3GPP TSG SA WG3 Security — S3#13 **S3-000319**

23-26 May, 2000

Yokohama, Japan

Source: **Secretary**

Title: **Documents Postponed from Meeting #12 to Meeting#13**

Document for: **Discussion**

Agenda Item: **Various**

The following documents were postponed at SA WG3 meeting #12 and should be further discussed in meeting #13.

Number	Title	Source	Document for	Comments Status
S3-000222	Initiation of COUNT-I and COUNT-C	Siemens Atea	Decision	Postponed to Meeting#13
S3-000223	LS on OPEN SERVICE ARCHITECTURE - SECURITY	SA WG2	Discussion	All to check OSA Security and revisit at SA3#13
S3-000253	CR to 33.102: Authentication and key agreement (editorial)	Siemens Atea	Information	CR082. Delegates to check the need for restucturing proposed in the CR. R99 and/or R00 ? Postponed to SA3#13
S3-000257	CR to 33.102: 3G-2G and 2G-3G Handover for CS services	Siemens Atea	Approval	CR086 Postponed to SA3#13
S3-000267	CN WG2 TD N2B000428 CR to 29.060	CN WG2	Information	To be considered for decision at meeting#13
S3-000270	Response Liaison to SMG9 on "Auto-Answer and Mute ringing"	SA WG3	Approval	Not presented. To be cobsidered at meeting#13
S3-000277	CR095 to 29.060: GTP Security	Nortel	Information	To be considered for meeting#13
S3-000290	CR to 33.102: Clarification on the UIA and UEA selection	Ericsson	Approval	CR081 Postponed to SA3#13
S3-000291	CR to 33.102: Limitation and reduction of the effective cipher key length by the serving network	Siemens Atea	Approval	CR087 Postponed to SA3#13

TSG-SA WG3 (Security) meeting #12
Stockholm, Sweden, 11-14 April 2000

S3-000222

Agenda Item:

Source: Siemens Atea

Title: Initiation of COUNT-I and COUNT-C

Document for: Decision

TS 25.331 currently describes that two "initial HFN values" are transported from the UE to the RNC. TS 33.102 only mentions one "START" value. This contribution addresses the following issues:

- Do we need a START-C and a START-I?
- What length should START have?
- Where is the START value stored at the user side and how is it managed?

Do we need a START-C and a START-I?

No.

START is needed to prevent that a COUNT-C or COUNT-I is re-used with the same CK or IK. Having only one START value, equal to the most significant bits of the maximum of all COUNT-C and all COUNT-I values, rather than having two, saves on signalling, storage and complexity. We suggest that TS 25.331 be amended to reflect this.

What length should START have?

The RRC HFN for integrity is 28 bits long, the RLC HFN for ciphering can be 20 or 25 bits long, the MAC HFN for ciphering RLC TM channels is 25 bits long. Does this require START to be equal to the maximum value? No. START can be smaller and just initialise the MSB of the different HFN; the remaining LSB are then set to zero.

START can however not be too short. Shortening START will lead to faster incrementation and leads to it that COUNT-C or COUNT-I sooner wraps around, or rather reaches its maximum value, or rather reaches its threshold value. However, the range for START is that large, that some shortening need not be a problem.

In RLC TM – assuming for a while COUNT-C is the fastest to increase (which is certain) and of all logical channels RLC TM is the one increasing fastest – HFN is incremented every 0,72 seconds. Then the 20^{th} bit is incremented every 23 seconds whereas the 16^{th} bit is incremented every 6 minutes. Therefore, with 24 bit, 20 bits, 16 bit START values, the initial HFN values increment every 1,5 seconds, 23 seconds, 6 minutes. And if a call is ended, the remaining time in the current interval between successive HFN increments is "lost". Given the fact the total HFN range accommodates for over 24 million seconds or 400 thousand minutes, loosing some seconds or even minutes does not appear to be a problem. Surely, because there is the recommendation/obligation for the serving network to refresh the keys at least every 24 hours, i.e., every 1440 minutes or 86 thousand seconds.

Therefore, we propose a 16 bit START value.

Where is the START value stored at the user side and how is it managed?

We propose the following:

> The UE and the USIM store a START value. When the USIM is removed, the UE deletes its START value. At insertion of a USIM, the USIM sends its START value to the UE, which stores the received START value.
>
> During an ongoing radio connection, the START value in the UE is defined as the 16 MSB of the maximum of the current COUNT-C and COUNT-I values, incremented by 1, i.e.,
>
> $$START = MSB_{16} (MAX \{COUNT\text{-}C, COUNT\text{-}I \mid \text{for all signalling and user data logical channels}\}) + 1$$
>
> In idle mode, the START value in the UE is the last START value reached during the previous radio connection or the START value received at USIM insertion.
>
> At radio connection establishment when in idle mode, the UE sends a message to the USIM to mark the START value stored in the USIM as invalid.

At radio connection establishment the UE sends the START value to the RNC in the *RRC connection setup complete* message.

The UE and the RNC then initialise the 16 most significant bits

- of the RRC HFN for integrity to START; the remaining 12 LSB are initialised to zero;
- of the RLC HFN for ciphering of RLC AM to START; the remaining 4 LSB are initialised to zero;
- of the RLC HFN for ciphering of RLC UM to START; the remaining 9 LSB are initialised to zero;
- of the MAC HFN for ciphering of RLC TM to START; the remaining 9 LSB are initialised to zero.

Upon connection release the UE sends a message to the USIM with the current START value. The USIM updates the START value and marks it as up-to-date.

3GPP TSG SA WG3 Security — S3#12 **S3-000223**

11-14 April, 2000

Stockholm, Sweden

Source: **SA WG2**

Title: **LS on OPEN SERVICE ARCHITECTURE - SECURITY**

Document for: **Discussion**

Agenda Item:

3GPP TSG SA2#12 **S2-000557**
Tokyo, Japan, March 6th – 9th, 2000

LIAISON STATEMENT

SOURCE: **3GPP TSG SA WG2** [1]

TO: **3GPP TSG SA WG3, TSG CN OSA Adhoc (For Information)**

TITLE: **OPEN SERVICE ARCHITECTURE - SECURITY**

An S2 – VHE/OSA drafting session has been held on 23-24 February in Stockholm, Sweden. The issue of security within the Open Service Architecture (OSA) has been discussed and agreed.

The agreed text regarding the security (Tdoc S2OSA-000022) has been attached for your information. If S3 has any comments that they would like to express to the attention of CN OSA and S2 experts then an LS would be appreciated.

For your information the following meeting schedule is applicable:

- CN OSA 28-29 February, 1st of March 2000, Antwerp, Belgium
- S2 6-9 March 2000, Tokyo, Japan

Attachment: **S2-000359**

---

[1] Contact: Alexander Milinski
Tel +49 89 722 29402 Email: Alexander-Milinski@icn.siemens.de

3GPP TSG SA2#12 S2-000359

Tokyo, Japan, March 6th – 9th, 2000

3GPP TSG-SA WG2 VHE/OSA Interim Meeting

February 23 - 24, 2000

Stockholm, Sweden

Title: **Proposed text for a new section on end-user related security (5.3) in 23.127 v.1.2.0**

Agenda Item: 'VHE/OSA'

Source: Ericsson

Document for: Discussion / Decision

INTRODUCTION

Security has been identified as a critical issue to be addressed in order for VHE/OSA to be part of 3GPP release 99. Especially the end-user security needs to be addressed. Therefore, in addition to the framework related sections on security: authentication (6.2) and authorisation (6.3), additional material is introduced here on end-user related security aspects. A new section 5.3 in document 23.127 v 1.3.0 is proposed here. Also, a number of error parameters are introduced to report security violations.

