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

S3-000251

Agenda Item:

Source: Siemens Atea

Title: Review of TS 24.008

Document for: Decision

1 Introduction

This document is the result of a review of TS 24.008. Most of the security is well-implemented but there are some incosistencies and some open issues, which are listed below. On the following pages the relevant clauses of TS 24.008 are presented as well as suggested changes.

2 Inconsistencies

1. In TS 33.102 the parameter AUTN has a fixed length of 16 octets (6 octets for SQN, 2 octets for AMF and 8 octets for MAC-A), in TS 24.008 the parameter AUTN has a variable length of 14 to 18 octets. This is due to the late decision of SA-3 to fix the length of SQN, a change that has not been carried out in TS 24.008.

2. In TS 33.102 the re-synchronisation parameter AUTS has a fixed length of 14 octets (6 octets for SQN-MS, 8 octets for MAC-S), in TS 24.008 the parameter AUTS has a variable length of 12 to 16 octets. This is again due to the late decision of SA-3 to fix the length of SQN, a change that has not been carried out in TS 24.008.

3. In TS 33.102 the derivation of a GSM cipher key when UMTS AKA is executed is optional, in TS 24.008 it is considered mandatory.

4. In TS 33.102 the authentication failure message indicating a MAC failure does not contain a parameter, in TS 24.008 it does.

5. In TS 33.102 the authentication failure message indicating a sync failure contain the parameter AUTS, in TS 24.008 it carries "parameters".

6. TS 33.102 specifies that while the VLR or SGSN waits for an authentication response, no further authentication requests must be sent out. There is no mention of that in TS 24.008.

7. TS 33.102 specifies that quintets must be deleted after use and must never be re-used. There is no mention of that in TS 24.008. On the contrary, for the PS domain it is described that the authentication and ciphering command can be repeated several times after time-out. Surprisingly, for the CS domain no such repetition is foreseen. The repetition in the PS domain may lead to unnecessary re-synchronisation procedures.

8. TS 33.102 specifies that the VLR or SGSN must delete all quintets in storage at the receipt of new quintets after the MS signalled a synchronisation failure. There is no mention of that in TS 24.008.

3 Open issues

9. TS 24.008 does not specify what the VLR or SGSN should do when the MS rejects a UMTS authentication token indicating a MAC failure.

10. TS 24.008 does not fully specify what the VLR or SGSN should do when the MS indicates a synchronisation failure to the network.

4.3.2 Authentication procedure

4.3.2a Authentication procedure used for a UMTS authentication challenge

The purpose of the authentication procedure is fourfold (see TS 33.102):

First to permit the network to check whether the identity provided by the mobile station is acceptable or not~~ (see TS 33.102)~~;

Second to provide parameters enabling the mobile station to calculate a new UMTS ciphering key.

Third to provide parameters enabling the mobile station to calculate a new UMTS integrity key.

Fourth to permit the mobile station to authenticate the network

The cases where the authentication procedure should be used are defined in ~~GSM 02.09~~TS 33.102.

The UMTS authentication procedure is always initiated and controlled by the network. However, ~~in the case of a UMTS authentication challenge, ~~there is the possibility for the MS to reject the UMTS authentication challenge sent by the network. UMTS authentication challenge shall be supported by a ME supporting GSM or UMTS radio access.

A UMTS security context is established ~~in ~~between the MS and the network when a UMTS authentication challenge is performed in GSM or in UMTS. After a successful UMTS authentication, the UMTS ciphering key, the UMTS integrity key, the GSM ciphering key and the ciphering key sequence number, are stored both in the network and the MS.

4.3.2b Authentication Procedure used for a GSM authentication challenge

The purpose of the authentication procedure is twofold (see GSM 03.20):

First to permit the network to check whether the identity provided by the mobile station is acceptable or not~~ (see GSM 03.20)~~;

Second to provide parameters enabling the mobile station to calculate a new GSM ciphering key.

The cases where the authentication procedure should be used are defined in GSM 02.09.

The authentication procedure is always initiated and controlled by the network. GSM authentication challenge shall be supported by a ME supporting GSM or UMTS radio access.

