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

***TSGS#8(00)273***

**Source** **TSG-SA WG3**

**Title** **4 Corrective Release 1999 CRs to 33.102 and 33.103 as requested by SA#7**

| S3Tdoc. | Spec. | Ver. | CR | Rev. | Cat. | Rel. | Subject |
|---|---|---|---|---|---|---|---|
| S3-000334 | 33.102 | 3.4.0 | 102 | | F | R99 | Removal of NW Wide Encryption |
| S3-000268 | 33.102 | 3.4.0 | 092 | | F | R99 | Removal of enhanced user identity confidentiality |
| S3-000335 | 33.103 | 3.2.0 | 007 | | F | R99 | Removal of EUIC from 33.103 |
| S3-000336 | 33.103 | 3.2.0 | 008 | | F | R99 | Removal of MAP Security from 33.103 |

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

***Document*** **S3-000334**
*e.g. for 3GPP use the format TP-99xxx*
*or for SMG, use the format P-99-xxx*

# CHANGE REQUEST

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

| **33.102** | **CR** | **102** | Current Version: | 3.4.0 |
|---|---|---|---|---|

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

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

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

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

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

**Subject:** Removal of NW Wide Encryption.

**Work item:** Security

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

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

**Reason for change:** Only hooks for NW Wide Encryption were meant to be defined during R99. Complete introduction of this feature into the specification shall take place during R00.

**Clauses affected:** 5.4.2, 5.5.1, 6.7

**Other specs affected:**

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

**Other comments:**


help.doc

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

~~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.~~

****** Next modified section ******

## 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).

****** Next modified section ******

# 6.7 Network-wide encryption

## 6.7.1 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.

## 6.7.2 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

## 6.7.3 Key management

### 6.7.3.1 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.

### 6.7.3.2 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.

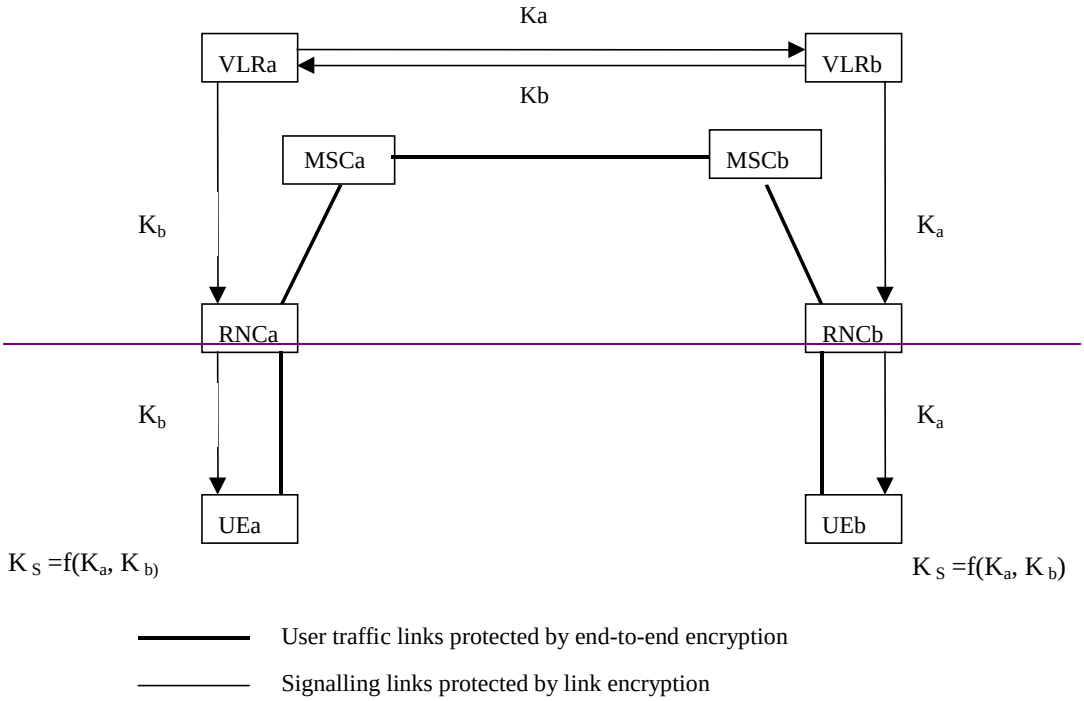



**Figure 17: Key management scheme for network-wide encryption**

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.