5.3 Handling of end-user related security

Once OSA basic mechanisms have ensured that an application has been authenticated and authorised to use network service capability features, it is important to also handle end-user related security aspects. These aspects consist of the following.

- **End-user authorisation to applications,** limiting the access of end-users to the applications they are subscribed to.
- **Application authorisation to end-users**, limiting the usage of network capabilities by the applications to be authorised (i.e. subscribed) to end-users.
- **End-user's privacy**, allowing the user to set privacy options.

These aspects are addressed in the following subsections~~. Also, a number of error parameters are introduced to handle security violations.~~

5.3.1 End-user authorisation to applications

An end-user is authorised to use an application only when he or she is subscribed to it.

In the case where the end-user has subscribed to the application ~~prior to~~ before the application accesses~~ing~~ the network SCF's, then the subscription is part of the Service Level Agreement signed between the HE and the HE-VASP.

After the application has been granted access to network SCF's, subscriptions are controlled by the Home Environment. Depending on the identity of an authenticated and authorised end-user, the Home Environment may use any relevant policy to define and possibly restrict the list of services to which a particular end-user can subscribe. At any time, the Home Environment may decide, unilaterally or after agreement with the HE-VASP, to cancel a particular subscription.

Service subscription and activation information need to be shared between the Home Environment and the HE-VASP, so that the HE-VASP knows which end-users are entitled to use its services. Appropriate online and/or offline

synchronisation mechanisms (e.g. SLA re-negotiation) can be used between the HE and the HE-VASP, which are not specified in OSA release 99~~parts of this specification~~.

End-to-end interaction between a subscribed end-user and an application may require the usage of appropriate authentication and authorisation mechanisms between the two, which are independent from the ~~VHE/~~OSA API, and therefore not in the scope of OSA standardisation~~subject to standardisation~~.

5.3.2 Application authorisation to end-users

The Home Environment is entitled to provide service capabilities to an application with regard to a specific end-user if the following conditions are met:

1) The end-user is subscribed to the application

2) The end-user has activated the application

3) The usage of this network service capability does not violate the end-users privacy settings (see next section).

~~It is the responsibility of t~~The service capability server ~~to~~ ensures that the above conditions are met whenever an application attempts to use a service capability feature for a given end-user, and to respond to the application accordingly, possibly using relevant error parameters (`USER_NOT_SUBSCRIBED`, `APPLICATION_NOT_ACTIVATED`, `USER_PRIVACY_VIOLATION`). The mechanism used by the SCS to ensure this is internal to the HE (e.g. access to user profile) and is not standardised in OSA release 99~~this specification~~.

5.3.3 End-user's privacy

The Home Environment may permit an end-user to set privacy options. For instance, it may permit the end-user to decide whether his or her location may be provided to 3rd parties, or whether he or she accepts information to be pushed to his or her terminal. Such privacy settings may have an impact on the ability of the network to provide service capability features to applications (e.g. user location, user interaction). Thus, even if an application is authorised to use an SCF and the end-user is subscribed to this application and this application is activated, privacy settings may still prevent the HE from~~to~~ fulfilling an application request.

~~It is the responsibility of t~~The service capability server ~~to~~ ensures that a given application request does not violate an end-users privacy settings or that the application has relevant privileges to override them (e.g. for emergency reasons). The mechanism used by the SCS to ensure this is internal to the HE and is not standardised in OSA release 99~~this specification~~.

(end of text to be inserted)

~~5.3.4~~SECURITY RELATED ERROR PARAMETERS

The following error parameters are introduced with respect to security and/or privacy violations.

- USER_NOT_SUBSCRIBED
- APPLICATION_NOT_ACTIVATED
- USER_PRIVACY_VIOLATION

These error parameters are added for the following SCS's and SCS methods:

```
Call Control                        enableCallNotification()
                                    routeCallToDestination_Req()

Network User Location               locationReportReq()
                                    periodicLocationReportingStartReq()
                                    triggeredLocationReportingStartReq()
```

User Status	statusReportReq() triggeredStatusReportingStartReq()
Generic User Interaction	createUI()

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

***Document* S3-000252**
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.

03.20	CR		Current Version:	8.0.0

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

For submission to: TSG SA #7	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	X	UTRAN / Radio		Core Network	X

Source: Siemens Atea **Date:** April 7, 2000

Subject: GPRS Ciphering algorithm negotiation

Work item: Security

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

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

Reason for change: GSM 03.20 does no reflect the fact that the SGSN and the ME are capable to negotiate an unciphered connection.

Clauses affected: D.4.8

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.

D.4.8 Negotiation of GPRS-A5 algorithm

Not more than seven versions of the A5 algorithm will be defined.

When an MS wishes to establish a connection with the network, the MS shall indicate to the network which version(s) of the GPRS-A5 algorithm it supports. The negotiation of GPRS-A5 algorithm happens during the authentication procedure.

The network may renegotiate the version of the GPRS-A5 algorithm in use at inter SGSN routing area update by performing an authentication procedure.

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 may take one of the following decisions:

~~1) The network decides to release the connection because no common version of the GPRS-A5 algorithm is available or because the MS indicated an illegal combination of supported algorithms.~~

~~2) The network selects one of the mutually acceptable versions of GPRS-A5 to be used.~~

1) If the MS and the network have no versions of the GPRS A5 algorithm in common and the network is not prepared to use an unciphered connections, then the connection is released.

2) If the MS and the network have at least one version of the GPRS A5 algorithm in common, then the network shall select one of the mutually acceptable versions of the GPRS A5 algorithms for use on that connection.

3) If the MS and the network have no versions of the GPRS A5 algorithm in common and the network is willing to use an unciphered version, then an unciphered connection shall be used.

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

***Document* S3-000253**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

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

33.102	**CR**		Current Version:	3.3.1

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

For submission to:	TSG SA #7	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 [ ]

Source: Siemens Atea **Date:** 2000-04-04

Subject: Authentication and key agreement

Work item: Security

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

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

Reason for change: Better presentation of the mechanism for authentication and key agreement. The mechanism for authentication and the mechanism for re-synchronisation are discussed separately. The procedures are discussed separately from the mechanisms, and the functions implemented in the USIM and the HLR/AuC are discussed separately from the procedures.

Clauses affected: 6.3

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: The existing 6.3 should be replaced by the attached text. (The traditional lay-out with change bars is not used as it does not improve readability in this case).


help.doc

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

6.3 Authentication and key agreement

6.3.1 General

The mechanism described here achieves mutual entity authentication and the establishment of a shared secret cipher key and integrity key between the MS at the user side and the VLR or SGSN on behalf of the user's HLR/AuC at the network side.

The mechanism uses symmetric key techniques using a secret subscriber authentication key K that is shared between and available only to the USIM and the AuC in the user's HE. In addition, the AuC keeps track of a counter SQN_{HE} and the USIM keeps track of a counter SQN_{MS} and stores additional data to support network authentication and to provide the user with assurance of key freshness.

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).

The HE, that manages both the HLR/AuC and the USIM, has some flexibility in the management of sequence numbers, but some requirements need to be fulfilled:

a) The mechanism shall support re-synchronisation of the counter SQN_{HE} in the AuC to the value of the counter SQN_{MS} in the USIM, as described in section 6.3.2.2;

b) The mechanism shall protect against wrap around of the counter SQN_{MS} in the USIM. A mechanism to achieve this is provided in C.2.

c) The mechanism should not compromise user identity and location confidentiality. If consecutive sequence numbers for the same user are highly correlated, sending them in the clear should be considered as a compromise of user identity and location confidentiality, and the use of concealment of the sequence number, described as an option throughout 6.4.3, is recommended. In case however, the sequence numbers SQN are partly derived from time, such correlation is minimised, and the concealment may not be required.

d) The mechanisms for verifying the freshness of sequence numbers in the USIM shall to some extent allow the out-of-order use of sequence numbers. This is to ensure that the authentication failure rate due to synchronisation failures is sufficiently low. This requires the capability of the USIM to store information on past successful authentication events (e.g. sequence numbers or relevant parts thereof). The mechanism shall ensure that a sequence number can still be accepted if it is among the last 50 sequence numbers generated.

