whether it is a CS or PS node.

Upon receipt of the request the VLRo verifies whether it has any unused authentication vectors of the appropriate mode in its database and if so, sends the unused authentication vectors to VLRn. The previously visited VLRo shall then delete these authentication vectors from its database.

Upon receipt the VLRn stores the received authentication vectors.

If VLRo indicates that it has no authentication vectors or the VLRo cannot be contacted, VLRn should request new authentication vectors from the user's HE using the procedure described in 6.3.2.

6.3.5 Re-synchronisation procedure

The purpose of this procedure is to re-synchronise a counter in the HLR/AuC with a counter in the USIM. The procedure may be invoked by the HLR/AuC in the event of:

- a database failure in the HLR/AuC whereby the value of the counter $SQN_{HE/MODE}$ is lost;

- a message coming from the SN/VLR saying that the user could verify the data integrity of AUTN sent by the SN/VLR, but that he rejected AUTN because $SQN \leq SQN_{MS/MODE}$. In normal operations this should not happen. This may point to a replay of AUTN || RAND, but may also be caused because the counter value in the HLR/AuC is accidentally set to a lower value than is required.

The re-synchronisation procedure is described in Figure 10:

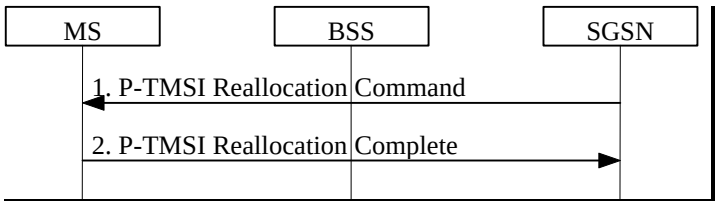

Figure 10: Re-synchronisation of the counter in the HLR/AuC

The HLR/AuC initiates the re-synchronisation procedure by sending a *re-synchronisation request* to the user that includes the appropriate mode.

Upon receipt of the request the USIM sends a *re-synchronisation response* back to the HLR/AuC that includes a RAND and AUTN pair with $SQN = SQN_{MS/MODE}$. The USIM has several ways to produce RAND || AUTN. Either it stores and returns the latest received RAND || AUTN pair, or it only stores the received RAND and re-computes AUTN, or it generates a RAND and computes the corresponding AUTN. AUTN is computed as described in 6.3.2.

Upon the receipt of the *re-synchronisation response* the HLR/AuC verifies the data integrity of AUTN as described in 6.3.3. Only if the received SQN is greater than $SQN_{HE/MODE}$, then $SQN_{HE/MODE}$ is set to SQN.

6.3.6 Length of sequence numbers

Sequence numbers shall be sufficiently long so that they cannot wrap around during the lifetime of the system. Consequently, in normal operations neither SQN_{MS} nor SQN_{HE} can wrap around during the lifetime of a USIM.

Note 1: If the counters would derive sequence numbers from time (see Annex C), then a 32-bit counter that is derived from the number of seconds that have elapsed since January 1, 2000 would only wrap around in the year 2136. So a length of 32-bits for the sequence numbers and counters should be sufficient. For individual incremental counters, a smaller range of sequence numbers should be sufficient, as authentication and key agreement is expected to occur far less frequently than once every second. Shorter lengths would however exclude the use of time-derived sequence numbers.

Note 2: Sequence numbers for CS and PS operation are expected to have the same length.

6.3.7 Interoperability with 2G networks

Note: This section should define the procedures and functions that are required to support roaming of UMTS users in GSM networks and handover of UMTS users between UMTS networks and GSM networks as regards the establishment of cipher and integrity keys.

In case of handover the user should receive the level of security that is usually provided in the network that is entered. Therefore the following functionality has to be provided in case of handover:

- system specific security keys have to be established

6.4 Data integrity of signalling elements

6.4.1 General

Some signalling information elements are considered sensitive and must be integrity protected. An integrity function shall be applied on certain signalling information elements transmitted between the MS and the SN.

The UMTS Integrity Algorithm (UIA) shall be implemented in the USIM and in the RNC.

The UIA shall be used with an Integrity Key (IK) to compute a message authentication code for a given message.

The following signalling elements sent by the MS to the RNC should be protected:

- The MS capabilities, including authentication mechanism, ciphering algorithm and message authentication function capabilities.
- The security mode accept/reject message.
- The called party number in a mobile originated call.
- Periodic message authentication messages.

The following signalling elements sent by the RNC to the MS should be protected:

- The security mode command, including whether ciphering is enabled or not and the ciphering and integrity algorithm to be used.
- Periodic message authentication messages.

Note: The point at which integrity protection is applied in the UTRAN architecture is for further study. At this stage we assume that integrity protection is applied at the RNC but may be applied at the MSC/VLR.

6.4.2 Integrity key setting

Mutual key setting is the procedure that allows the MS and the RNC to agree on the key IK used to compute message authentication codes using algorithm UIA. Key setting is triggered by the authentication procedure and described in 6.3. 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. TMUI or IMUI) is known by the SN/VLR. The key IK is stored in the SN/VLR and transferred to the RNC when it is needed. The key IK is stored in the USIM until it is updated at the next authentication.

6.4.3 Key set identifier

The key set identifier (KSI) is a number which is associated with the cipher and integrity keys derived during authentication. It is stored together with the cipher and integrity keys in the MS and in the network.

The key set identifier is used to allow key re-use during subsequent connection set-ups. The KSI is used to verify whether the MS and the SN are to use the same cipher key and integrity key.

6.4.4 Integrity key lifetime

A mechanism is needed to ensure that a particular integrity key is not used for an unlimited period of time, to avoid attacks using compromised keys. Authentication which generates integrity keys is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. The USIM shall therefore contain a mechanism to limit the number of calls that can be made with a specific integrity key.

Operators shall decide on the value of this number of calls, and write this parameter on the USIM. The USIM shall have a counter that counts the number of times the integrity key is used and shall trigger the generation of a new integrity key if the counter reaches the maximum value set in the USIM[1]. This mechanism will ensure that an integrity key cannot be reused more times than the limit set by the operator.

[1] *Which message should be chosen as a parameter? Using this would register call attempts as well as calls...*

Note: The decision on when a key needs to be updated may depend on a number of factors, including the time since the last key update, the amount of data protected using that key, and the cost/value of the services protected through the use of that key. Unfortunately they cannot be easily measured by the USIM, so it is suggested that the number of calls made using the key should be measured instead. Some concern exists whether this is a good enough measure. Should also the (periodic) in-call authentication messages be counted, such that long calls weigh more than short calls? Should also the authentications based on a shared integrity key be counted, invoked for other purposes than for calls?

6.4.5 UIA numbering

Table Error! Style not defined..Error! Bookmark not defined. **- UIA numbering**

Information Element	Length	Value	Remark
UIA Number	4	0000_2	Standard UMTS Integrity Algorithm, UIA1
		0001_2	Standard UMTS Integrity Algorithm, UIA2
		0010_2	Standard UMTS Integrity Algorithm, UIA3
		0011_2 to 0111_2	Reserved for future expansion
		$1xxx_2$	Proprietary UMTS Algorithms

6.4.6 UIA negotiation

Not more than [n] versions of the UIA algorithm will be defined.

When an MS wishes to establish a connection with the network, the MS shall indicate to the network in the MS/USIM classmark which version of the UIA algorithm the USIM supports.

Note: This message itself must be integrity protected itself which effectively means that there must be at least one UIA algorithm in common, otherwise the connection is released.

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 UEA algorithm for use on that connection.

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

6.4.7 Integrity protection procedures

Note: The integrity protection procedures are for further study.

6.4.7.1 Handover

Note: It is expected that in case of inter-operator handover a handover agreement exists that covers all charging aspects. Agreements on cipher key transportation/re-use shall also be included.

1) Intra-system:

When a handover occurs, the IK is transmitted within the system infrastructure from the old RNC to the new one to enable the communication to proceed, and the synchronisation procedure is resumed. The key IK remains unchanged at handover.

2) Inter-system/ (between 2G and other 3G mobile radio systems and UMTS):

The following functionality has to be provided.

2G and other 3G mobile radio systems → UMTS

The UMTS network entered by the user handing over from other systems will enable integrity protection. This will involve setting the integrity protection key. There are two options:

a) Establishing the integrity protection key (with UMTS key formats) using the UMTS authentication and key agreement mechanism.

b) Deriving of integrity protection key (with UMTS key formats) from the existing cipher key (e.g. GSM formats).

Note 1: One of the two possibilities a), b) has to be chosen and agreed!

Note 2: A third option may be that a user at handover to the UMTS network returns to a previously visited UMTS network, with which he still shares a cipher and integrity key (e.g., because he was handed over from that UMTS network to the 2G or other 3G mobile radio system previously, during the same call). M

UMTS → other systems

The integrity protection key has to be deleted securely.

Note: Rather than deleting the integrity key, the UMTS network may store the integrity key securely for use in case the user would return to the UMTS network in a second handover.

6.5 Local authentication

Note: This section should define a mechanism for authentication based on a shared integrity key. It is ffs. whether a separate mechanism is required, or whether the security feature is implicitly provided through the use of the integrity key for signalling messages.

6.6 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 clause 6.1), the Temporary Mobile User Identity must be transferred in a protected mode at allocation time and at other times when the signalling procedures permit it. The confidentiality of user traffic concerns the information transmitted on traffic channels.

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

6.6.2 Ciphering algorithm

Algorithm UEA is implemented in both the MS and the RNC. On the RNC side the description below assumes that one algorithm UEA is implemented for each dedicated physical channel [not yet decided]. The data flow on dedicated channels is ciphered by a bit per bit or stream cipher generated by an algorithm UEA.

The UEA shall produce one output as a sequence of keystream bits referred to as a Key Stream Segment (KSS). A KSS of length n shall be produced to encrypt a given segment of plaintext of length n. The bits of KSS are labelled KSS(0), …KSS(n-1), where KSS(0) is the first bit output from the generator. The bits in the KSS shall be used to encrypt or decrypt the data.

Note: [The point at which confidentiality protection is applied in the UTRAN architecture is for further study. At this stage we assume that confidentiality protection is applied at the RNC.]

6.6.3 Cipher key establishment

The establishment of a new cipher key CK is integrated in the user authentication mechanism described in 6.3. A new cipher key CK is established each time an authentication protocol is executed between the USIM and the core network node that initiated the authentication.