### 6.7.3.3 Variant on the outline scheme

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

NOTE: As opposed to the scheme in section 8.2.3, the access link keys Ka and Kb could be used for access link encryption of other data.

**3GPP TSG SA WG 3 Meeting #12**
**Stockholm, Sweden, 11-14 April 2000**

***Document* S3-000268**
*e.g. for 3GPP use the format TP-99xxx*
*or for SMG, use the format P-99-xxx*

# CHANGE REQUEST

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

| 33.102 | CR | 092 | Current Version: | 3.4.0 |
|---|---|---|---|---|

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

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

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

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

**Source:** TSG SA WG 3 **Date:** 11 April 2000

**Subject:** Removal of enhanced user identity confidentiality

**Work item:** Security

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

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

**Release:**

| | |
|---|---|
| Phase 2 | |
| Release 96 | |
| Release 97 | |
| Release 98 | |
| Release 99 | X |
| Release 00 | |

**Reason for change:** Decision taken by the SA#7.

**Clauses affected:** 3.2, 3.3, 5.1.1, 6.2, Annex B

**Other specs affected:**

| | | |
|---|---|---|
| Other 3G core specifications | X | → List of CRs: CR against 33.103<br>CR against 33.105 |
| Other GSM core specifications | | → List of CRs: |
| MS test specifications | | → List of CRs: |
| BSS test specifications | | → List of CRs: |
| O&M specifications | | → List of CRs: |

**Other comments:**

help.doc

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

## 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:

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

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

### 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.~~

## 6.2 Identification by a permanent identity

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

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

The mechanism is illustrated in Figure 4.