   Note 1: This shall not preclude that a sequence number is rejected for other reasons such as a limit on the age for time-based sequence numbers.

   Note 2: The same minimum number (50) needs to be used across the systems to guarantee that the synchronisation failure rate is sufficiently low under various usage scenarios, in particular simultaneous registration in the CS- and the PS-service domains, user movement between VLRs and/or SGSNs that do not exchange authentication data and super-charged networks.

Annex C contains a detailed description of a sequence number management scheme that satisfies the above conditions.

6.3.2 Mechanisms

6.3.2.1 Authentication and key agreement

An overview of the mechanism for authentication and key agreement is shown in Figure 6.3.1.

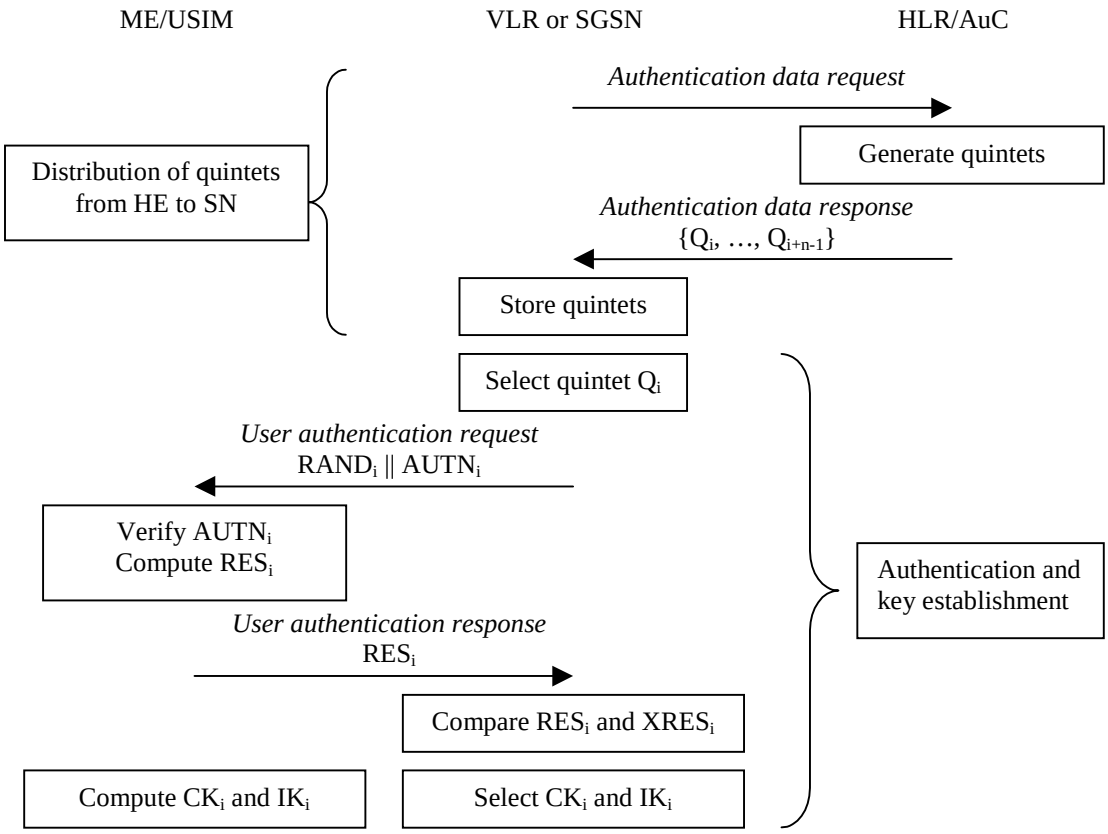

Figure 6.3.1: Authentication and key agreement mechanism

The procedure for distribution of authentication data from the HE to a service domain in the SN (described in 6.3.3.1) starts with the VLR or SGSN sending a request to the user's HLR/AuC. Upon receipt of that request the HLR/AuC sends a quintet (the equivalent of a GSM "triplet") or an ordered array of n quintets to the VLR or SGSN. Each quintet consists of the following components: a challenge RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each quintet is good for one authentication and key agreement between the VLR or SGSN and the MS.

When the VLR or SGSN initiates the over-the-air authentication and key agreement procedure (described in 6.3.3.2), it selects the next quintet from the array and sends the parameters RAND and AUTN to the user. The USIM checks whether AUTN can be accepted and, if so, produces a response RES which is sent back to the VLR or SGSN. The USIM also computes CK and IK. The VLR or SGSN compares the received RES with XRES. If they match the VLR or SGSN considers the authentication and key agreement exchange to be successfully completed and selects the corresponding CK and IK from the quintet. The established keys CK and IK are transferred by the USIM to the ME and by the VLR or SGSN to RNC; the entities that perform ciphering and integrity protection. The USIM stores the established cipher/integrity keys until the next successful authentication and key agreement.

If the USIM also supports cipher key agreement for the GSM radio interface, the USIM in addition derives a GSM cipher key Kc that is passed along to the ME (see 6.8.1).

The over-the-air authentication and key agreement procedure can fail for three reasons:

a) The USIM may successfully verify the integrity of the (RAND, AUTN) pair, but may be unable to verify the freshness of the (RAND, AUTN) pair. In this case the USIM shall trigger the re-synchronisation mechanism (see 6.3.3.2).

b) The USIM may find that the integrity of the (RAND, AUTN) pair could not be verified. In that case, the user informs the VLR or SGSN of the failure and of its nature, but no parameters are sent. The VLR or SGSN shall inform the HLR/AuC (see 6.3.3.4) about the failure and may request for new quintets (see 6.3.3.1). The VLR or SGSN may also decide to initiate a new identification and authentication procedure towards the user.

c) The VLR or SGSN may find that the user response RES and the expected response XRES do not match. In that case the VLR or SGSN sends *user authentication reject* to the MS. The VLR or SGSN shall inform the HLR/AuC (see

6.3.3.4) about the failure and may request for new quintets (see 6.3.3.1).

The VLR and SGSN shall use or attempt to use a quintet only once. Hence, quintets cannot be re-used. A VLR or SGSN can serve a user securely even when links to the user's HLR/AuC are unavailable by means of re-use of previously derived cipher and integrity keys. In this manner a secure connection can be set up without the need for an authentication and key agreement and a fresh quintet. Authentication is in that case based on a shared integrity key, by means of data integrity protection of signalling messages (see 6.4).