A GSM security context is established in the MS and the network when a GSM authentication challenge is performed in GSM or in UMTS. After a successful GSM authentication, the GSM ciphering key and the ciphering key sequence number, are stored both in the network and the MS.

4.3.2.1 Authentication request by the network

The network initiates the authentication procedure by transferring an AUTHENTICATION REQUEST message across the radio interface and starts the timer T3260. The AUTHENTICATION REQUEST message contains the parameters necessary to calculate the response parameters (see GSM 03.20 (in case of GSM authentication challenge) and TS 33.102 (in case of an UMTS authentication challenge)).

In a GSM authentication challenge, the AUTHENTICATION REQUEST message also contains the GSM ciphering ciphering key sequence number allocated to the key which may be computed from the given parameters. The network shall mark the used GSM authentication challenge as "used". GSM authentication challenges should not be re-used; they may be re-used under the strict conditions described in GSM 02.09.

In a UMTS authentication challenge, the AUTHENTICATION REQUEST message also contains the ciphering key sequence number allocated to the key set of UMTS ciphering key, UMTS integrity key and GSM ciphering key which may be computed from the given parameters. The network shall delete the used UMTS authentication challenge but store the network challenge RAND until the user has responded or the timer T3260 has expired for re-synchronisation. UMTS authentication challenges shall not be re-used by the network.

4.3.2.2 Authentication response by the mobile station

The mobile station shall be ready to respond upon an AUTHENTICATION REQUEST message at any time whilst a RR connection exists. With exception of the cases described in 4.3.2.5.1, it shall process the challenge information and send back an AUTHENTICATION RESPONSE message to the network.

In a GSM authentication challenge, the new GSM ciphering key calculated from the challenge information shall overwrite the previous GSM ciphering key and any previously stored UMTS ciphering key and UMTS integrity key shall be deleted. The new GSM ciphering key shall be stored on the SIM together with the ciphering key sequence number.

In a UMTS authentication challenge, the new UMTS ciphering key, the new GSM ciphering key and the new UMTS integrity key calculated from the challenge information shall overwrite the previous UMTS ciphering key, GSM ciphering key and UMTS integrity key. The new UMTS ciphering key, GSM ciphering key and UMTS integrity key are stored on the SIM together with the ciphering key sequence number.

The SIM will provide the mobile station with the authentication response, based upon the authentication challenge from the network. A UMTS authentication challenge will result in the SIM passing a RES, a UMTS ciphering key, a UMTS integrity key to the ME. In addition, a UMTS authentication challenge may result in the SIM passing a GSM ciphering key to the ME. A GSM authentication challenge will result in the SIM passing a SRES and a GSM ciphering key to the ME.

4.3.2.3 Authentication processing in the network

Upon receipt of the AUTHENTICATION RESPONSE message, the network stops the timer T3260 and checks the validity of the response (see GSM 03.20 in case of a GSM authentication challenge respective TS 33.102 in case of an UMTS authentication challenge). If authentication fails, see 4.3.2.5.

Upon receipt of the AUTHENTICATION FAILURE message, the network stops the timer T3260.

In MAC failure case, the network may distinguish between the two different ways of identification used by the mobile station:

- the TMSI was used;
- the IMSI was used.

If the TMSI has been used, the network may decide to initiate the identification procedure. If the IMSI given by the mobile station then differs from the one the network had associated with the TMSI, the authentication should be restarted with the correct parameters. If the IMSI provided by the MS is the expected one (i.e. authentication has really failed), the network should proceed as described in 4.3.2.5.

~~the procedural behaviour is ffs.~~ In Synch failure case, the ~~core~~ network ~~may~~ shall send the user's HLR/AuC a request for new quintets, include an indication of synchronisation failure, and include the random challenge RAND and the re-synchronisation token AUTS. The procedures at the radio side are ffs. ~~renegotiate with the HLR/AuC and provide the MS with new authentication parameters.~~

4.3.2.4 Ciphering key sequence number

The security parameters for authentication and ciphering are tied together in sets. In a GSM authentication challenge, from a challenge parameter RAND both the authentication response parameter SRES and the GSM ciphering key can be computed given the secret key associated to the IMSI. In a UMTS authentication challenge, from a challenge parameter RAND, the authentication response parameter RES and the UMTS ciphering key and the UMTS integrity key can be computed given the secret key associated to the IMSI. In addition, a GSM ciphering key can be computed from the UMTS ciphering key and the UMTS integrity key by means of an unkeyed conversion function. The computation of a GSM ciphering key is optional.