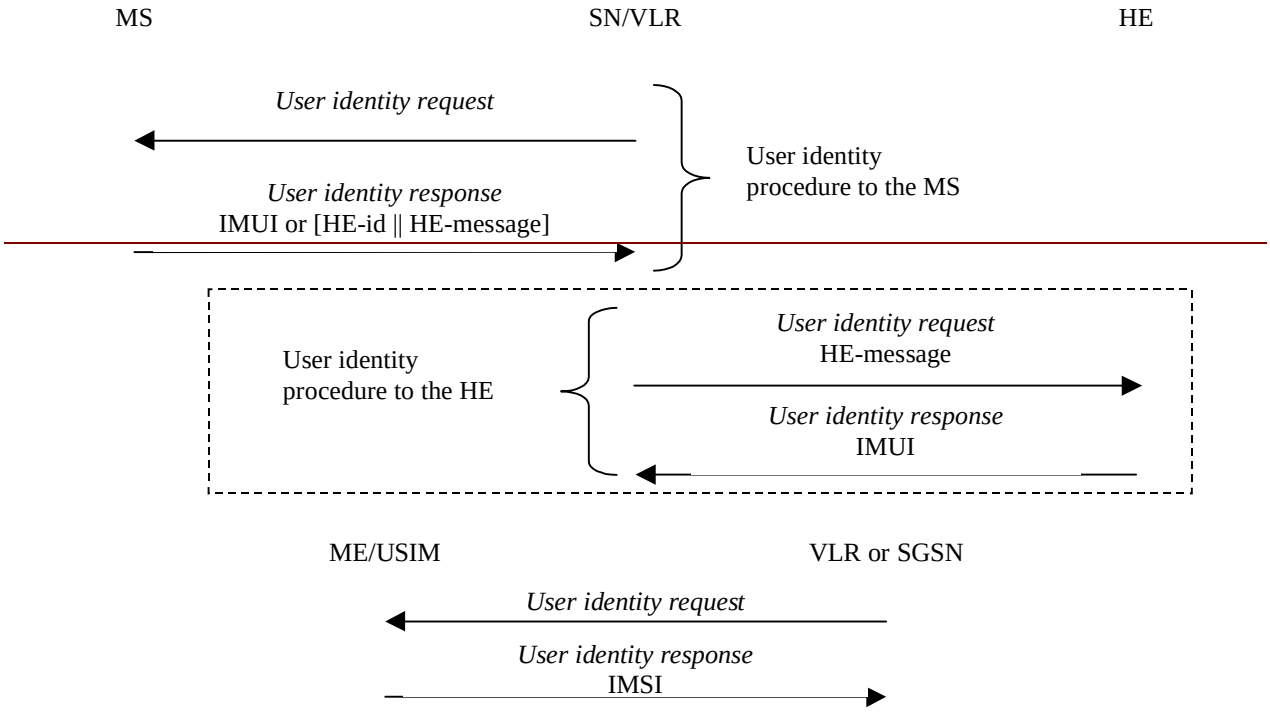



**Figure 4: Identification by the permanent identity**

The mechanism is initiated by the visited ~~SN/~~VLR or SGSN that requests the user to send its permanent identity. ~~According to the user's preferences, his~~ The user's response ~~may~~ contains ~~either 1)~~ the ~~IMSA~~ IMSI in cleartext~~, or 2) the Extended Encrypted Mobile Subscriber Identity (XEMSI).~~

~~A mobile station configured for Enhanced User Identity Confidentiality shall always use the XEMSI instead of the IMSI. XEMSI consists of the User Identity Decryption Node address (UIDN_ADR, see below) and a container transporting the Encrypted Mobile Subscriber Identity EMSI. UIDN_ADR shall consist of a global title according to E164. For details concerning the structure of the XEMSI see [26].~~

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

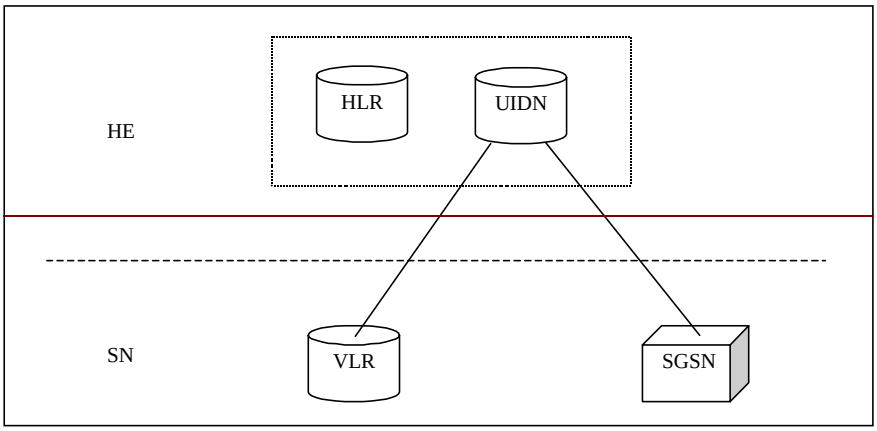
~~In case the response contains the XEMSI, the visited SN/VLR/SGSN forwards the EMSI to the user's UIDN/HE in a request to send the user's IMSI and TEMSI (Temporary EMSI). The user's UIDN/HE then derives the IMSI from EMSI, calculates TEMSI and sends the IMSI and TEMSI back to the SN/VLR/SGSN. Annex B describes an example mechanism that makes use of group keys to encrypt the IMSI and to calculate the TEMSI and provides details on EMSI.~~

~~The SN shall use TEMSI instead of IMSI to page a particular user because using the IMSI in clear would compromise the security goal of the Enhanced User Identity Confidentiality feature. Therefore on UE side the TEMSI is calculated and stored by USIM and transmitted to the UE. On both sides, in the UE and VLR/SGSN, the TEMSI shall become active if the following authentication procedure has successfully been performed. After the current TEMSI has successfully been used once SN shall trigger the *User Identity Request* procedure to establish a new TEMSI.~~

~~For the case the VLR/SGSN has lost the TEMSI related to a particular IMSI the VLR/SGSN shall request the most recently derived TEMSI from the UIDN. Therefore the UIDN has to store necessary information for each IMSI.~~