6.3.2.2 Re-synchronisation

An overview of the mechanism for resynchronisation is shown in Figure 6.3.2:

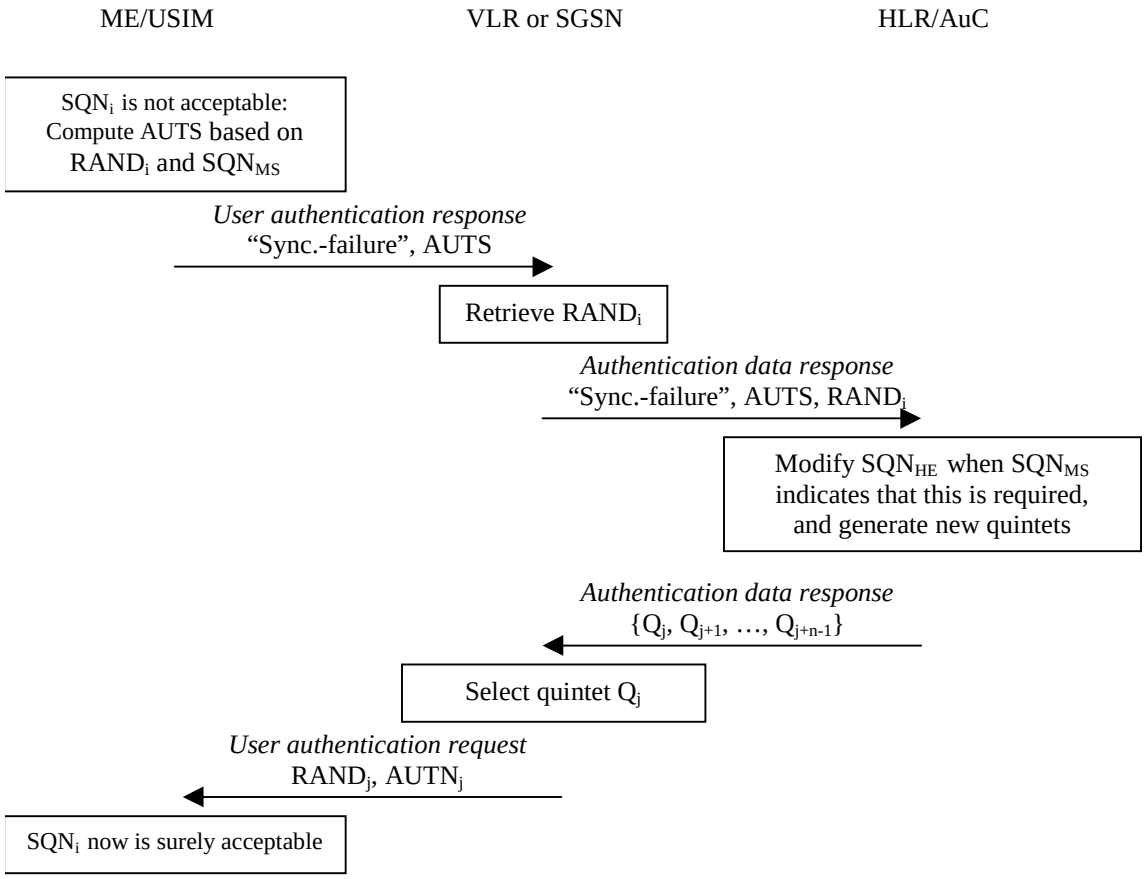

Figure 6.3.2: Re-synchronisation mechanism

The mechanism for re-synchronisation is triggered by the unsuccessful verification by the USIM of the freshness of SQN_i that is included in $AUTN_i$ (see 6.3.2.1). The USIM then sends a *user authentication response* to the VLR or SGSN including an indication of synchronisation failure and a re-synchronisation token AUTS, that includes the current value of the counter SQN_{MS}. The VLR or SGSN appends the challenge $RAND_i$ and sends an *authentication data request* to the HLR/AuC with indication of synchronisation failure and including ($RAND_i$, AUTS). Upon receipt of such a request, the HLR/AuC verifies whether the value of SQN_{MS} mandates that the SQN_{HE} needs to be modified. If necessary, the HLR/AuC shall set SQN_{HE} equal to SQN_{MS}. Consecutively, the HLR/AuC sends the VLR quintets generated from the current SQN_{HE}, which are forwarded to the user.

The new quintet will now surely be acceptable to the user. For a formal proof see TR 33.902.

6.3.3 Procedures

6.3.3.1 Distribution of authentication data from HE to SN

The purpose of this procedure is to provide the VLR or SGSN with an array of fresh quintets from the user's HE to perform a number of authentication and key agreement exchanges.

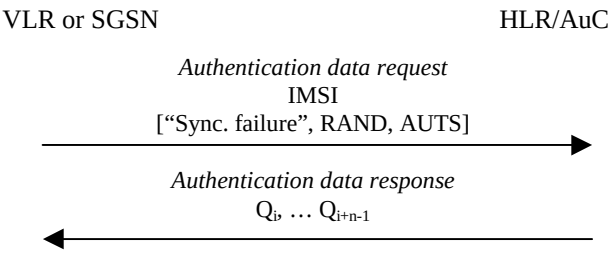

Figure 6.3.3: Distribution of authentication data from HE to SN

The VLR or SGSN invokes the procedures by requesting quintets to the HLR/AuC.

The protocol steps are as follows:

a) The VLR or SGSN sends an *authentication data request* to the HLR/AuC; this message shall contain the IMSI and may contain an indication of synchronisation failure and shall in that case also contain a re-synchronisation token AUTS and a challenge RAND.

b) Upon receipt of an *authentication data request* with an indication of synchronisation failure the HLR/AuC acts as described in 6.3.4.4. It shall verify whether the counter SQN_{HE} needs to be modified and contingent on the outcome set SQN_{HE} to SQN_{MS}.

c) The HLR/AuC then sends an authentication data response back to the VLR or SGSN that includes a quintet Q or an ordered array of quintets $\{Q_i, \ldots, Q_{i+n-1}\}$ that have/has been generated as described in 6.3.4.1. The quintet(s) may have been generated in advance or on demand. In case a synchronisation failure caused the counter SQN_{HE} to be reset the quintet(s) are/is generated on demand.

d) Upon receipt the VLR or SGSN stores the user identity and/or quintets it receives, maintaining the ordering.

6.3.2.2 Authentication and key agreement

The purpose of this procedure is to authenticate the user and establish a new pair of cipher and integrity keys between the VLR or SGSN and the ME/USIM. During the authentication, the user verifies data origin, the integrity and the freshness of the quintet that is used. The procedure is shown in Figure 6.3.4.

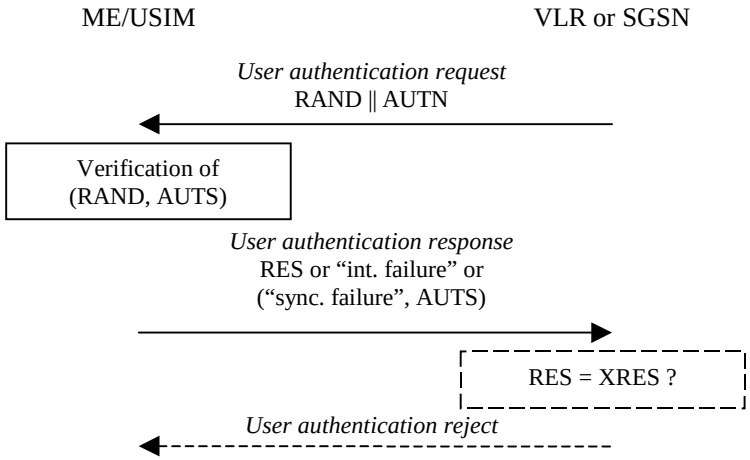

Figure 6.3.4: Over-the-air authentication and key agreement procedure

The VLR or SGSN invokes the procedure by selecting the next unused quintet from the ordered array of quintets in the VLR or SGSN database.