6.6.4 Cipher key selection

Because of the separate mobility management for CS and PS services, the USIM establishes cipher keys with both the CS and the PS core network nodes. Currently two options are considered for the selection of the cipher key:

6.6.4.1 Option 1: Two key solution

The CS user data connections are ciphered with the most recent cipher key CK_{CS} agreed between the user and the 3G CS core network node. The PS user data connections are ciphered with the most recently cipher key CK_{PS} agreed between the user and the 3G PS core network node. The (common) signalling data connections are ciphered with the most recently cipher key established between the user and the network, i.e., the youngest of CK_{CS} and CK_{PS}. This requires that the cipher key of an (already ciphered) ongoing signalling connection is changed. This change should be completed within five seconds after an authentication and key establishment protocol has been executed.

6.6.4.2 Option 2: One key solution

All connections (CS user data, PS user data and signalling data) are ciphered with the most recently cipher key CK agreed between the user and either one of the core network nodes. This requires that the cipher key of any (already ciphered) ongoing connection is changed. This change should be completed within five seconds after an authentication an key establishment protocol has been executed.

6.6.5 Key set identifier

The key set identifier (KSI) is a number which is associated with the cipher and integrity keys derived during authentication. It is stored together with the cipher and integrity keys in the MS and in the network.

The key set identifier is used to allow key re-use during subsequent connection set-ups. The KSI is used to verify whether the MS and the SN are to use the same cipher key and integrity key.

6.6.6 Cipher key lifetime

A mechanism is needed to ensure that a particular cipher key is not used for an unlimited period of time to avoid attacks using compromised keys. Authentication and key agreement which generates new cipher keys is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. The USIM shall therefore contain a mechanism to limit the number of calls that can be made with a specific cipher key.

Operators shall decide on the value of this number of calls, and write this parameter on the USIM. The USIM shall have a counter that counts the number of times the cipher key is used and shall trigger the generation of a new cipher key if the counter reaches the maximum value set in the USIM. This mechanism will ensure that an cipher key cannot be reused more times than the limit set by the operator.

The cipher key lifetime is linked to the integrity key lifetime.

Note: The decision on when a key needs to be updated may depend on a number of factors, including the time since the last key update, the amount of data protected using that key, and the cost/value of the services protected through the use of that key. Unfortunately they cannot be easily measured by the USIM, so it is suggested that the number of calls made using the key should be measured instead. Some concern exists whether this is a good enough measure. Should also the (periodic) in-call authentication messages be counted, such that long calls weigh more than short calls? Should also the authentications through the use of the shared integrity call be counted?

6.6.7 UEA numbering

[The following table is for illustration only]

Table Error! Style not defined..Error! Bookmark not defined. **– UEA numbering**

Information Element	Length	Value	Remark
UEA Number	4	0000_2	Standard UMTS Encryption Algorithm, UEA1
		0001_2	Standard UMTS Encryption Algorithm, UEA2
		0010_2	Standard UMTS Encryption Algorithm, UEA3
		0011_2 to 0111_2	Reserved for future expansion
		$1xxx_2$	Proprietary UMTS Algorithms

6.6.8 UEA negotiation

Not more than [n] versions of the UEA algorithm will be defined.

When an MS wishes to establish a connection with the network, the MS shall indicate to the network which version of the UEA algorithm it supports.

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

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

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

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

6.6.9 Ciphering procedures

6.6.9.1 Starting of the ciphering and deciphering processes

The MS and the RNC must co-ordinate the instants at which the enciphering and deciphering processes start.

This procedure takes place under the control of the network some time after the completion of the authentication procedure (if any), or after the key CK has been made available at the RNC.

No information elements for which protection is needed must be sent before the ciphering and deciphering processes are operating.

The transition from clear text mode to ciphered mode proceeds as follows: deciphering starts in the RNC, which sends in clear text to the MS a specific message, here called "Start cipher". Both the enciphering and deciphering start on the MS side after the message "Start cipher" has been correctly received by the MS. Finally, enciphering on the RNC side starts as soon as a frame or a message from the MS has been correctly deciphered at the RNC.

[diagram to be added]

6.6.9.2 Synchronisation

The enciphering stream at one end and the deciphering stream at the other end must be synchronised, for the enciphering bit stream and the deciphering bit streams to coincide.

Synchronisation is guarantied by driving UEA by an explicit time variable, COUNT, derived from an appropriate frame number available at the MS and at the RNC.

The diagram below summarises the implementation indications listed above, with only one enciphering/deciphering procedure represented (the second one for deciphering/enciphering is symmetrical).

[diagram to be added]

6.6.9.3 Handover

Note: It is expected that in case of inter-operator handover a handover agreement exists that covers all charging aspects. Agreements on cipher key transportation/re-use shall also be included.

1) Intra-system

When a handover occurs, the CK is transmitted within the system infrastructure from the old RNC to the new one to enable the communication to proceed, and the synchronisation procedure is resumed. The key CK remains unchanged at handover.

2) Inter-system

The following functionality has to be provided.

2G and other 3G mobile communications systems → UMTS

The UMTS network entered by the user handing over will enable integrity protection. This will involve setting the integrity protection key. There are two options:

a) Establishing the cipher key CK (with UMTS key format) using the UMTS authentication and key agreement mechanism.

b) Deriving of cipher key (with UMTS key formats) from the existing cipher key (e.g. GSM formats).

UMTS → 2G and other 3G mobile communications systems

a) Establishing the system specific security key (e.g. in case of GSM: cipher key Kc with GSM key format) using the system specific key agreement mechanisms.

b) Deriving the system specific security keys (e.g. in case of GSM: cipher key K_C with GSM key format) from the UMTS cipher key.

Note: One of the two possibilities a), b) has to be chosen and agreed!

7 Network domain security mechanisms

The authentication and key agreement scheme assumes that authentication information passed between network nodes in appropriate signalling information elements is adequately protected. Also administrative network element commands, e.g. HLR Reset, have to be protected.

This subclause describes mechanisms for establishing secure signalling links between network nodes, in particular between SN/VLRs and HE/AuCs. Such procedures may be incorporated into the roaming agreement establishment process.

Note: Mechanisms are required to allow all SN-HE pairs to establish a secure signalling connection. These mechanisms could be part of the roaming agreement establishment process between operators. In addition to the usual signalling link establishment and testing, the SN-HE pair could agree on algorithms and keys for protecting signalling links.

The mechanism described in annex E ‘A Proposal for Securing SS7 Based Transmission of Sensitive Data between Network Elements’ will be used as a basis for further developments.

8 User domain security mechanisms

8.1 User-USIM Authentication

8.1.1 Overview

The User-USIM Authentication (UUA) mechanism provides access control to particular files on the USIM.

Each file in the USIM is under access control. To that extent each file is associated to a user name (UN). Each (UN) has the following attributes:

1) Expected user response (XUR): a value stored in the USIM to verify the responses of the user, as it is described in 8.1.2. This value may be modified by the procedure described in 8.1.5.

2) Activity state: either ENABLED or DISABLED. If enabled, access is granted only when the user has identified himself. The transition between the two states is defined by the procedures described in 8.1.3 and 8.1.4.

3) Block state: either BLOCKED or UNBLOCKED. A UN gets blocked when the number of consecutive failed authentication attempts for that UN reaches a certain threshold. The user name can be unblocked after a successful User-USIM authentication for a UN* that controls access to the Block state of the UN.

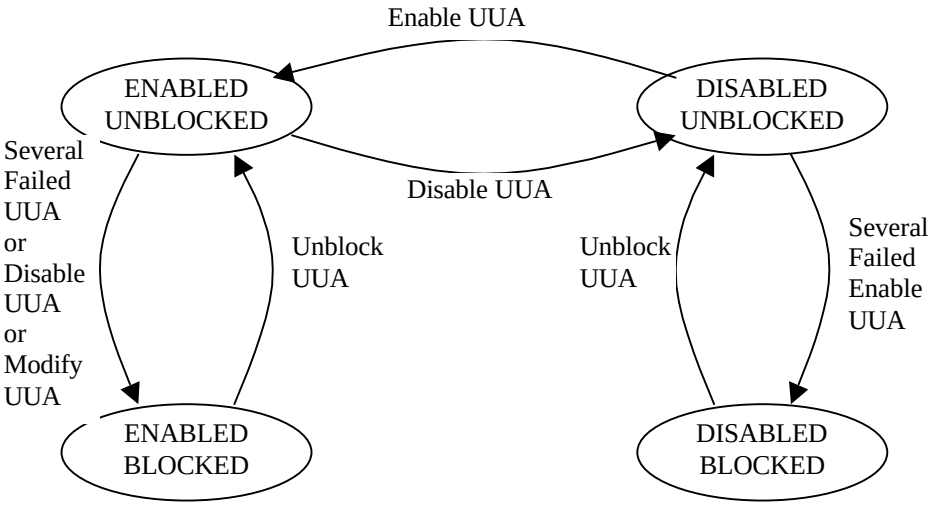

Figure 11: User-USIM Authentication State Model

8.1.2 User-USIM Authentication

This procedure allows the USIM to corroborate the user identity.

The procedure is described in Figure 12.

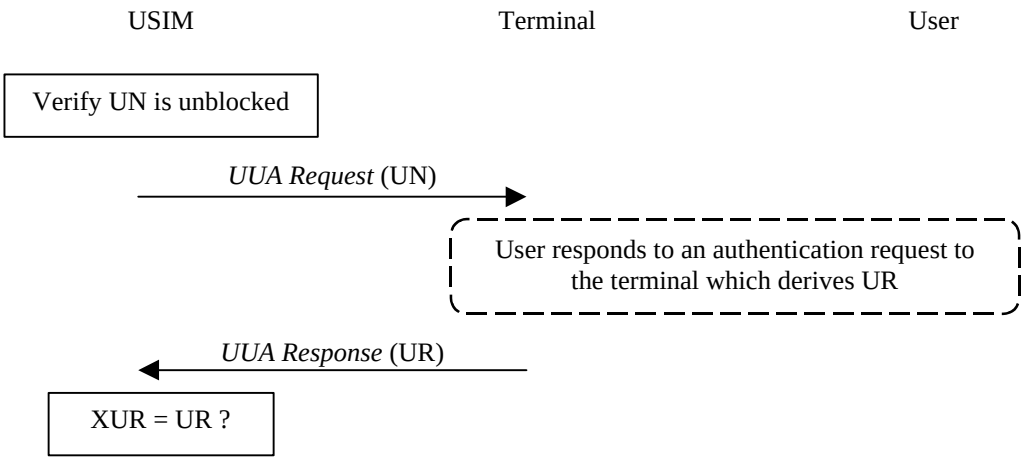

Figure 12: User-USIM Authentication

The procedure is invoked by the USIM when a user attempts to access certain restricted files in the USIM that are associated to a User Name (UN) and User-USIM Authentication for that UN is enabled. Depending on the access rights for the files, access is granted for the execution of a single action or for the duration of a USIM session.