~~For the purpose of the Enhanced User Identity Confidentiality a new logical network node UIDN is introduced. The serving VLR or SGSN shall be able to request decryption of the user identity and calculation/providing of paging identities by this home network node.~~

~~The UIDN is in charge of decrypting the encrypted IMSI provided by the mobile station in EMSI and of calculating the TEMSI. The UIDN is a home network operator specific logical network node and may be co-located with the HLR.~~




**~~Figure 5: Core Network Architecture for Enhanced User Identity Confidentiality~~**

~~The interface between the VLR/SGSN and the UIDN is used by the VLR/SGSN to request the~~

- ~~revelation of the IMSI contained in EMSI from the UIDN;~~
- ~~calculation of the TEMSI for the circuit/packet switched domain;~~
- ~~most recently derived TEMSI.~~

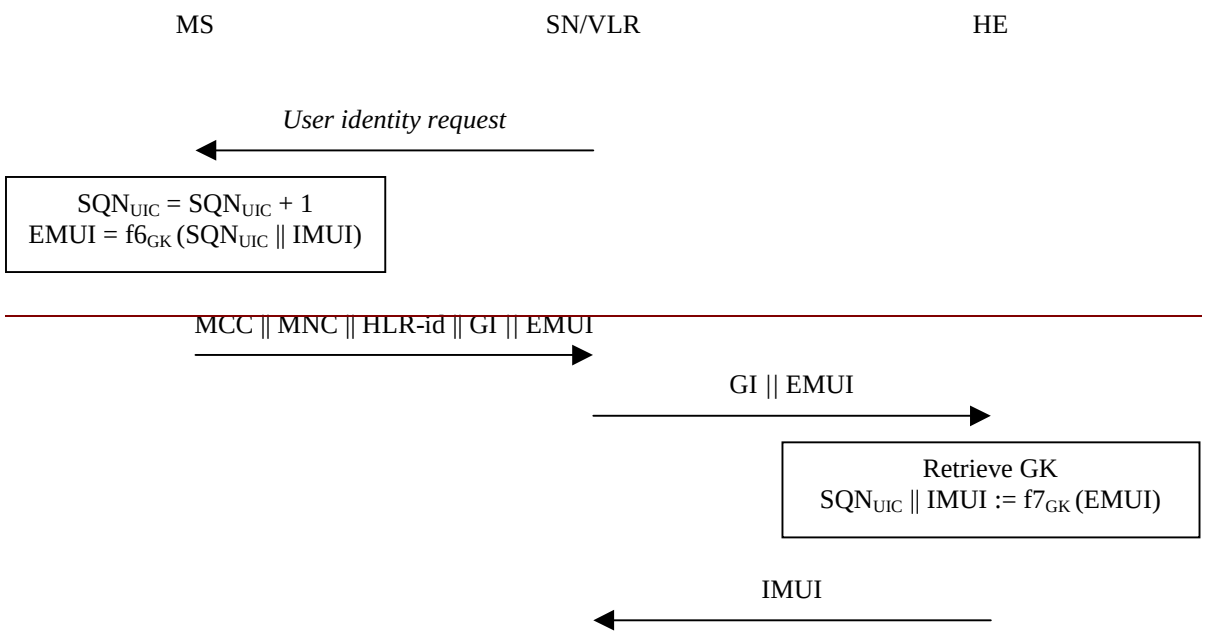
# Annex B ~~(informative)~~: Void

~~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/UIDN.~~

~~The mechanism is illustrated in Figure B.1.~~




**~~Figure B.1: Identification by means of the IMSI encrypted by means of a group key~~**

~~The mechanism illustrated in Figure B.1 works as follows:~~

~~1) The user identity procedure is initiated by the visited VLR/SGSN. The visited VLR/SGSN requests the USIM to send its XEMSI.~~

~~2) Upon receipt the USIM:~~

- ~~increments $SQN_{UIC}$ as a time variant parameter;~~
- ~~encrypts $SQN_{UIC}$ and its MSIN with enciphering algorithm f6 and its group key GK. The result is called EMSIN, encrypted MSIN;~~
- ~~constructs EMSI as concatenation of the group identifier GI and EMSIN;~~
- ~~constructs XEMSI as concatenation of UIDN_ADR and EMSI;~~
- ~~sends XEMSI in a response to the SN/VLR/SGSN;~~
- ~~derives TEMSI from IMSI and $SQN_{UIC}$ with cryptographic algorithm f10 and the group key GK.~~