The protocol steps are the following:

a) The VLR or SGSN sends to the user a *user authentication request*, including the network challenge RAND and the authentication token AUTN from the selected quintet.

b) The USIM then verifies the (RAND, AUTN) pair as described in 6.3.4.2, and contingent on the outcome acts as follows:

   i) In case the data origin and integrity of (RAND, AUTN) is successfully verified, and the sequence number is acceptable, the ME sends a *user authentication response* back with an indication of success and including the user response RES;

   ii) In case the data origin and integrity of (RAND, AUTN) is not successfully verified, the ME sends a *user authentication response* back with and indication of integrity failure (without any parameter);

   iii) In case the data origin and integrity of (RAND, AUTN) is successfully verified, but the sequence number is not acceptable, the ME sends a *user authentication response* back with and indication of synchronisation failure and including the re-synchronisation token AUTS.

c) Upon receipt of the *user authentication response*, the VLR or SGSN acts as follows:

   i) In case of success, the VLR or SGSN compares the received response RES with the expected response XRES. In case there is a match, the VLR or SGSN selects the CK and IK and authentication ends successfully. On the other hand, in case there is a mismatch, the VLR or SGSN sends *user authentication reject* to the user and authentication ends unsuccessfully. The VLR or SGSN should in that case report the failure to the HE, as described in 6.3.2.4.

   ii) In case of integrity failure, the VLR or SGSN may report the failure to the HE, as described in 6.3.2.4 or may request for new quintets using the procedure described in 6.3.2.1.

   iii) In case of synchronisation failure, the VLR or SGSN may report the failure to the HE, as described in 6.3.2.4 but should request for new quintets using the procedure described in 6.3.2.1, include an indication of synchronisation failure, the parameter AUTS and the parameter RAND. The VLR or SGSN deletes the user's quintets from the database.

The VLR or SGSN shall discard any unsolicited user authentication response, in particular, it shall discard an unsolicited user authentication response with indication of synchronisation failure.

The VLR or SGSN shall not send a user new *user authentication requests* before it has received a response of the user or the before a certain time period has elapsed.

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

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

The procedure is shown in Figure 6.3.5.

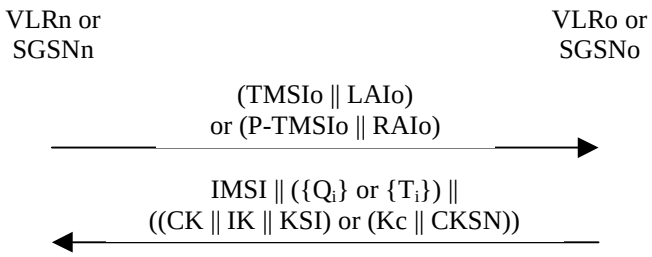

Figure 6.3.5: Distribution of IMSI and temporary authentication data within one serving network domain

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

The protocol steps are as follows:

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

b) The VLRo (resp. SGSNo) searches the user data in the database.

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

   i) shall include the IMSI,

   ii) may include a number of unused authentication vectors (quintets or triplets) and

   iii) may include the current security context data: CK, IK and KSI (UMTS) or Kc and CKSN (GSM).

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

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

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

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

6.3.2.4 Reporting authentication failures from SN to HE

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

The procedure is shown in Figure 6.3.6.

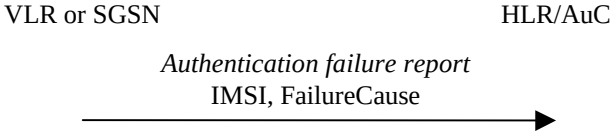

Figure 6.3.6: Reporting authentication failures from SN to HE

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

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

6.3.4 Functions

6.3.4.1 Generation of quintets in the AuC

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

The AuC generates quintets as follows:

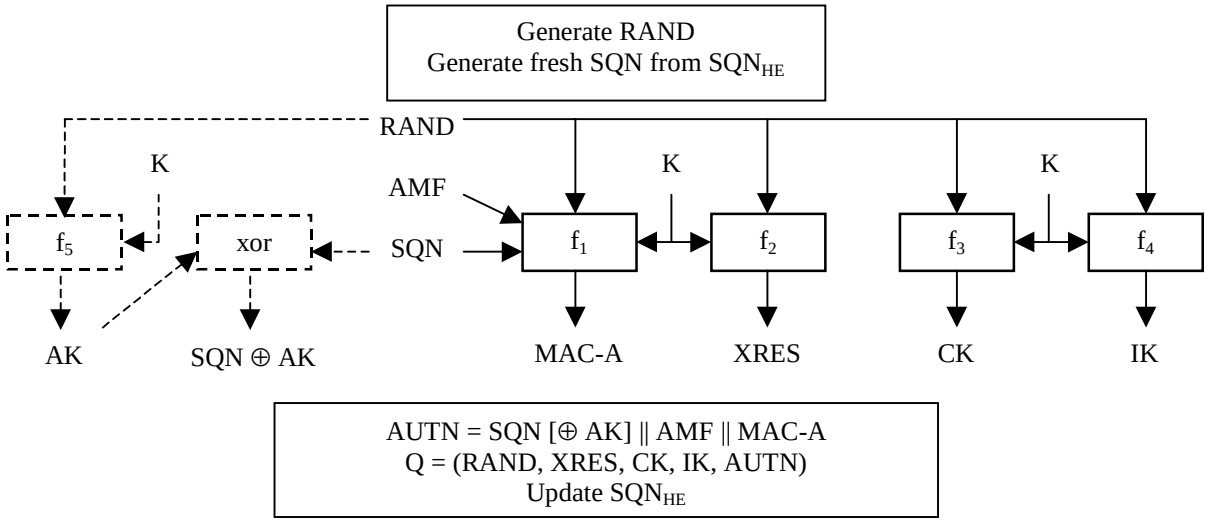

Figure 6.3.7: Generation of quintets in the AuC

a) The HLR/AuC generates a fresh sequence number SQN from the counter SQN_{HE}. The HE has some flexibility in the management of sequence numbers, but the requirements listed in 6.3.1 need to be fulfilled, in particular, the generation mechanism needs to support the re-synchronisation mechanism described in 6.3.2.2. Annex C.1 contains a detailed description of a mechanism to generate sequence numbers that satisfies all conditions.

b) The HLR/AuC generates an unpredictable challenge RAND.

c) The HLR/AuC then computes

   i) a message authentication code for authentication MAC-A = $f1_K$(SQN || RAND || AMF) where f1 is a message authentication function;

   ii) an expected response XRES = $f2_K$ (RAND) where f2 is a (possibly truncated) message authentication function;

   iii) a cipher key CK = $f3_K$ (RAND) where f3 is a key generating function;

   iv) an integrity key IK = $f4_K$ (RAND) where f4 is a key generating function;

d) If SQN is to be concealed, in addition the HLR/AuC computes an anonymity key AK = $f5_K$ (RAND) where f5 is a key generating function and computes the concealed sequence number SQN ⊕ AK = SQN xor AK.

e) Finally, the HLR/AuC assembles the authentication token AUTN = SQN [⊕ AK] || AMF || MAC-A and the quintet Q = (RAND, XRES, CK, IK, AUTN) and updates the counter SQN_{HE}.

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

The concealment of the sequence number is optional. Concealment is recommended when sequence numbers are derived from counters whereby strong correlation exists between consecutive sequence numbers that are sent to the same user. In that the concealment is required to provide location and identity confidentiality. However, when time-based counters are used to derive sequence numbers from, this lowers the correlation considerably, and the concealment can safely be omitted.