The USIM verifies whether the state of the UN is unblocked. If UN is blocked, the procedure is terminated unsuccessfully, i.e., access to the file is not granted.

If the UN is unblocked, the USIM sends a *UUA request* to the terminal to authenticate the user. This request includes the UN that is associated to the file. The terminal then initiates an authentication procedure with the user. This typically involves a request to the user, a response from the user and may involve some processing to transform the response from the user into a standardised format. The terminal then sends *UUA response* that includes the user response (UR) back to the USIM.

Upon receipt of that message the USIM compares the received UR with the stored XUR associated to the UN. If there is a match, the authentication failure counter for that user name is reset to zero and the procedure is terminated successfully.

Otherwise, the USIM increases the authentication failure counter by one. If that counter reaches a certain threshold value, the USIM will enter blocked mode for that user and refuse to initiate any further User-USIM Authentication procedures. The procedure is ended unsuccessfully, i.e., access to the file is not granted.

8.1.3 Enable User-USIM Authentication for a user name

This procedure is used by the user to enable the User-USIM Authentication procedure.

The procedure is described in Figure 13.

The procedure is initiated by the user who enters a request to enable User-USIM Authentication for a particular UN. The terminal forwards that request to the USIM. Upon receipt of the request the USIM verifies whether the user state is set to DISABLED. If this is not the case the procedure is abandoned unsuccessfully.

The USIM then invokes the User-USIM Authentication procedure described in 8.1.2. If this procedure is ended successfully, the state of UUA for the user is set to ENABLED.

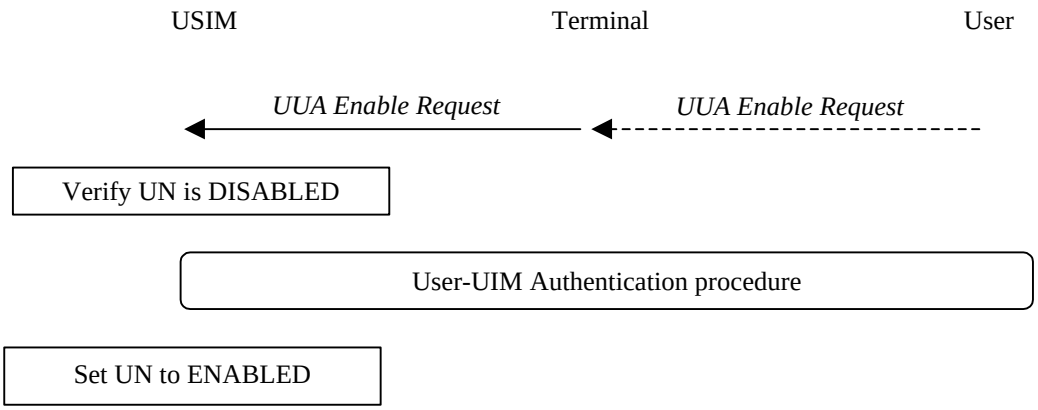

Figure 13: Enable User-USIM Authentication

8.1.4 Disable User-USIM Authentication

This procedure is used by the user to disable the User-USIM Authentication procedure.

The procedure is described in Figure 14.

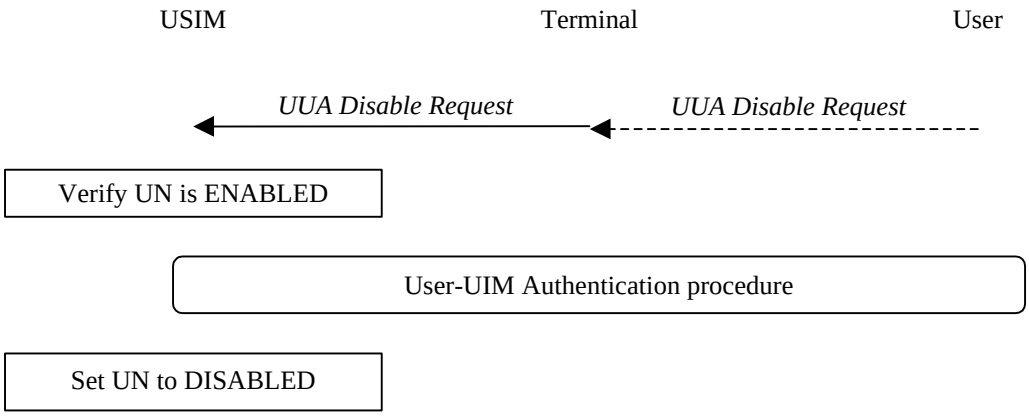

Figure 14: Disable User-USIM Authentication

The terminal initiates the procedure sending a request to the USIM. The USIM then checks whether the User-USIM Authentication is enabled. If this is not the case, the procedure is abandoned unsuccessfully.

The USIM then initiates the User-USIM Authentication procedure described in 8.1.2. If this procedure is ended successfully, the UUA state for the user is set to DISABLED.

8.1.5 Modify expected user response

This procedure is used by the user to modify the expected user response for a user name.

The procedure is described in Figure 15.

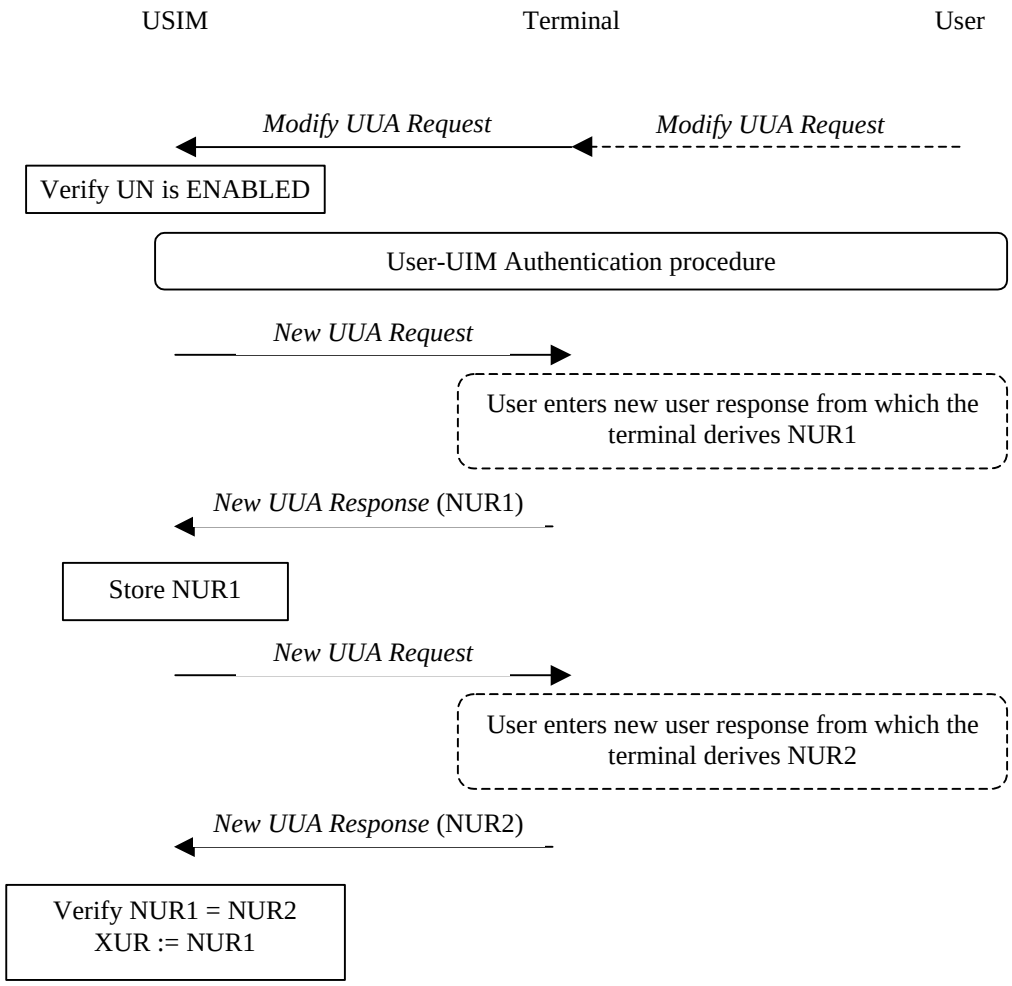

Figure 15: Modify expected user response

The procedure is invoked by the user who enters a request to modify the XUR for a UN. The terminal forwards the request to the USIM. The USIM then checks whether the User-USIM Authentication is enabled for that user name. If this is not the case, the procedure is ended unsuccessfully.

The USIM then initiates the User-USIM Authentication procedure described in 8.1.2. If this procedure is ended successfully, the user is asked a first time to enter his new user response. This value is subsequently stored in the USIM and the user is requested a second time to enter his new user response. The value received the second time is compared with the value received the first time. If both are unequal, the procedure is ended unsuccessfully without changing the expected user response. If there is a match the user response is modified accordingly to the new value.

8.1.6 Unblock User-USIM Authentication

This procedure is used by the user to unblock a user name. The procedure is described in Figure 16.

The procedure is invoked by a user request. The terminal forwards the request to the USIM. Upon receipt the USIM verifies that the user name is BLOCKED. If this is not the case, the procedure is abandoned.

The USIM invokes the User-USIM Authentication procedure for the user name UN* that controls the block state of the user name. If User-USIM authentication is ended successfully for UN*, the block state for UN is set to UNBLOCKED and the failure counter is reset to zero.

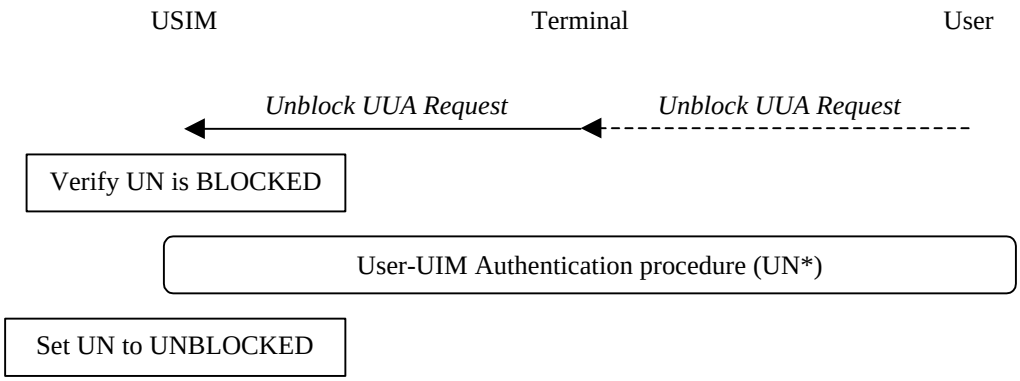

Figure 16: Unblock User-USIM Authentication

8.2 USIM-Terminal Lock

Note: The text included here is written starting from GSM 11.11. It should be compared with GSM 02.22 and it should be studied whether the mechanisms specified in there can be used as a basis for the specification of user-USIM authentication is UMTS.