~~The $SQN_{UIC}$ prevents traceability attacks and synchronizes the derivation of TEMSI in the USIM and HE.~~

~~3) Upon receipt of that response the SN/VLR/SGSN resolves the UIDN_ADR from XEMSI and forwards EMSI to the user's HE/UIDN.~~

4) Upon receipt the HE/UIDN:

- retrieves the group identity GI contained in EMSI;
- retrieves the group key GK associated with the group identity GI;
- decrypts EMSIN with the deciphering algorithm f7 (f7 = $f6^{-1}$) and the group key GK and retrieves $SQN_{UIC}$ and MSIN;
- constructs the user's IMSI according to the following rule: IMSI := $MCC_{UIDN\_ADR}$ || $MNC_{UIDN\_ADR}$ || MSIN (UIDN_ADR := $MCC_{UIDN\_ADR}$ || $MNC_{UIDN\_ADR}$ || $MSIN_{UIDN\_ADR}$);
- calculates TEMSI as TEMSI := $f10_{GK}$ ($SQN_{UIC}$ || IMSI);
- sends IMSI and TEMSI in a response to the visited SN/VLR/SGSN.

$SQN_{UIC}$ is no longer used. The HE/HLR then sends the IMUI in a response to the visited SN/VLR.

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

***Document*** **S3-000335**
*e.g. for 3GPP use the format TP-99xxx*
*or for SMG, use the format P-99-xxx*

# CHANGE REQUEST

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

| **33.103** | **CR** | **007** | Current Version: | 3.2.0 |
|---|---|---|---|---|

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

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

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

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

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

**Subject:** Removal of EUIC from 33.103

**Work item:** Security

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

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

**Release:**

| | |
|---|---|
| Phase 2 | |
| Release 96 | |
| Release 97 | |
| Release 98 | |
| Release 99 | X |
| Release 00 | |

**Reason for change:** As per SA#7 decision, EUIC is not a R99 feature. EUIC is therefore removed from 33.103.

**Clauses affected:** 4.2.1, 4.3.4, 4.5.2, 4.7.

**Other specs affected:**

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

**Other comments:**

help.doc

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

## 4.2.1 Enhanced User Identity Confidentiality ($EUIC_{USIM}$)

For UMTS users with EUIC, the USIM has to store additional data and have additional functions implemented to encrypt the permanent user identity (IMSI). We describe the requirements as regards data storage and algorithm implementation for an example mechanism in annex B of 3G TS 33.102.

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

a) $SQN_{UIC}$: a counter that is equal to the highest $SQN_{UIC}$ generated and sent by the USIM to the HE/UIDN;

b) GK: the group key used to encrypt the MSIN and $SQN_{UIC}$;

c) GI: a group identifier that identifies the group the user refers to as well as the GK;

d) TEMSI: a temporary identity used for paging instead of IMSI;

d) UIDN_ADR: address of UIDN according to E.164.

**Table 1: USIM – Enhanced User Identity Confidentiality – Data elements**

| Symbol | Description | Multiplicity | Lifetime | Length | Mandatory / Optional |
|---|---|---|---|---|---|
| GK | Group key | 1 per user group the user belongs to | Permanent | 128 bits (Note 1) | Optional |
| $SQN_{UIC}$ | Counter | 1 per user | Updated when protocol for EUIC is executed | 32 bits | Optional |
| GI | Group Identity | 1 per user | Permanent | 32 bits | Optional |
| TEMSI | Temporary identity used for paging instead of IMSI | 1 per user | Updated when a new identity request has been performed | As per IMSI | Optional |
| UIDN_ADR | Address of UIDN according to E.164 | 1 per user | Permanent | 15 digits | Optional |

NOTE 1: The table entry is for the example secret key mechanism given in annex B of 33.102

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

- f6: the user identity encryption function;
- f10: TEMSI calculation function.