6.3.4.2 Authentication and key derivation in the USIM

Upon receipt of a (RAND, AUTN) pair the USIM acts as follows:

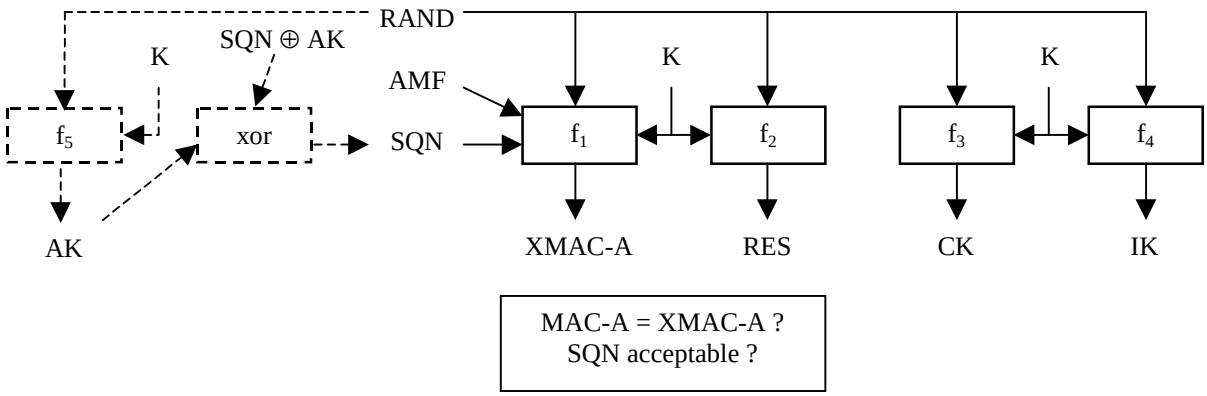

Figure 6.3.8: Authentication and key derivation in the USIM

a) If the sequence number is concealed, the USIM computes the anonymity key AK = $f5_K$(RAND) and retrieves the unconcealed sequence number SQN = (SQN ⊕ AK) xor AK.

b) The USIM then computes XMAC-A = $f1_K$ (SQN || RAND || AMF) and compares XMAC-A with MAC-A included in AUTN.

c) If they are different, the USIM triggers the ME to send back a *user authentication response* with indication of integrity failure to the VLR or SGSN and abandons the procedure. The remainder of this paragraph applies thus for the case where XMAC-A and MAC-A are equal.

d) Next the USIM verifies that the received sequence number SQN is acceptable. The HE has some flexibility in the management of sequence numbers, but the requirements listed in 6.3.1 need to be fulfilled, in particular, the verification mechanism needs to protect against wrap around and allow to a certain extent the out-of-order use of quintets. Annex C.2 contains a detailed description of a mechanism to generate sequence numbers that satisfies all conditions.

e) If the sequence number SQN is not acceptable, the USIM computes the re-synchronisation token AUTS as described in 6.4.3.3 and triggers the ME to send back a *user authentication response* back to the VLR or SGSN, with an indication of synchronisation failure, including the re-synchronisation token AUTS and abandons the procedure. The remainder of this paragraph applies thus for the case where SQN is acceptable.

f) The USIM then computes the response RES = $f2_K$(RAND) and triggers the ME to send back a user authentication response back to the VLR or SGSN, with an indication of successful receipt of the signed challenge and including the response RES.

g) Finally the user computes the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND).

Note: If this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND.

6.3.4.3 Generation of re-synchronisation token in the USIM

Upon the assertion of a synchronisation failure, the USIM generates a re-synchronisation token as follows:

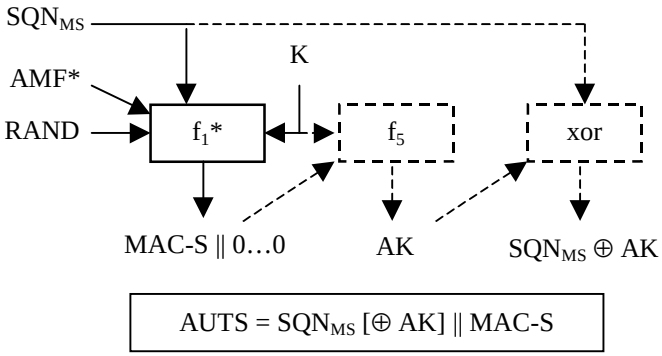

Figure 6.3.9: Generation of re-synchronisation token in the USIM

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

b) If SQN$_{MS}$ is to be concealed with an anonymity key AK, the USIM computes AK = $f5_K$(MAC-S || 0…0) and the concealed counter value is then computed as SQN$_{MS}$ ⊕ AK.

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

6.3.4.4 Re-synchronisation in the HLR/AuC

Upon receipt of an indication of synchronisation failure and a (AUTS, RAND) pair, the HLR/AuC acts as follows:

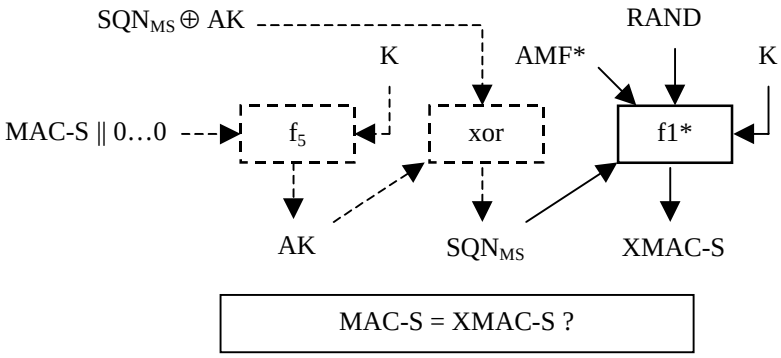

Figure 6.3.10: Re-synchronisation in the HLR/AuC

a) If SQN$_{MS}$ is concealed with an anonymity key AK, the HLR/AuC computes AK = $f5_K$(MAC-S || 0…0) and retrieves the unconcealed counter value as SQN$_{MS}$ = (SQN$_{MS}$ ⊕ AK) xor AK.

b) The HLR/AuC now verifies whether SQN generated from SQN$_{HE}$ would be acceptable for a USIM that has SQN$_{MS}$. This test is identical to the test performed by the USIM described in 6.3.4.2. If SQN generated from SQN$_{HE}$ would be acceptable, then the value of SQN$_{HE}$ need not be modified and the function is aborted.

c) If SQN generated from SQN$_{HE}$ would not be acceptable, then the HLR/AuC computes XMAC-S = $f1^*_K$(SQN$_{MS}$ || RAND || AMF*), whereby AMF* is a default value for AMF used in re-synchronisation and the HLR/AuC then compares MAC-S and XMAC-S. If there is a match, the need to modify SQN$_{HE}$ is recognised, otherwise again, it is decided that SQN$_{HE}$ should not be modified.

Note: When a synchronisation failure is caused by an out-of-order use of a quintet, SQN$_{HE}$ will be such that SQN generated from SQN$_{HE}$ would be acceptable for a USIM that has SQN$_{MS}$. Therefore SQN$_{HE}$ will not have to be modified and XMAC-S need not be computed. If SQN$_{MS}$ is not concealed no cryptographic computation is required in this case.

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

***Document* S3-000257**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

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

33.102	CR		Current Version:	3.4.0

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

For submission to:	SA 3 #12	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: Siemens Atea **Date:** 3 April 2000

Subject: 3G-2G and 2G-3G Handover for CS services

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	X

Reason for change: Removal of storage of CK and IK in the non-anchor MSC/VLR, as it is the anchor MSC/VLR that provides the new keys in the event of handover.

Clauses affected: 6.8.4, 6.8.5

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.

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

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

6.8.4.1 UMTS security context

A UMTS security context in UTRAN is only established for a UMTS subscriber with a R99+ ~~UE~~ME.

At the network side, three cases are distinguished:

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

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

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

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

6.8.4.2 GSM security context

A GSM security context in UTRAN is only established for a GSM subscribers with a R99+ ~~UE~~ME.

At the network side, two cases are distinguished:

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

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

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

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

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

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

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

6.8.5.1 UMTS security context

A UMTS security context in GSM BSS is only established for UMTS subscribers with R99+ ~~UE~~ME under GSM BSS controlled by a R99+ VLR/SGSN.

At the network side, two cases are distinguished:

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

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

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

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

6.8.5.2 GSM security context

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

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

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

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

S3-000267

3GPP TSG-CN WG2
Kista, Sweden, 2-3 March 2000

Document N2B000428
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.

29.060	CR	080r1	Current Version:	3.3.0

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

For submission to:	CN#7	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 [X] Core Network [X]

Source: Ericsson **Date:** 2000-03-01

Subject: GTP Security

Work item: GTP Enhancements

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

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

Reason for change: The Security Group (S3) have requirements on the Core Network signalling protocols (MAP and GTP).