In order to allow start of ciphering on a RR connection without authentication, the ciphering key sequence numbers are introduced. The ciphering key sequence number is managed by the network in the way that the AUTHENTICATION REQUEST message contains the ciphering key sequence number allocated to the GSM ciphering key (in case of a GSM authentication challenge) or the UMTS ciphering key and the UMTS integrity key (in case of a UMTS authentication challenge) which may be computed from the RAND parameter carried in that message.

The mobile ~~station~~ equipment and the SIM store~~s~~ the ciphering key sequence number with the GSM ciphering key (in case of a GSM authentication challenge) and the UMTS ciphering key and the UMTS integrity key (in case of a UMTS authentication challenge) and indicates to the network in the first message (LOCATION UPDATING REQUEST, CM SERVICE REQUEST, PAGING RESPONSE, CM RE-ESTABLISHMENT REQUEST) which ciphering key sequence number the stored GSM ciphering key (in case of a GSM authentication challenge) or set of UMTS ciphering and UMTS integrity keys and possibly a derived GSM ciphering key (in case of a UMTS authentication challenge) has.

When the deletion of the ciphering key sequence number is described this also means that the associated GSM ciphering key, the UMTS ciphering key and the UMTS integrity key shall be considered as invalid (i.e. the established GSM security context or the UMTS security context is no longer valid).

In GSM, the network may choose to start ciphering with the stored GSM ciphering key (under the restrictions given in GSM 02.09) if the stored ciphering key sequence number and the one given from the mobile station are equal.

In UMTS, the network may choose to start ciphering and integrity with the stored UMTS ciphering key and UMTS integrity key (under the restrictions given in GSM 02.09 and TS 33.102) if the stored ciphering key sequence number and the one given from the mobile station are equal.

NOTE: In some specifications the term KSI (Key Set Identifier) might be used instead of the term ciphering key sequence number.

4.3.2.5 GSM Authentication not accepted by the network

If GSM authentication fails, i.e. if the response is not valid, the network may distinguish between the two different ways of identification used by the mobile station:

- the TMSI was used;
- the IMSI was used.

If the TMSI has been used, the network may decide to initiate the identification procedure. If the IMSI given by the mobile station then differs from the one the network had associated with the TMSI, the authentication should be restarted with the correct parameters. If the IMSI provided by the MS is the expected one (i.e. authentication has really failed), the network should proceed as described below.

If the IMSI has been used, or the network decides not to try the identification procedure, an AUTHENTICATION REJECT message should be transferred to the mobile station.

After having sent this message, all MM connections in progress (if any) are released and the network should initiate the RR connection release procedure described in section 3.5.of 04.18 (GSM) or in TS 25.331 (UMTS).

Upon receipt of an AUTHENTICATION REJECT message, the mobile station shall set the update status in the SIM to U2 ROAMING NOT ALLOWED, delete from the SIM the stored TMSI, LAI and ciphering key sequence number. The SIM shall be considered as invalid until switching off or the SIM is removed.

If the AUTHENTICATION REJECT message is received in the state IMSI DETACH INITIATED the mobile station shall follow section 4.3.4.3 of 04.18 (GSM) or in TS 25.331 (UMTS).

If the AUTHENTICATION REJECT message is received in any other state the mobile station shall abort any MM specific, MM connection establishment or call re-establishment procedure, stop any of the timers T3210 or T3230 (if running), release all MM connections (if any), start timer T3240 and enter the state WAIT FOR NETWORK COMMAND, expecting the release of the RR connection. If the RR connection is not released within a given time controlled by the timer T3240, the mobile station shall abort the RR connection. In both cases, either after a RR connection release triggered from the network side or after a RR connection abort requested by the MS-side, the MS enters state MM IDLE, substate NO IMSI. If the MS has a separate ongoing RR connection to a different core network node, it shall consider this separate connection as still being good.