For a summary of the data elements and cryptographic function of the $EUIC_{HE}$ function see table 2.

**Table 2: USIM – Enhanced User Identity Confidentiality – Cryptographic functions**

| Symbol | Description | Multiplicity | Lifetime | Standardised / Proprietary | Mandatory / Optional |
|---|---|---|---|---|---|
| f6 | User identity encryption function | 1 | Permanent | Proprietary | Optional |
| f10 | TEMSI calculation function | 1 | Permanent | Proprietary | Optional |

## 4.3.4 Enhanced user identity confidentiality ($EUIC_{UE}$)

The UE shall support the UMTS mechanism for enhanced user identity confidentiality described in 6.2 of 3G TS 33.102.

The UE shall store the following data elements:

- the TEMSI: a temporary identity used for paging instead of IMSI.

**Table 9a: UE – User Identity Confidentiality – Data elements**

| Symbol | Description | Multiplicity | Lifetime | Length | Mandatory / Optional |
|---|---|---|---|---|---|
| TEMSI | Temporary identity used for paging instead of IMSI | 1 per user | Updated when a new identity request has been performed | As per IMSI | Optional |

## 4.5.2 Enhanced user identity confidentiality ($EUIC_{SN}$)

The VLR (equivalently the SGSN) shall support the UMTS mechanism for enhanced user identity confidentiality described in 6.2 of 3G TS 33.102.

The VLR shall store the following data elements:

- the TEMSI: a temporary identity used for paging instead of IMSI.

**Table 15a: VLR – User Identity Confidentiality – Data elements**

| Symbol | Description | Multiplicity | Lifetime | Length | Mandatory / Optional |
|---|---|---|---|---|---|
| TEMSI | Temporary identity used for paging instead of IMSI | 1 per user | Updated when a new identity request has been performed | As per IMSI | Optional |

Equivalently, the SGSN shall store the following data elements:

- the TEMSI: a temporary identity used for paging instead of IMSI.

**Table 15b: SGSN – User Identity Confidentiality – Data elements**

| Symbol | Description | Multiplicity | Lifetime | Length | Mandatory / Optional |
|---|---|---|---|---|---|
| TEMSI | Temporary identity used for paging instead of IMSI | 1 per user | Updated when a new identity request has been performed | As per IMSI | Optional |

## 4.7 Enhanced user identity confidentiality ($EUIC_{HE}$)

For UMTS users with EUIC, the UIDN has to store additional data and have additional function implemented to decrypt the permanent user identity (IMSI) and to calculate the paging identity TEMSI to be used instead of IMSI. We describe the requirements as regards data storage and algorithm implementation for the example mechanism in annex B of 3G TS 33.102.

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

a) GK: the group key used to decrypt the IMSI and $SQN_{UIC}$;

b) GI: a group identifier that identifies the group the user refers to as well as the GK;

c) TEMSI: a temporary identity used for paging instead of IMSI;

d) IMSI: the IMSI of the user the feature is applied to.

**Table 21a: UIDN – Enhanced User Identity Confidentiality – Data elements**

| Symbol | Description | Multiplicity | Lifetime | Length | Mandatory / Optional |
|---|---|---|---|---|---|
| GK | Group key | 1 per user group | Permanent | 128 | Optional |
| GI | Group Identity | 1 per user | Permanent | 32 bits | Optional |
| TEMSI | Temporary identity used for paging instead of IMSI | 1 per user | Updated when a new identity request has been performed | As per IMSI | Optional |
| IMSI | IMSI | 1 per user | Permanent | 64 bits | Optional |

The following cryptographic functions need to be implemented in UIDN:

- f7: the user identity decryption function.

- f10: TEMSI calculation function.

For a summary of the data elements and cryptographic function of the $EUIC_{HE}$ function see table 2.