8.2.1 Overview

This mechanism allows the owner of mobile equipment who is at the same time the user associated to a USIM, to restrict the usage of certain mobile equipment to his USIM.

The mechanism assumes that two passwords V1 and V2 are stored permanently in the USIM. Furthermore, it assumes that two user names are defined in the USIM: UN1 and UN2. Access to V1 is granted after an authentication as UN1 or UN2, access to V2 is granted after an authentication as UN2.

The mechanism consists of three procedure: 1) a procedure to enable the lock, whereby the USIM exports both passwords, 2) a procedure to verify the USIM by the terminal, whereby the USIM exports V1 which is verified by the terminal, and 3) a procedure to disable the lock, whereby the USIM exports V2.

8.2.2 Enable USIM-Terminal Lock

This procedure is used to lock a terminal and a USIM.

The procedure is described in Figure 17.

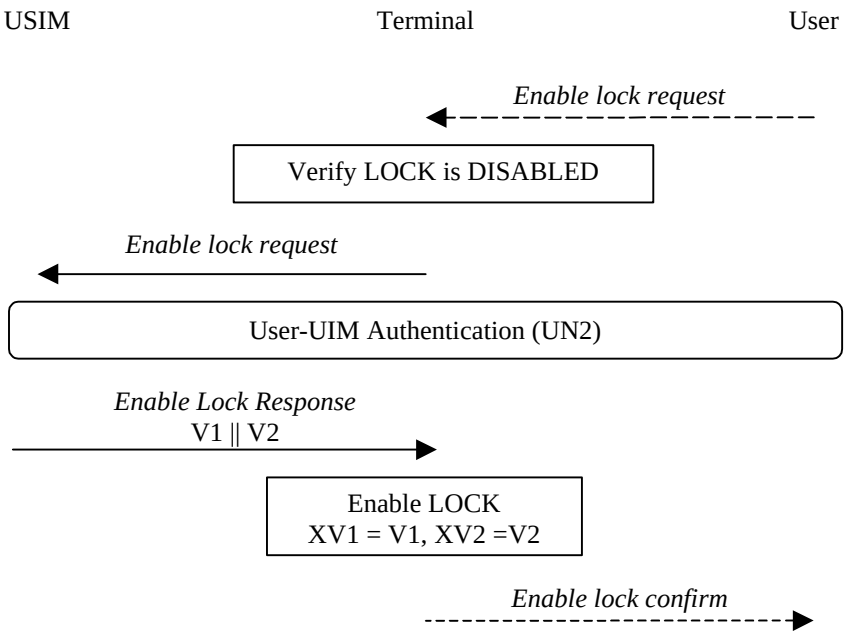

Figure 17: Enable USIM-Terminal lock

The user enters a request to enable the USIM-terminal lock. The terminal first verifies the lock state is set to DISABLED. Only if this is the case, the terminal sends a request to the USIM to enable the USIM-terminal lock. Upon receipt, the USIM initiates a User-USIM Authentication for the user name UN2. If that procedure is successful, the USIM sends V1 and V2 to the terminal. Upon receipt the terminal sets the USIM-terminal LOCK STATE to ENABLED and stores V1 and V2 in protected memory.

8.2.3 USIM-terminal authentication

This procedure is used to authenticate the USIM.

The procedure is described in Figure 18:

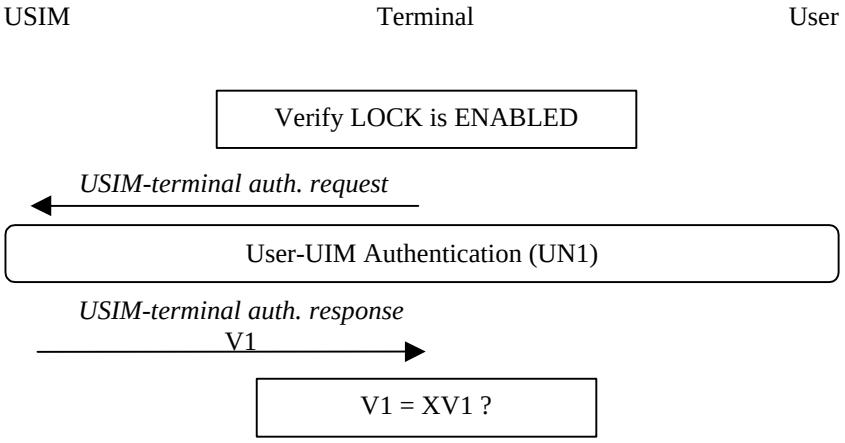

Figure 18: USIM-terminal Authentication

If the mobile station is powered-on or a USIM is inserted in the terminal and the USIM-terminal LOCK STATE in the terminal is set to ENABLED, the terminal sends a request to the USIM to authenticate. If the user-USIM authentication for UN1 is enabled, the USIM initiates a procedure to authenticate the user. If the authentication is disabled or if it is enabled and the authentication is successful, the USIM sends V1 to the terminal. Upon receipt the terminal compares the received value with the one which is stored in protected memory. If there is a match the procedure ends successfully. Otherwise, the terminal refuses operation.

8.2.4 Disable USIM-terminal Lock

This procedure is used to unlock a terminal and a USIM.

The procedure is described in Figure 19.

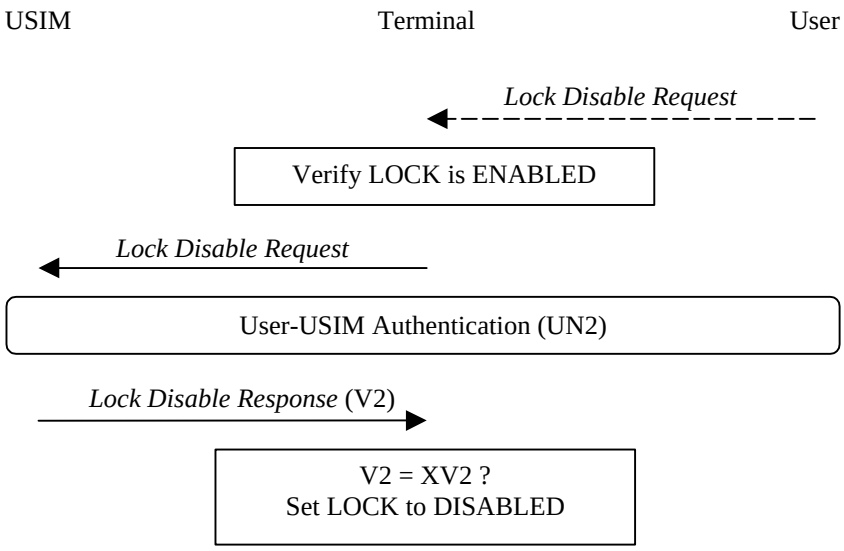

Figure 19: Disable USIM-terminal lock

The user enters a request to disable the USIM-terminal lock. The terminal first verifies the USIM-terminal LOCK STATE is set to ENABLED. Only if this is the case, the terminal sends a request to the USIM to disable the USIM-terminal lock. Upon receipt, the USIM initiates a User Authentication for the user name UN2. If the user authentication is successful, the USIM sends V2 to the terminal. Upon receipt the terminal compares the received value with the value stored in its protected memory. If there is a match the terminal sets the LOCK to DISABLED and removes XV1 and XV2 from protected memory.

9 Application security mechanisms

9.1 Secure messaging between the USIM and the network

This clause will specify the structure of the secured messsages 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.

9.2 Network-wide user traffic confidentiality

9.2.1 Introduction

Subclause 6.6 specifies how signalling information, user identity and user traffic information may be confidentiality protected by providing a protected mode of transmission on dedicated channels between the UE and the RNC. Network-wide confidentiality is an extension of this security feature which provides a protected mode of transmission on user traffic channels across the entire network. This gives users assurance that their traffic is protected against eavesdropping on every link within the network, i.e. not just the particularly vulnerable radio links in the access network, but also on the fixed links within the core network.

If network-wide confidentiality of user traffic is provided we assume that access link confidentiality of user traffic between UE and RNC will be replaced with the network-wide service. However, we note that access link confidentiality of signalling information and user identity between UE and RNC will be applied regardless of whether the network-wide user traffic confidentiality service is applied or not.

The provision of an network-wide confidentiality service in 3GMS has an obvious impact on lawful interception. We assume that the same lawful interception interface is required in 3GMS as in second generation systems regardless of whether network-wide confidentiality is applied by the network or not. Thus, we assume that it must be possible to remove any network-wide confidentiality protection within the core network to provide access to plaintext user traffic at the lawful interception interface.

We assume that network-wide confidentiality will be provided by protecting transmissions on user traffic channels using a synchronous stream cipher. This will involve the specification of a standard method for ciphering user traffic on an end-to-end basis and a standard method for managing the ciphering key required at the end points of the protected channel.

9.2.2 Ciphering method

It is assumed that the network-wide encryption algorithm shall be a synchronous stream cipher similar to the access link encryption algorithm. Indeed, it would be desirable to use the same algorithm for access link encryption and for network-wide encryption.

The network-wide synchronous stream cipher shall contain a key stream generator which shall have (at least) two inputs: the end-to-end cipher key (Ks) and an initialisation value (IV). The plaintext shall be encrypted using the key stream by applying an exclusive-or operation to the plaintext on a bit per bit basis to generate the ciphertext. The decryption operation shall involve applying the same key stream to the ciphertext to recover the plaintext.

Synchronisation of the key stream shall be achieved using the initialisation value. Synchronisation information shall be available at both end points of the communication and shall be used to maintain alignment of the key stream. For example, it might be necessary to transmit explicit end-to-end synchronisation frames with the user traffic at certain intervals. Alternatively, it might be possible to use some existing frame structure for network-wide encryption synchronisation purposes. The frequency at which synchronisation information must be made available at each end to ensure reliable transmission will depend on the exact nature of the end-to-end user traffic channel.