4.3.2.5a UMTS Authentication not accepted by the network

In the following cases:

– If the MS returns an AUTHENTICATION RESPONSE with an invalid response;

– If the MS returns an AUTHENTICATION FAILURE with an indication of MAC failure, and the MS has been identified by means of the IMSI, or the network decides not to try the identification procedure;

the network sends the MS an AUTHENTICATION REJECT message.

After having sent this message, all MM connections in progress (if any) are released and the network should initiate the RR connection release procedure described in section 3.5.of 04.18 (GSM) or in TS 25.331 (UMTS).

Upon receipt of an AUTHENTICATION REJECT message, the mobile station shall set the update status in the SIM to U2 ROAMING NOT ALLOWED, delete from the SIM the stored TMSI, LAI and ciphering key sequence number. The SIM shall be considered as invalid until switching off or the SIM is removed.

If the AUTHENTICATION REJECT message is received in the state IMSI DETACH INITIATED the mobile station shall follow section 4.3.4.3 of 04.18 (GSM) or in TS 25.331 (UMTS).

If the AUTHENTICATION REJECT message is received in any other state the mobile station shall abort any MM specific, MM connection establishment or call re-establishment procedure, stop any of the timers T3210 or T3230 (if running), release all MM connections (if any), start timer T3240 and enter the state WAIT FOR NETWORK COMMAND, expecting the release of the RR connection. If the RR connection is not released within a given time controlled by the timer T3240, the mobile station shall abort the RR connection. In both cases, either after a RR connection release triggered from the network side or after a RR connection abort requested by the MS-side, the MS enters state MM IDLE, substate NO IMSI. If the MS has a separate ongoing RR connection to a different core network node, it shall consider this separate connection as still being good.

4.3.2.5.1 Authentication not accepted by the MS

In a UMTS authentication challenge, the authentication procedure is extended to allow the MS to check the authenticity of the core network. Thus allowing, for instance, detection of false base station.

A R99 GSM-only MS connected to a R99 core network (even using the GSM radio access) shall support a UMTS authentication challenge.

Following a UMTS authentication challenge, the MS may reject the core network, on the grounds of an incorrect AUTN parameter (see TS 33.102). This parameter contains two possible causes for authentication failure:

a) MAC code failure

> If the MS considers the MAC code (supplied by the core network in the AUTN parameter) to be invalid, it shall send a AUTHENTICATION FAILURE message to the network, with the failure cause ‘MAC failure’ (see TS 33.102).

b) SQN failure

> If the MS considers the SQN (supplied by the core network in the AUTN parameter) to be out of range, it shall send a AUTHENTICATION FAILURE message to the network, with the failure cause ‘Synch failure’ and ~~parameters~~ a re-synchronisation token AUTS provided by the SIM (see TS 33.102)

~~NOTE: Actions might vary according to the presence/absence of an integrity protected connection to a different core network node.~~

4.3.2.6 Abnormal cases

(a) RR connection failure:

> Upon detection of a RR connection failure before the AUTHENTICATION RESPONSE is received, the network shall release all MM connections (if any) and abort any ongoing MM specific procedure.

(b) Expiry of timer T3260:

> The authentication procedure is supervised on the network side by the timer T3260. At expiry of this timer the network may release the RR connection. In this case the network shall abort the authentication procedure and any ongoing MM specific procedure, release all MM connections if any, and initiate the RR connection release procedure described in section 3.5.

```
mobile station                   network
                AUT REQ
          <------------------        Start T3260
                AUT RES
           ------------------>      Stop T3260
                  (a)
                AUT REJ
          < - - - - - - - - - -
                  (b)
```

Figure 4.2/TS 24.008: Authentication sequence: (a) authentication; (b) authentication rejection.

4.3.2.7 Handling of keys at intersystem change from UMTS to GSM

At intersystem change from UMTS to GSM, ciphering may be started (see GSM 04.18) without any new authentication procedure. Deduction of the appropriate security key for ciphering in GSM, depends on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GSM ciphering key according to Table 4.3.2.7.1.