**Table 21b: UIDN – Enhanced User Identity Confidentiality – Cryptographic functions**

| Symbol | Description | Multiplicity | Lifetime | Standardised / Proprietary | Mandatory / Optional |
|---|---|---|---|---|---|
| f7 | User identity decryption function | 1 | Permanent | Proprietary | Optional |
| f10 | TEMSI calculation function | 1 | Permanent | Proprietary | Optional |

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

***Document*** **S3-000336**
*e.g. for 3GPP use the format TP-99xxx*
*or for SMG, use the format P-99-xxx*

# CHANGE REQUEST

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

| **33.103** | **CR** | **008** | Current Version: | 3.2.0 |
|---|---|---|---|---|

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

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

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

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

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

**Subject:** Removal of MAP Security from 33.103

**Work item:** Security

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

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

**Release:**

| | |
|---|---|
| Phase 2 | |
| Release 96 | |
| Release 97 | |
| Release 98 | |
| Release 99 | X |
| Release 00 | |

**Reason for change:** As per SA#7 decision, MAP Security is not a R99 feature. MAP Security is therefore removed from 33.103.

**Clauses affected:** 5

**Other specs affected:**

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

**Other comments:**

help.doc

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

# 5 Provider domain security

## 5.1 Functional security architecture

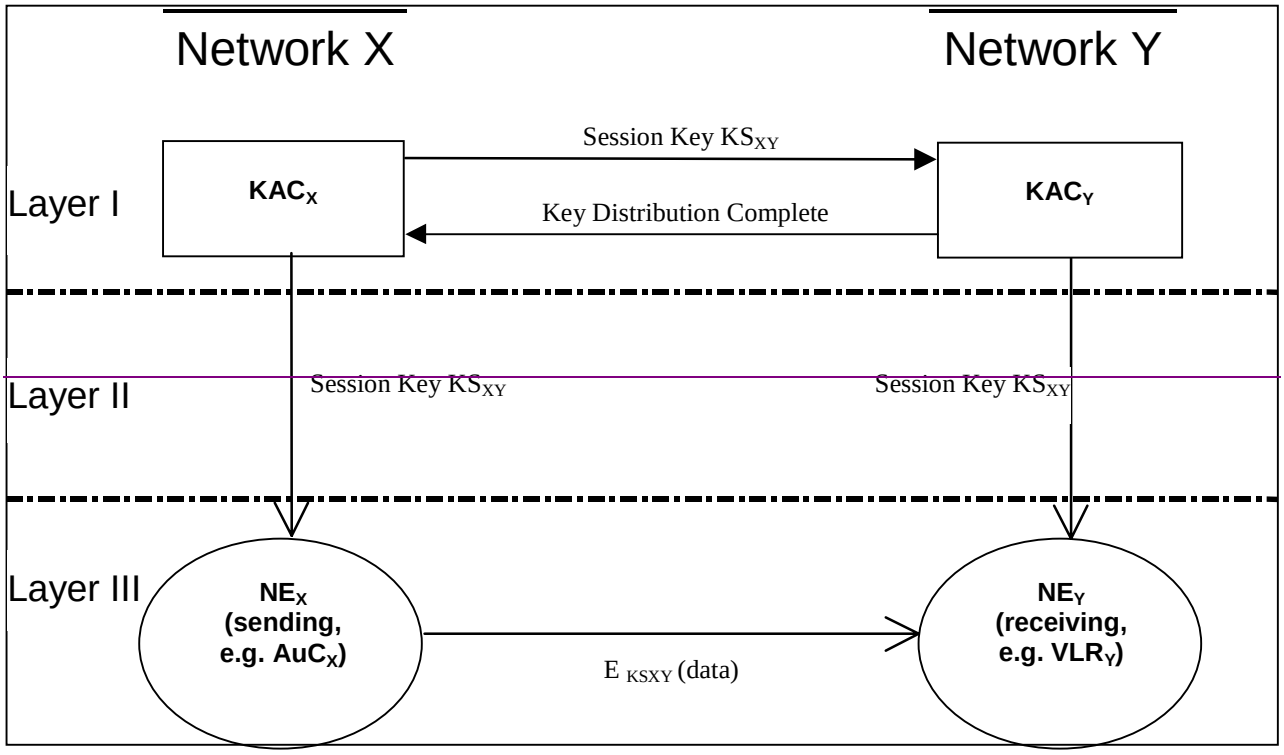



**Figure 5: Overview of Proposed Mechanism**

This mechanism establishes a secure signalling links between network nodes, in particular between VLR/SGSNs and HE/AuCs. Such procedures may be incorporated into the roaming agreement establishment process.