Protection against replay of user traffic shall be achieved through the use of a time variable initialisation vector combined with a time variable cipher key. If the same cipher key is used in more than one call then it may be necessary to include a third input to the key stream generator such as a call-id or a time-stamp to protect against replay of the whole call. Note that the stream cipher does not protect against bit toggling so other mechanisms must be used if this type of integrity protection is required on user traffic.

For encryption of voice traffic we assume that Transcoder Free Operation (TFO) is used between the two end points such that the structure and ordering of the transmitted data is maintained with the same boundary conditions at each end of the link. Note that in the initial phases of 3GMS, transcoder free operation may only be possible for user traffic channels which terminate within the same serving network. Furthermore, TFO may only be possible if the entire communication path is within the same serving network. Thus, in non optimal routing cases where the tromboning effect occurs, TFO may not be available, even if the traffic channel terminates within the same serving network.

For encryption of data traffic we assume that a transparent data service is used between the two end points such that the structure and ordering of transmitted data is maintained with the same boundary conditions at each end of the link.

To satisfy lawful interception requirements it must be possible to decrypt end-to-end encrypted traffic within the core network to provide access to plaintext user traffic. Thus decryption facilities (and the end-to-end encryption key) must be available in the core network for lawful interception reasons. Note also that if transcoder free operation is used on voice traffic channels, transcoders must be available in the core network for lawful interception reasons whether network-wide encryption is provided or not.

Issues for further study:

- Specification of encryption synchronisation mechanism;
- Adaptation of TFO voice traffic channels for network-wide confidentiality;
- Adaptation of data traffic channels for network-wide confidentiality;

- The ability to terminate network-wide encryption at network gateways for inter-network user traffic channels;
- The ability to handle multiparty calls, explicit call transfer and other supplementary services;
- Network-wide encryption control – algorithm selection, mode selection, user control

9.2.3 Key management

9.2.3.1 General case

We assume that signalling links within the network are confidentially protected on a link-by-link basis. In particular, we assume that the UE to RNC signalling links are protected using access link security domain keys (see clause 6). We also assume that VLR to RNC signalling links and core network signalling links are protected using network security domain keys (see clause 7). Note that if network-wide encryption can be provided across serving network boundaries (e.g. because inter-network TFO is available) then the signalling links requiring protection will cross network boundaries. In this situation it is important to note that the two serving networks may not be roaming partners yet they still must be able to confidentially protect inter-network signalling by establishing appropriate keys.

The key management scheme for network-wide encryption involves establishing an end-to-end session key between the end points of the traffic channel. It should not be possible to obtain this key by eavesdropping on any transmission links within the network. However, it may be possible to obtain the end-to-end key by compromising certain nodes within the network (e.g. nodes where link encryption terminates).

To satisfy lawful interception requirements it must be possible to decrypt end-to-end encrypted traffic within the core network to provide access to plaintext user traffic. Thus, the end-to-end encryption key (and decryption facilities) must be available in the core network for lawful interception reasons.

Issues for further study:

- Specification of key management scheme for the general case;
- – - The ability to terminate network-wide encryption key management at network gateways for inter-network user traffic channels.

9.2.3.2 Outline scheme for intra-serving network case

In this case we make the following assumptions:

- Two UEs registered on the same serving network wish to set up an network-wide confidentiality protected call
- The appropriate user traffic channel for encryption can be established between the two UEs
- During connection establishment, the appropriate control information is transmitted to the called party indicating that the incoming connection is end-to-end encrypted.
- During connection establishment, the appropriate control information is transmitted to the relevant VLRs (or other core network entities) indicating that the connection being established is end-to-end encrypted.
- The keys Ka and Kb used to derive the end-to-end session key shall not be used for access link encryption of other data, nor for the derivation of end-to-end session keys with other parties.

The key management scheme is illustrated in the diagram below.

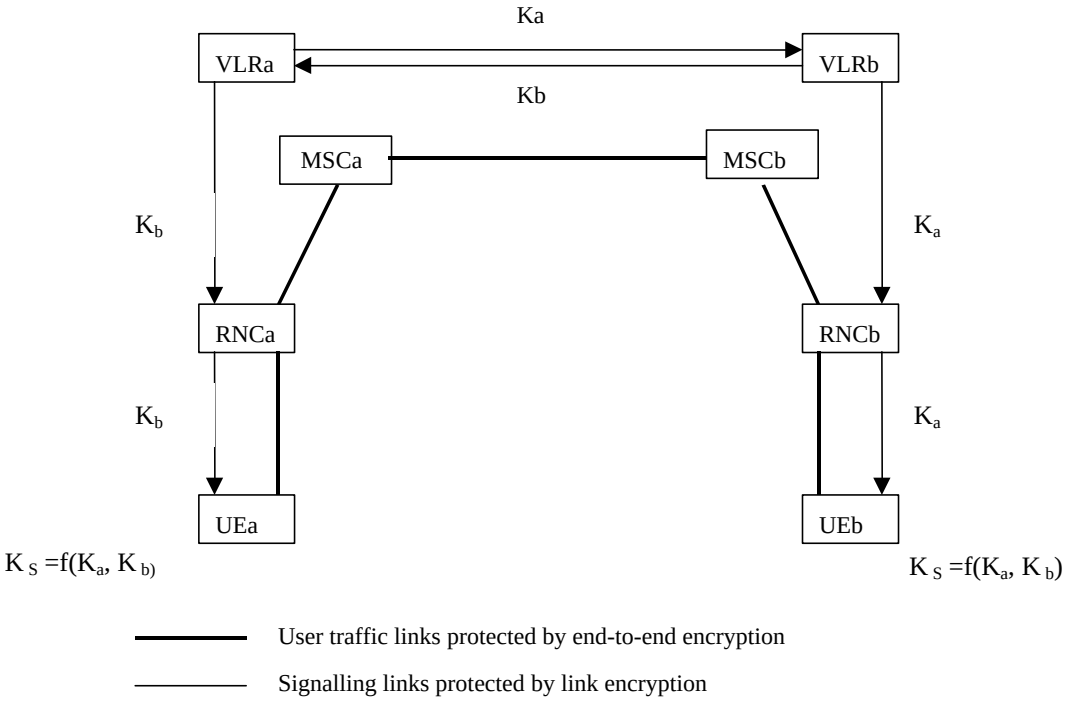

Figure 20: Key management scheme for network-wide encryption

In this scheme VLRa and VLRb exchange access link cipher keys for UEa and UEb. VLRa then passes Kb to UEa, while VLRb passes Ka to UEb. At each end the access link key is transmitted to the UE over protected signalling channels (which may be protected using different access link keys Ka' and Kb'). When each UE has received the other party's access link key, the end-to-end session key Ks is calculated as a function of Ka and Kb.

This key management scheme satisfies the lawful interception requirement since Ks can be generated by VLRa or VLRb and then used by decryption facilities in the core network to provide plaintext user traffic at the lawful interception interface.

Issues for further study:

- The exact mechanism by which the VLRs exchange access link keys during connection set up.

9.2.3.3 Variant on the outline scheme

VLRa and VLRb mutually agree Ks over a secure signalling link using an appropriate key agreement protocol. VLRa then passes Ks to UEa and VLRb passes Ks to UEb.

Note: As opposed to the scheme in section 9.2.3.2, the access link keys Ka and Kb could be used for access link encryption of other data.

9.3 IP security

[ffs]

Annex A:
Requirements analysis

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

Annex B:
Enhanced user identity confidentiality

This mechanism allows the identification of a user on the radio access by means of the permanent user identity encrypted by means of a group key. The mechanism described here can be used in combination with the mechanism described in 6.2 to provide user identity confidentiality in the event that the user not known by means of a temporary identity in the serving network.

The mechanism assumes that the user belongs to a user group with group identity GI. Associated to the user group is a secret group key GK which is shared between all members of the user group and the user's HE, and securely stored in the USIM and in the HE.

The mechanism is illustrated in Figure B.1.

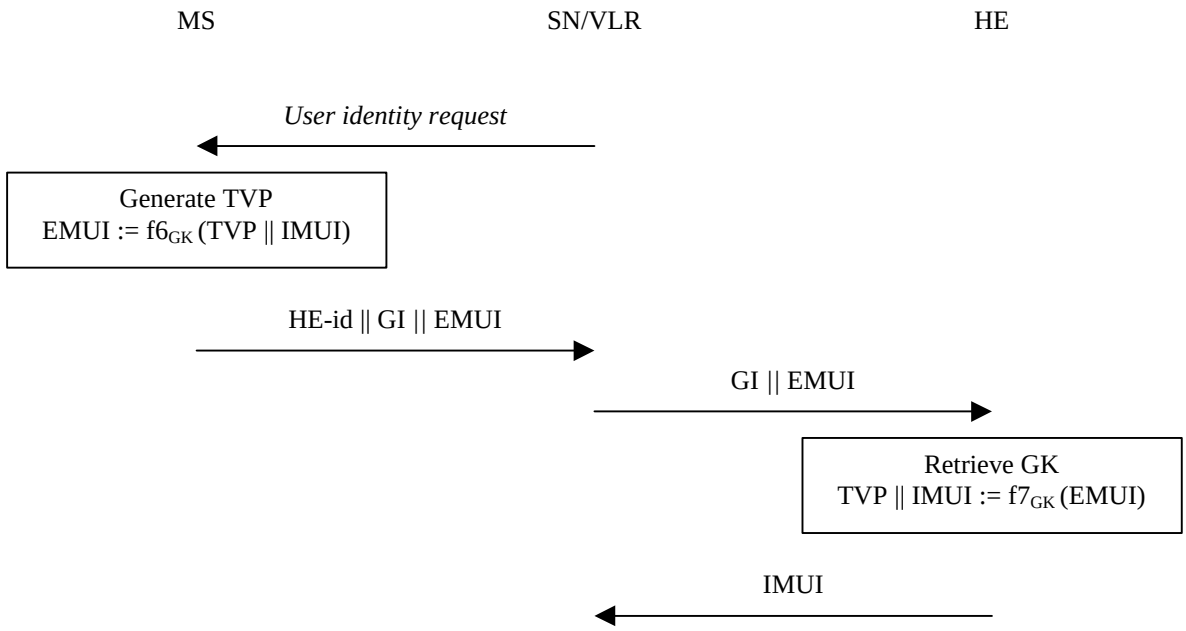

Figure B.1: Identification by means of the IMUI encrypted by means of a group key

The user identity procedure is initiated by the visited VLR. The visited VLR requests the user to send its permanent user identity.