For GTP signalling it is proposed that, since IP is the transport technology used, IP Security shall be used. A reference to 3G TS 33.102 is proposed to be made in a new section 13.3 on GTP Security.

Clauses affected: Clause 4, 13.3

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 General

This document defines the GPRS Tunnelling Protocol (GTP), i.e. the protocol between GPRS Support Nodes (GSNs) in the UMTS/GPRS backbone network. It includes both the GTP signalling (GTP-C) and data transfer (GTP-U) procedures. It also lists the messages and information elements used by the GTP based charging protocol GTP', which is described in GSM 12.15.

GTP is defined for the Gn interface, i.e. the interface between GSNs within a PLMN, and for the Gp interface between GSNs in different PLMNs. Only GTP-U is defined for the Iu interface between Serving GPRS Support Node (SGSN) and the UMTS Terrestrial Radio Access Network (UTRAN).

The Internet protocol (IP) is the transport network technology used to carry GTP. In order to secure GTP signalling IP Security will be used.

On the Iu interface, the Radio Access Network Application Part (RANAP) protocol is performing the control function for GTP-U.

GTP' is defined for the interface between CDR generating functional network elements and Charging Gateway(s) within a PLMN. Charging Gateway(s) and GTP' protocol are optional, as the Charging Gateway Functionalities may either be located in separate network elements (Charging Gateways), or alternatively be embedded into the CDR generating network elements (GSNs) when the GSN-CGF interface is not necessarily visible outside the network element. These interfaces relevant to GTP are between the grey boxes shown in the figure below.

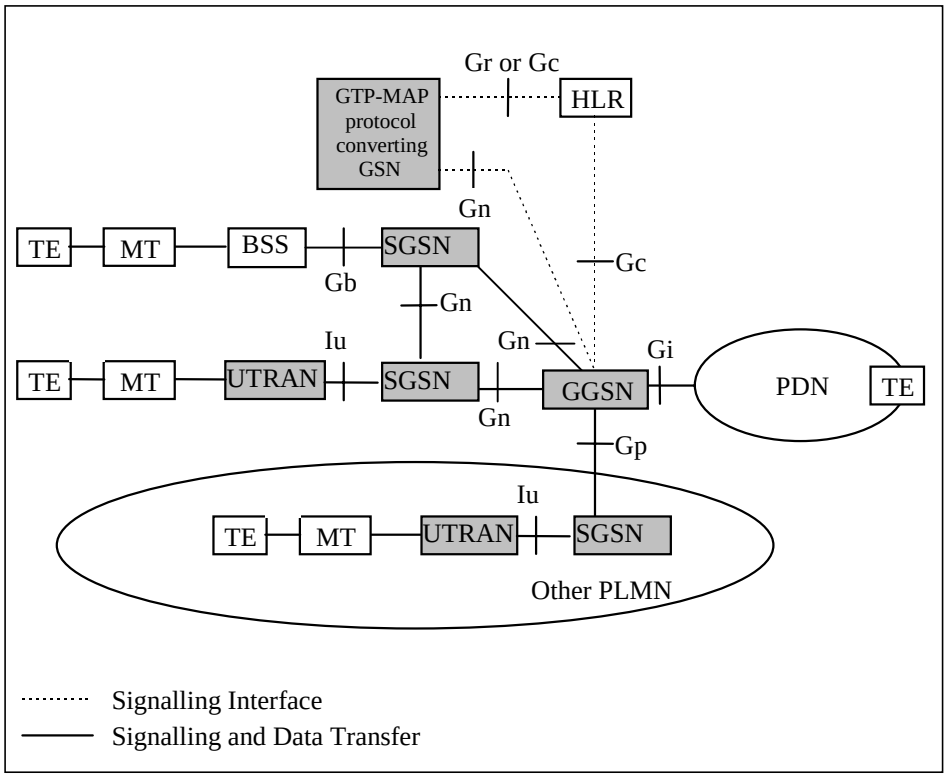

Figure 1: GPRS Logical Architecture with interface name denotations

GTP allows multiprotocol packets to be tunnelled through the UMTS/GPRS Backbone between GSNs and between SGSN and UTRAN.

In the signalling plane, GTP specifies a tunnel control and management protocol (GTP-C) which allows the SGSN to provide packet data network access for an MS. Signalling is used to create, modify and delete tunnels.

In the transmission plane, GTP uses a tunnelling mechanism (GTP-U) to provide a service for carrying user data packets. The choice of path is dependent on whether the user data to be tunnelled requires a reliable link or not.

The GTP-U protocol is implemented by SGSNs and GGSNs in the UMTS/GPRS Backbone and by Radio Network Controllers (RNCs) in the UTRAN. The GTP-C protocol is implemented by SGSNs and GGSNs in the UMTS/GPRS Backbone. No other systems need to be aware of GTP. UMTS/GPRS MSs are connected to an SGSN without being aware of GTP.

It is assumed that there will be a many-to-many relationship between SGSNs and GGSNs. A SGSN may provide service to many GGSNs. A single GGSN may associate with many SGSNs to deliver traffic to a large number of geographically diverse mobile stations.

SGSN and GGSN implementing GTP protocol version 1 should be able to fallback to GTP protocol version 0. All GSNs should be able to support all earlier GTP versions.

*** *Next Change* ***

13.3 GTP Security

In order to secure GTP signalling IP Security mechanisms will be used. The requirements on GTP Security and the mechanisms to be used are further described in TS 3G 33.102 “3G Security; Security Architecture” [18].

3GPP TSG SA WG3 Security — S3#12 **S3-000270**

11-14 April, 2000, Stockholm, Sweden

From: TSG SA WG3

To: SMG9, TSG SA WG1

Title: Draft Answer to LS New SIM toolkit feature: "Auto-answer & Mute-ringing"

Contact: Ludovic Rousseau, Email: Ludovic.Rousseau@gemplus.com

---

S3 thanks SMG9 for their liaison statement entitled New SIM toolkit feature: "Auto-answer & Mute-ringing" (3GPP S3 document: TSG S3-000164, SMG9 document Tdoc 9-00-0158).

S3 has studied the proposed security mechanisms to secure this “Auto-answer & Mute-ringing” feature:

- Loud sound signal
- Timeout control
- CLI (Calling Line Identifier) control

The CLI cannot be used as a secure authentication. The CLI is controlled by the operator and could easily be faked. This is a major concern when the user is roaming in a “foreign” operator network.

S3 sees a major security problem: this feature will provide a way to listen to vocal communications occurring in a room. It is worst than eavesdropping an existing phone call.

This Auto-answer & Mute-ringing feature brings a lot of security impacts and new threats. CLI authentication is not enough. S3 decided to not support this feature for now.

If S1 wants to support this feature, S3 will examine it again provided a new security mechanism is proposed.

S3-000277

3GPP TSG-CN 4
Charleston, USA, 27-31 March 2000

Document N4-000046
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.

29.060	**CR**	**095**	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:	CN#8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic	X	

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

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

Source: Nortel Networks **Date:** 22 March 2000

Subject: GTP Security

Work item: GTP Enhancements

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

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

Reason for change: The Security Group (S3) have requirements on the Core Network signalling protocols (MAP and GTP).

For GTP it is proposed that, since IP is the transport technology used, IP Security techniques may be used. It is assumed that 3G TS 33.102 shall specify the GTP Security Requirements.

Clauses affected: Clause 4, 13.3

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 General

This document defines the GPRS Tunnelling Protocol (GTP), i.e. the protocol between GPRS Support Nodes (GSNs) in the UMTS/GPRS backbone network. It includes both the GTP signalling (GTP-C) and data transfer (GTP-U) procedures. It also lists the messages and information elements used by the GTP based charging protocol GTP', which is described in GSM 12.15.