A secret key transport mechanism based on an asymmetric crypto system i used to agree on a symmetric session key for each direction of communication between two networks X and Y.

The party wishing to send sensitive data initiates the mechanism and chooses the symmetric session key it wishes to use for sending the data to the other party. The other party shall choose a symmetric session key of its own, used for sending data in the other direction. This second key shall be transported immediately after the first key has been successfully transported. The session symmetric keys are protected by asymmetric techniques. They are exchanged between certain elements called the *Key Administration Centres* (KACs) of the network operators X and Y.

**Transport of Session Keys**

In order to establish a symmetric session key with version no. i to be used for sending data from X to Y, the $KAC_X$ sends a message containing the following data to the $KAC_Y$:

$E_{PK(Y)}${X||Y||i||$KS_{XY}$(i)||$RND_X$||Text1||$D_{SK(X)}$(*Hash*(X||Y||i||$KS_{XY}$(i)||$RND_X$||Text1))||Text2}||Text3

After having successfully distributed the symmetric session key received by network X to its own network entities, network Y sends to X a Key Distribution Complete Message. This is an indication to $KAC_X$ to start with the distribution of the key to its own entities, which can then start to use the key immediately.

The message takes the form

KEY_DIST_COMPLETE||Y||X||i||$RND_Y$||$D_{SK(Y)}$(*Hash*(KEY_DIST_COMPLETE||Y||X||i||$RND_Y$)

where i indicates the distributed key and $RND_Y$ is a random number generated by Y. The digital signature is appended for integrity and authenticity purposes. Y includes $RND_Y$ to make sure that the message contents determined by X will be modified before signing.

Since most of the signalling messages to be secured are bidirectional in character, immediately after successful completion the procedure described here shall be repeated, now with Y choosing a key $KS_{YX}(i)$ to be used in the reverse direction, and X being the receiving party. Thereby keys for both directions are established.

## 5.2 Key Authentication Centre

Details in security architecture to be finalised

## 5.3 Core network entities

**Table 22: Signalling Protection- Data Elements**

| Symbol | Description | Multiplicity | Lifetime | Length | Mandatory / Optional |
|---|---|---|---|---|---|
| PVTK-s | Network's own Private Key ( signing) | 1 | According to roaming agreement | < or = 2048 bits | Mandatory |
| PVTK-d | Network's own Private Key (decryption) | 1 | According to roaming agreement | < or = 2048 bits | Mandatory |
| $PUBKv_1$ | $PKR_1$ Public Key for network #1 (verify) | 1 per roaming agreement | According to roaming agreement | < or = 2048 bits | Mandatory |
| $PUBKe_1$ | $PKR_1$ Public Key for network #1 (encryption) | 1 per roaming agreement | According to roaming agreement | < or = 2048 bits | Mandatory |
| $KS_{XY}(i)$ | Symmetric Send Key #i for sending data from X to Y | 1 per session | According to roaming agreement | 128 bits | Mandatory |
| $KS_{YX}(j)$ | Symmetric Send Key #j for sending data from Y to X | 1 per session | According to roaming agreement | 128 bits | Mandatory |
| I | Session key Sequence Number (for sending data from X to Y) | 1 per session | According to roaming agreement | 32 – 64 bits | Mandatory |
| J | Session key Sequence Number (for sending data from Y to X) | 1 per session | According to roaming agreement | 32 – 64 bits | Mandatory |
| $RND_X$ | Unpredictable Random Value generated by X | 1 per session | Session | 128 bits | Mandatory |
| $RND_Y$ | Unpredictable Random Value generated by Y | 1 per session | Session | 128 bits | Mandatory |

**Table 23: Signalling Protection – Cryptographic Functions**

| Symbol | Description | Multiplicity | Lifetime | Standardised / Proprietary | Mandatory / Optional |
|---|---|---|---|---|---|
| BEANO | Block Encryption Algorithm for Network Operators | 1 | Permanent | Standardised | Mandatory |