Upon receipt the user generates a time variant parameter TVP. The user encrypts the time variant parameter TVP and the IMUI with enciphering algorithm f6 and his group key GK. The TVP prevents traceability attacks. The user sends a response to the VLR that includes the HE identity, the group identity GI and the encrypted mobile user identity (EMUI).

Upon receipt of that response the SN/VLR should resolve the user's HE address from HE-identity and forwards the group identity GI and the user's EMUI to the user's HE.

Upon receipt the HE retrieves the group key GK associated with the group identity GI. The HE then decrypts EMUI with the deciphering algorithm f7 ($f7 = f6^{-1}$) and the group key GK and retrieves TVP and IMUI. The HE then sends the IMUI in a response to the visited SN/VLR.

Annex C:
Management of sequence numbers

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

C.1 A mechanism using two individual counters on each side

This is the mechanism included in the main body of this specification.

C.2 A mechanism using a global counter in the HE and two counters in the MS

In this mechanism the HLR/AuC keeps track of time, while the USIM keeps track of a counters for PS mode $SQN_{MS/PS}$ and a counter for CS mode $SQN_{MS/CS}$.

The HLR/AuC may for instance use as a sequence number the number of seconds t that have elapsed since the start of the year 2000 (GMT). Then, a 32-bit sequence number will suffice for 136 years of operation. When an array of n authentication vectors is generated, the values t, t+1, …, t+n-1 could be used.

At the user end, SQN is treated as in the mechanism described under C.1.

Note 1: When using a time-value to generate sequence numbers it may not be necessary to conceal the sequence number to avoid user identification.

Note 2: The re-synchronisation procedure is not required in this case, as time can be recovered from any source.

C.3 A mechanism using two individual counters in the HE and a window in the USIM

In this mechanism the sequence numbers are generated as in the mechanism described in C.1. However, the USIM verifies the freshness differently. In addition to the highest sequence number SQN_{MS} it has accepted, it keeps track of which values in a window ($SQN_{MS,}$ $SQN_{MS} - w$] it has already seen, and this for each mode. If a sequence number is received that is lower than SQN_{MS} but has not been seen before, it is nevertheless accepted.

Using this mechanism, it is not required that a previously visited SN/VLR deletes the unused authentication vectors when a user de-registers from the network and may be more efficient as regards long distance signalling when a user abroad switches a lot between two serving networks.

Note: 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 use before (because w is 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.

C.4 A mechanism using a global counter in the HE and a list in the USIM

In this mechanism the sequence numbers are generated as in the mechanism described in C.2. However, the USIM verifies the freshness differently. Instead of keeping track of the highest sequence number SQN_{MS} only, it keeps track of

an ordered list of the b highest values is has received, and this for each mode. If a sequence number is received that is lower than the lowest value in that list, it is rejected. If however, a sequence number is received that is larger than the lowest, but lower than the highest sequence number and was not seen before it is accepted and included in the list.

Using this mechanism, it is not required that a previously visited SN/VLR deletes the unused authentication vectors when a user de-registers from the network and may be more efficient as regards long distance signalling when a user abroad switches a lot between two serving networks.

Note: 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 use before (because b is 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.

Annex D:
A mechanism for authentication based on a temporary key

D.1 Authentication based on a Temporary Key

D.1.1 General

The mechanism described here achieves mutual authentication and key agreement between the USIM and the AuC in the user's HE, showing knowledge of a secret key K which is shared between and available only to these two parties. The temporary key generated during the protocol is shared with the visited SN/VLR, and can be used subsequently with the local authentication and session key agreement protocol described in section D.2 or with the other local authentication mechanisms described in section Local authentication. Additionally, session keys for the first session are created during the protocol.

The method was chosen in such a way as to reduce signalling between the HE and the SN/VLR. The method is composed of a mutually authenticated challenge/response protocol with key agreement.

An overview of the mechanism is shown in Figure D.1.

When the mobile first requests service from the SN/VLR, a random seed RSu created by the user (USIM or terminal) is included in the request message. The message including RSu is forwarded to the HE/AuC, which generates its own random challenge RSn. An authentication vector is returned to the SN/VLR. The vector contains {RSn, RES1, XRES2, KT}, where RES1 is the response to the user's challenge, XRES2 is the response to the network's challenge which is expected from the user, and KT is the temporary authentication key shared with the SN/VLR. The network's challenge RSn and the network authentication response RES1 are sent to the MS. If the MS verifies RES1, thereby authenticating the identity of the network, it responds with RES2 and generates the new temporary key KT. The SN/VLR then verifies that RES2 equals XRES2, thereby authenticating the identity of the USIM, and stores the new temporary key KT. Furthermore, both the USIM and the SN/VLR immediately use KT with the random seeds RSu and RSn to generate the first session keys CK and IK. The established keys CK and IK will then be transferred by the USIM and the SN/VLR to the entities which perform ciphering and integrity functions.

The SN/VLR can offer secure service to the USIM without reference to the home system HE/AuC by using the temporary key KT. This local authentication mechanism is described in section D.2.

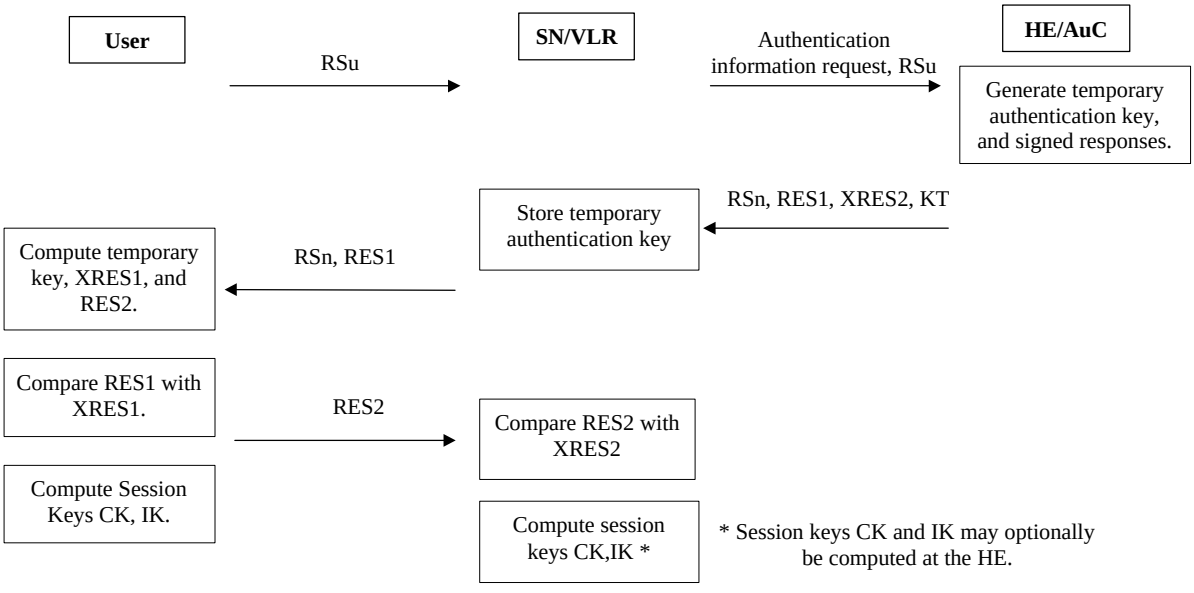

Figure D.1: Authentication

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 generate a new temporary authentication key and session keys, and distribute the temporary authentication key from the HE/AuC to the SN/VLR. This procedure is described in D.1.2. The SN/VLR 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 SN/VLR to the HE/AuC are adequately secure. Mechanisms to secure these links are described in clause 7. It is further assumed that the user trusts the HE.

A procedure to distribute the temporary authentication key from a previously visited VLR to the newly visited VLR. This procedure is described in D.1.3. It is also assumed that the links between SN/VLRs are adequately secure. Mechanisms to secure these links are described in clause 7.

D.1.2 Temporary Key Generation with Session Key Agreement

The services provided by this mutually authenticated key agreement protocol are:

- the SN/VLR authenticates the MS;
- the MS verifies that the SN/VLR is allowed to offer it services on behalf of its HE;
- the MS and the HE establish a new temporary authentication key with freshness guarantees to both parties;
- the HE distributes this temporary key to the SN/VLR for subsequent use in local authentication protocols; and,
- the MS and the SN/VLR establish new cipher and integrity keys with freshness guarantees to both parties.

The procedure is illustrated in Figure D.2.