GTP is defined for the Gn interface, i.e. the interface between GSNs within a PLMN, and for the Gp interface between GSNs in different PLMNs. Only GTP-U is defined for the Iu interface between Serving GPRS Support Node (SGSN) and the UMTS Terrestrial Radio Access Network (UTRAN).

The Internet protocol (IP) is the transport network technology used to carry GTP. IP Security techniques such as IPSec may be used to provide secure transport of GTP.

On the Iu interface, the Radio Access Network Application Part (RANAP) protocol is performing the control function for GTP-U.

GTP' is defined for the interface between CDR generating functional network elements and Charging Gateway(s) within a PLMN. Charging Gateway(s) and GTP' protocol are optional, as the Charging Gateway Functionalities may either be located in separate network elements (Charging Gateways), or alternatively be embedded into the CDR generating network elements (GSNs) when the GSN-CGF interface is not necessarily visible outside the network element. These interfaces relevant to GTP are between the grey boxes shown in the figure below.

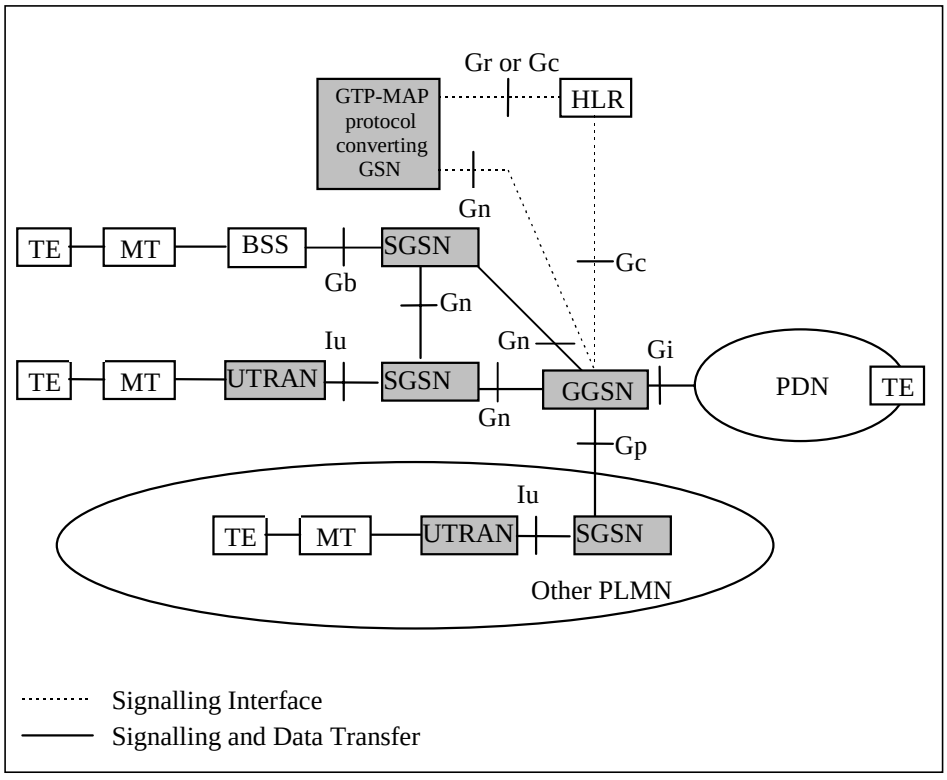

Figure 1: GPRS Logical Architecture with interface name denotations

GTP allows multiprotocol packets to be tunnelled through the UMTS/GPRS Backbone between GSNs and between SGSN and UTRAN.

In the signalling plane, GTP specifies a tunnel control and management protocol (GTP-C) which allows the SGSN to provide packet data network access for an MS. Signalling is used to create, modify and delete tunnels.

In the transmission plane, GTP uses a tunnelling mechanism (GTP-U) to provide a service for carrying user data packets. The choice of path is dependent on whether the user data to be tunnelled requires a reliable link or not.

The GTP-U protocol is implemented by SGSNs and GGSNs in the UMTS/GPRS Backbone and by Radio Network Controllers (RNCs) in the UTRAN. The GTP-C protocol is implemented by SGSNs and GGSNs in the UMTS/GPRS Backbone. No other systems need to be aware of GTP. UMTS/GPRS MSs are connected to an SGSN without being aware of GTP.

It is assumed that there will be a many-to-many relationship between SGSNs and GGSNs. A SGSN may provide service to many GGSNs. A single GGSN may associate with many SGSNs to deliver traffic to a large number of geographically diverse mobile stations.

SGSN and GGSN implementing GTP protocol version 1 should be able to fallback to GTP protocol version 0. All GSNs should be able to support all earlier GTP versions.

*** *Next Change* ***

13.3 GTP Security

In order to provide secure transport of GTP IP Security techniques defined by the IETF may be used, for example IPSec. The requirements on GTP Security are described in TS 3G 33.102 “3G Security; Security Architecture” [18].

3GPP TSG SA WG3 (Security) meeting #12
Stockholm, 11-14 April, 2000

***Document* S3-000290**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

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

33.102	CR		Current Version:	3.4.0

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

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

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

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

Source: Ericsson **Date:** 2000-04-13

Subject: Clarification on the UIA and UEA selection

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: - to clarify how the HE preference is taken into account when selecting UIA and UEA

Clauses affected: 6.4.2, 6.4.5

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.

6.4.2 Ciphering and integrity mode negotiation

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

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

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

2) If the MS and the SN have at least one version of the UIA algorithm in common, then the network shall select one of the mutually acceptable versions of the UIA algorithm for use on that connection. The network shall then take into account the UIA preferences of the MS and select among the common UIAs the most preferred UIA of the MS.

The network shall compare its ciphering capabilities and preferences, and any special requirements of the subscription of the MS, with the~~ose~~ ciphering capabilities and preferences 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. The network shall then take into account the UEA preferences of the MS and select among the common UEAs the most preferred UIA of the MS.

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

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

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

***Document* S3-000291**
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	087	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:	TSG 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	X	UTRAN / Radio	X	Core Network	

Source: TSG SA WG 3 **Date:** 13 April 2000

Subject: Limitation and reduction of the effective cipher key length by the serving network

Work item: Security

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

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

Reason for change: The definition of a second ciphering capability with reduced effective key length facilitates the deployment of UMTS in countries where lawful restrictions exist on the use of cipher keys with a long effective key length.

Clauses affected: 6.6.6

Other specs affected:

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

Other comments: Is there a need to reserve some UEA-values for proprietary use?

help.doc

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

6.6.6 ~~UEA identification~~Ciphering capabilities

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

"0000_2" : UEA0, no encryption.

"0001_2" : UEA1, f8 with Kasumi with effective key length of the cipher key up to 128 bits.

"0010_2" : UEA2, f8 with Kasumi with effective key length of the cipher key up to ~~64~~56 bits.

~~"0011_2" : UEA3, f8 with Kasumi with effective key length of the cipher key up to 54 bits.~~

~~"0100_2" : UEA4, f8 with Kasumi with effective key length of the cipher key up to 40 bits.~~

The remaining values are not defined.

In case of UEA1, the RNC and the ME feed the cipher key CK (as it was provided by the VLR or SGSN and the USIM) as input to the Kasumi algorithm.

In case of UEA2~~-UEA4~~, the RNC and the ME derive from the cipher key CK (as it was provided by the VLR or SGSN and the USIM) a modified cipher key CK' with a reduced effective key length ~~n (respectively 64~~56~~, 54 and 40)~~ bits, from the cipher key CK:

CK'[k] = CK[k mod ~~n~~56], for $0 \leq k < 128$.

The RNC and the ME then feed the modified cipher key CK' as input to the Kasumi algorithm.