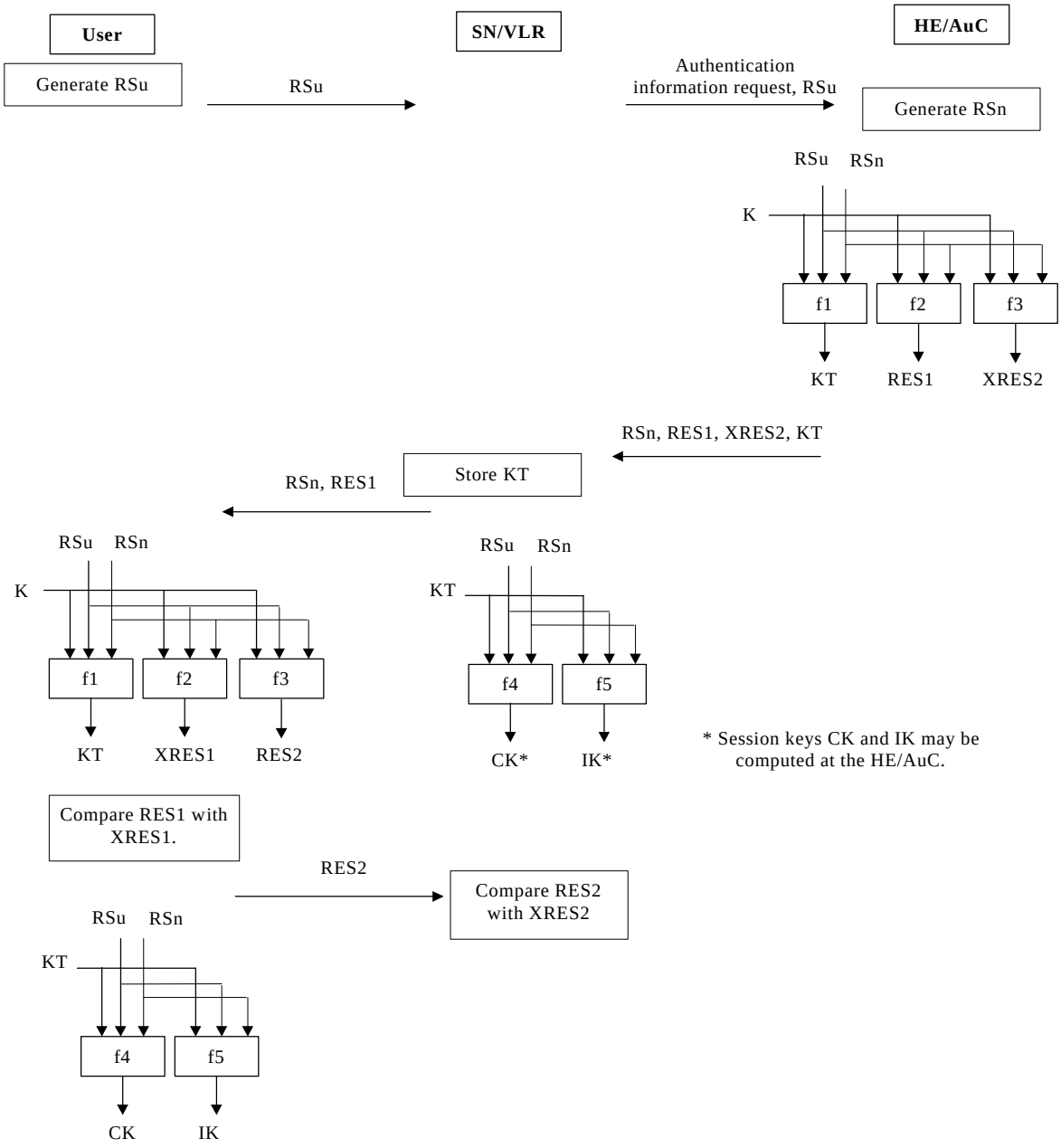

Figure D.2: Temporary Key Generation Protocol

The user (USIM/terminal) invokes the procedure by requesting service from the SN/VLR. This service request contains an unpredictable random seed RSu, generated by the user. The SN/VLR sends the HE/AuC an *authentication data request*, which includes RSu as well as either the IMUI or an EMUI for the user. In case an EMUI is used, the mechanism described in 6.2 is integrated in this procedure.

Upon the receipt of the authentication data request from the SN/VLR, the HE/AuC generates the authentication vector. To generate an authentication vector AV the HE/AuC generates an unpredictable random value RSn. Subsequently the following values are computed:

- a temporary key KT = $f1_K$(PAR1 || RSu || RSn) where f1 is a key generating function.

- an authentication response RES1 = $f2_K$ (PAR2 || RSu || RSn) where f2 is a (possibly truncated) MAC function.
- an expected response XRES2 = $f3_K$ (PAR3 || RSu || RSn) where f3 is a (possibly truncated) MAC function.

Note 1: The need for f2 and f3 to use a long-term key different from K is ffs.

Note 2: It is also ffs in how far the functions f1, ..., f5 need to differ and how they may be suitably combined.

Note 3: PAR1, ..., PAR5 are different fixed initial values which may be used when similar or identical functions are used for f1, ..., f5. The need for the inclusion of PAR1, ... PAR5 is ffs. When omitted they may be thought of as being integrated in the definition of the functions f1, ..., f5 respectively.

These authentication parameters are used to construct an ordered array of authentication vectors for the user consisting of {RSn, RES1, XRES2, KT}.

The HE/AuC sends the requested authentication vector to the SN/VLR in a response message.

The serving system SN/VLR may generate the session keys locally, or they may be generated by the HE/AuC and sent to the SN/VLR. In either case, the following session keys are computed:

- a cipher key CK = $f4_{KT}$ (PAR4 || RSu || RSn) where f4 is a key generating function.
- an integrity key IK = $f5_{KT}$ (PAR5 || RSu || RSn) where f5 is a key generating function.

Note 4: The requirements on f4 and f5 are ffs.

Note 5: (See notes 2 and 3 above).

The SN/VLR sends to the user the random challenge RSn and the network's authentication response RES1, taken from the authentication vector.

Upon receipt of RSn and RES1 the user first computes XRES1 = $f2_K$ (PAR2 || RSu || RSn) from RSu, RSn, and the secret key K, and compares this with the value of RES1 received from the SN/VLR. If they are unequal, the user sends a message back indicating that the authentication token was corrupt and abandons the authentication protocol. If the equality holds, the user has authenticated the identity of the home system.

The user then computes RES2 = $f3_K$ (PAR3 || RSu || RSn), which is sent back to the SN/VLR, and the temporary key KT = $f1_K$ (PAR1 || RSu || RSn). KT is subsequently used to generate the cipher key CK = $f4_{KT}$ (PAR4 || RSu || RSn) and the integrity key IK = $f5_{KT}$ (PAR5 || RSu || RSn). Note that if this is more efficient, XRES1, RES2, KT, CK and IK can be computed earlier at any time after receiving RSn (although KT must be computed before CK and IK).

When the SN/VLR receives RES2 it compares it with the expected response XRES2 from the selected authentication vector. If XRES2 equals RES2 then the user is authenticated. The SN/VLR also distributes the derived cipher key CK and derived integrity key IK to the appropriate entities for integrity and ciphering.

D.1.3 Distribution of temporary keys between VLRs

The purpose of this procedure is to provide a newly visited VLR with the current temporary authentication key from a previously visited VLR.

The procedure is initiated by the visited VLR and illustrated in the following figure:

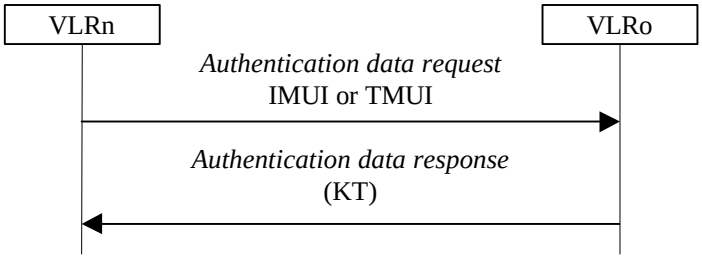

Figure D.3: Distribution of authentication data between VLRs

The procedure is invoked by the newly visited VLRn after a location update request of the user. Typically the user identifies himself using a temporary user identity TMUIo and the location area identity LAIo of a location area under the jurisdiction of VLRo. In that case this procedure is integrated with the procedure described in 6.1.

Upon receipt of the request the VLRo verifies whether it has a current temporary authentication key in its database and if so, sends the current temporary authentication key to VLRn. The previously visited VLRo deletes the temporary authentication key from its database.

Upon receipt the VLRn stores the temporary authentication key. If VLRo indicates that it has no current temporary authentication key or the VLRo cannot be contacted, VLRn should request new a authentication vector from the user's HE using the procedure described in D.1.2.

D.1.4 Handover

[More detailed description on handover from GSM to a TETRA-based network, and vice-versa, is ffs]

In case of handover the security level of the network entered by the user has to be fulfilled.

Therefore the following functionality has to be provided in case of handover:

Re-authentication using the (probably network specific) authentication mechanisms of the system entered by the user in case of handover.

Note: There is only one exception, when UMTS operators allow a user to roam in their networks with a GSM subscription.

Note: In case of inter-system/intra-operator handover (between GSM and UMTS) there is no strong requirement for re-authentication because of the original authentication having been done by the same operator, because of the service capabilities after handing over will be equivalent to GSM level. After service termination re-authentication and LUP has to be fulfilled as required for roamers.

This is restricted to phase 1. In future releases of phase 1 and later phases, mechanisms shall be specified to enable the level of security, after an inter-system or inter-operator handover, which normally is achieved in the radio network to which handover is done.

D.2 Local authentication

D.2.1 Session Key Agreement based on Temporary Authentication Key

The services provided by this mutually authenticated key agreement protocol are:

- the SN/VLR authenticates the MS;
- the MS verifies that the SN/VLR is allowed to offer it services on behalf of its HE;
- the MS and the SN/VLR establish new cipher and integrity keys with freshness guarantees to both parties.

The procedure is illustrated in figure D.4.

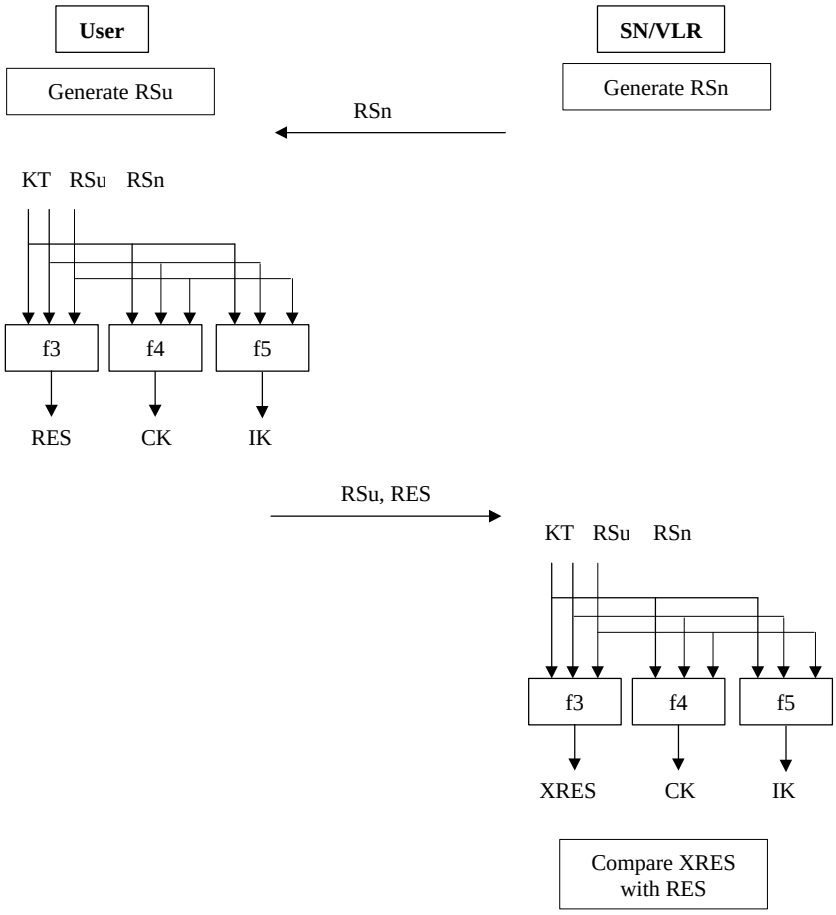

Figure D.4: Locally authenticated session key agreement

The SN/VLR initiates the procedure. It generates a unpredictable random challenge RSn which is sent to the user.

The user (USIM/terminal) generates its own random challenge RSu. Upon receipt of the network's challenge RSn, the user calculates the following values:

- an authentication response RES = $f3_{KT}$ (PAR3 || RSu || RSn) where f3 is a (possibly truncated) MAC function.
- a cipher key CK = $f4_{KT}$ (PAR4 || RSu || RSn) where f4 is a key generating function.
- an integrity key IK = $f5_{KT}$ (PAR5 || RSu || RSn) where f5 is a key generating function.

Note 1: (See notes 1-5 in Clause D.1.2)

The USIM/terminal sends the network the random challenge RSu and the authentication response RES, and distributes the session keys CK and IK to the appropriate entities for ciphering and integrity.

Upon receipt of RSu and RES the SN/VLR computes XRES = $f3_{KT}$ (PAR3 || RSu || RSn) from RSu, RSn, and the temporary authentication key KT that is stored in the VLR database, and compares this with the value of RES received from the user. If they are unequal, the network sends a message back indicating that authentication has failed and abandons the authentication protocol. If the equality holds, the user is authenticated to the network.

The SN/VLR then computes the ciphering key CK = $f4_{KT}$ (PAR4 || RSu || RSn) and the integrity key IK = $f5_{KT}$ (PAR5 || RSu || RSn), which it distributes to the appropriate entities for ciphering and integrity.

Annex E:
Proposal for Securing SS7 Based Transmission of Sensitive Data between Network Elements

(See: 3GPP TSGS3H#1(99)006, ETSI SMG 10 WPB SS7 adhoc Tdoc (99)009,
Source: T-Mobil, Mannesmann Mobilfunk, Deutsche Telekom, version: 1.1)

E.1 Scope and Objectives

The security of the global SS7 network as a transport system for sensitive signalling messages is open to major compromise. Messages can be eavesdropped, altered, injected or deleted in an uncontrolled manner. In this document a mechanism for securing the transmission of sensitive data, e.g. authentication material, between network elements belonging to different network operators is described. **2** The mechanism is aimed at confidentiality, authenticity and integrity of the messages exchanged.

E.2 Description of Mechanism

The mechanism consists of three layers:

Layer I is a secret key transport mechanism based on an asymmetric cryptosystem and is aimed at agreeing on a symmetric key for each direction of communication between two networks A and B. The party wishing to send sensitive data initiates the mechanism and chooses the symmetric key it wishes to use for sending the data to the other party. The other party may choose a symmetric key of its own, used for sending data in the other direction. The symmetric keys are protected by asymmetric techniques. They are exchanged between certain elements called the *Key Administration Centres* (KACs) of the network operators A and B.

In Layer II the agreed symmetric keys for sending and receiving data are distributed by the KACs in each network to the relevant network elements. For example, an AuC will normally send sensitive authentication data to VLRs belonging to other networks and will therefore get a "send"-key from its KAC. Layer II is carried out entirely inside one operator's network, so the details of Layer II can be left to the operators; however, the distribution of keys should be performed in a secure way as not to compromise the whole mechanism. **3**

Layer III uses the distributed symmetric keys for securely exchanging sensitive data between the network elements of different operators by means of a symmetric encryption algorithm.

Figure 1 may help to clarify the proposal. It provides an overview of the whole mechanism, while at the same time giving some more details on the single layers.

2 For secure transmission of sensitive data between elements of one and the same network operator only Layer II and Layer III will be involved. In this case Layer I can be dropped.

3 For example, it has been suggested to use the same mechanism for distributing the keys as in Layer I also for Layer II in order to achieve a more consistent overall scheme.

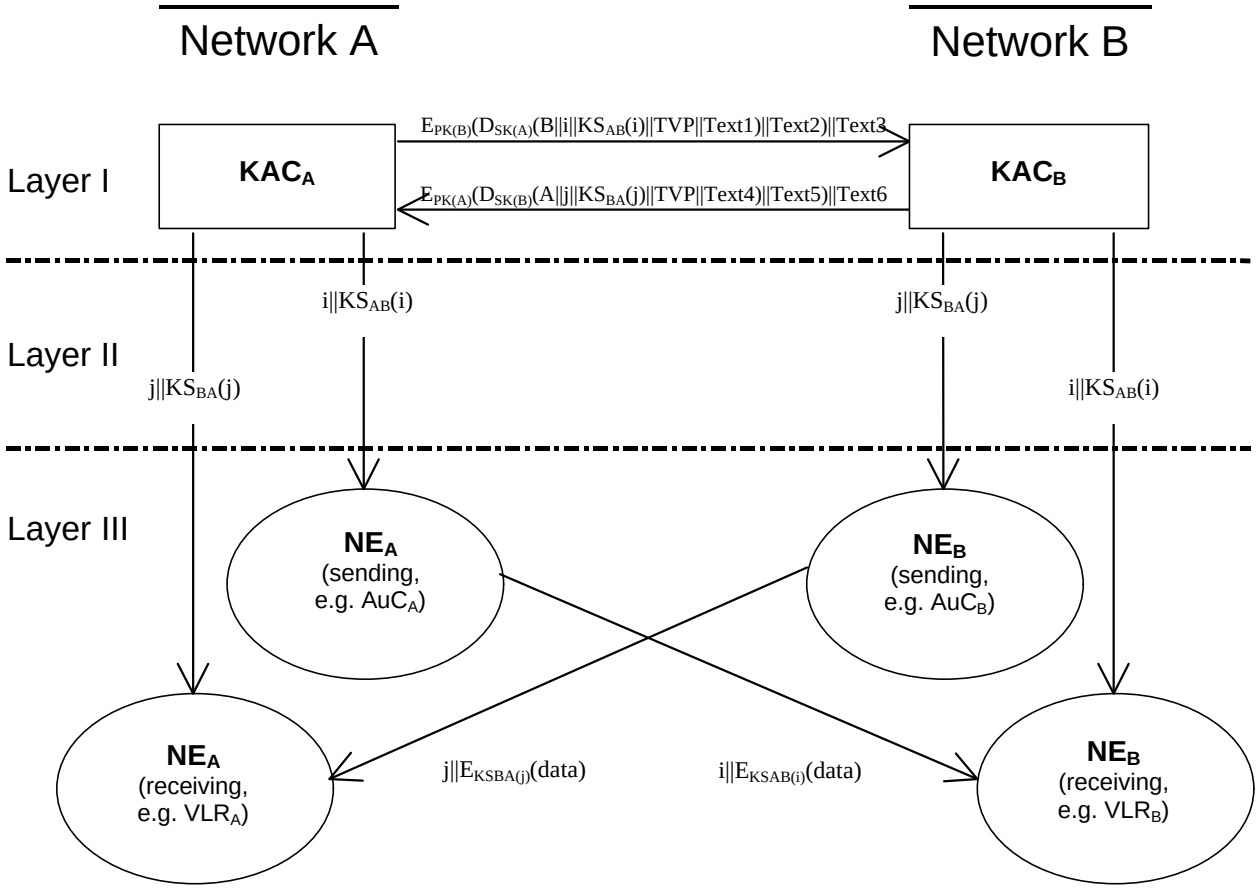

Figure E.1: Overview of Proposed Mechanism

E.2.1 Abbreviations

The following abbreviations are used in figure 1:

X	Placeholder for Network Operator Identifier A, B
KAC_X	Key Administration Centre of Network X
NE_X	Network Element of Network X
$KS_{XY}(i)$	Symmetric Session Key #i for sending data from X to Y
$KS_{YX}(j)$	Symmetric Session Key #j for sending data from Y to X
$E_{PK(X)}(data)$	Encryption of "data" with Public Key of X
$D_{SK(X)}(data)$	Decryption of "data" with Secret Key of X (i.e., X electronically signs "data")
TVP	Time Variant Parameter (e.g. Sequence Number or Time Stamp)
$E_{KSXY(i)}(data)$	Encryption of "data" with Symmetric Session Key #i for sending data from X toY
$E_{KSYX(j)}(data)$	Encryption of "data" with Symmetric Session Key #j for sending data from Y to X
i	Session Key Sequence Number (for sending data from X to Y)
j	Session Key Sequence Number (for sending data from Y to X)
$m_1 \| \| m_2$	Concatenation of message m_1 and m_2

E.2.2 Additional Remarks

1. In general a Public Key Infrastructure (PKI) is required to handle Public Keys and the appropriate certificates. For example, the Public Keys of the networks could be stored by a central server and Public Key certificates have to be issued. They can be appended to Layer I transmissions (the data fields Text3, Text6 may be used for this). Alternatively, Public Keys could also be exchanged between a pair of network operators when setting up a roaming agreement. In this case no PKI is required. [4]

2. The format of Layer I transmissions is based on ISO/IEC 11770-3: *Key Management – Mechanisms using Asymmetric Techniques*.

3. As already mentioned, the Layer II transmissions should be secured either by asymmetric or symmetric mechanisms. This is for further study.

4. For key synchronisation purposes a Session Key Sequence Numbers i, j are added.

5. The symmetric session keys $KS_{AB}(i)$, $KS_{BA}(j)$ should be periodically updated, thereby moving on to $KS_{AB}(i+1)$, $KS_{BA}(j+1)$.

6. Authenticity and integrity of the symmetric session keys in Layer I are achieved by the digital signature of the initiating network. Message integrity on Layer III may be achieved by adding a MAC to the Layer III messages.

7. Two issues are left open for further study, namely the impact of the proposed scheme on the overall signalling load and the question whether the MAP protocol has to be modified in order to cope with the encrypted messages of Layer III.

8. As is well known there are also special potentially sensitive (and dangerous) commands within SS7 protocol set. Their authenticity, integrity and confidentiality can also be protected by the mechanism.

[4] For UMTS a large number of network operators is expected. In this case key transport mechanisms based on asymmetric algorithms offer advantages regarding key management. Therefore, we propose to use an asymmetric scheme in Layer I.

Annex Z:
Document history

Document history		
0.0.1	10 February 1999	Start
0.0.2	19 February 1999	Extensions on contents, relevant chapter headings added
0.1.1	17 March 1999	Extensions (BV)
0.1.2	19 March 1999	Extensions (SP)
0.1.3	30 March 1999	Extensions (SP)
0.1.4	9 April 1999	Revisions in view of the discussion in TSG SA-3 #2. (BV)
0.2.0	19 April 1999	Editorial changes and inclusion of text on network-wide encryption. (BV)
0.2.1	21 April 1999	Further editorial changes. (BV)
0.2.2	22 April 1999	Further minor editorial changes. (PH)
2.0.0	23 April 1999	Formatted into 3GPP deliverable for approval at TSG SA Meeting #3