Table 4.3.2.7.1/TS 24.008: Intersystem change from UMTS to GSM

Security context established in MS and network in UMTS	At intersystem change to GSM:
GSM security context	An ME shall apply the GSM cipher key received from the GSM security context residing in the SIM.
UMTS security context	An ME shall apply the GSM cipher key derived by the SIM from the UMTS cipher key and the UMTS integrity key.

NOTE A SIM with UMTS security context, passes the UMTS cipher key, the UMTS integrity key and the derived GSM cipher key to the ME independent on the current radio access being UMTS or GSM (The derivation of a GSM ciphering key is optional).

4.3.2.8 Handling of keys at intersystem change from GSM to UMTS

At intersystem change from ~~UMTS ~~GSM to ~~GSM~~UMTS, ciphering and integrity may be started (see TS 25.331) without any new authentication procedure. Deduction of the appropriate security keys for ciphering and integrity check in UMTS, depend on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the UMTS cipher key and the UMTS integrity key according to Table 4.3.2.8.1.

Table 4.3.2.8.1/TS 24.008: Intersystem change from GSM to UMTS

Security context established in MS and network in GSM	At intersystem change to UMTS:
GSM security context	An ME shall derive the UMTS cipher key and UMTS integrity key from the GSM cipher key provided by the SIM. The conversion functions named “c4” and “c5” in TS 33.102 are used for this purpose.
UMTS security context	An ME shall apply the UMTS ciphering key and the UMTS integrity key received from the UMTS security context residing in the SIM.

NOTE A SIM with UMTS security context, passes the UMTS cipher key, the UMTS integrity key and the derived GSM cipher key to the ME independent on the current radio access being UMTS or GSM (The derivation of a GSM ciphering key is optional).

4.3.2.9 Use of established security contexts

In GSM, in the case of an established GSM security context, the GSM ciphering key shall be taken into use by the ME when any valid CIPHERING MODE COMMAND is received during an RR connection (the definition of a valid CIPHERING MODE COMMAND message is given in GSM 04.18 section 3.4.7.2).

In GSM, in the case of an established UMTS security context, the GSM ciphering key shall be taken into use by the MS when a valid CIPHERING MODE COMMAND is received during an RR connection (the definition of a valid CIPHERING MODE COMMAND message is given in GSM 04.18 section 3.4.7.2). The network shall derive a GSM ciphering key from the UMTS ciphering key and the UMTS integrity key by using the conversion function named “c3” defined in TS 33.102.

In UMTS, in the case of an established GSM security context, the ME shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named “c4” and “c5” defined in TS 33.102. The derived UMTS ciphering key and UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating CS domain is received during an RR connection (the definition of a valid SECURITY MODE COMMAND message is given in TS 25.331). The network shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named “c4” and “c5” defined in TS 33.102.

In UMTS, in the case of an established UMTS security context, the UMTS ciphering key and UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating CS domain is received during a RR connection (the definition of a valid SECURITY MODE COMMAND message is given in TS 25.331).

NOTE: In UMTS and GSM, during an ongoing, already ciphering and/or integrity protected RR connection, the network might initiate a new Authentication procedure in order to establish a new GSM/UMTS security context. The new keys are taken into use in the MS when a new valid SECURITY MODE COMMAND indicating CS domain in UMTS, or a new valid CIPHERING MODE COMMAND in GSM, is received during the RR connection.

9.2.2 Authentication request

This message is sent by the network to the mobile station to initiate authentication of the mobile station identity. See table 9.2.3/TS 24.008.

Message type: AUTHENTICATION REQUEST

Significance: dual

Direction: network to mobile station

Table 9.2.3/TS 24.008: AUTHENTICATION REQUEST message content

IEI	Information element	Type / Reference	Presence	Format	Length
	Mobility management protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	Authentication Request message type	Message type 10.4	M	V	1
	Ciphering key sequence number	Ciphering key sequence number 10.5.1.2	M	V	1/2
	Spare half octet	Spare half octet 10.5.1.8	M	V	1/2
	Authentication parameter RAND (UMTS challenge or GSM challenge)	Auth. parameter RAND 10.5.3.1	M	V	16
20	Authentication Parameter AUTN	Auth. parameter AUTN 10.5.3.1.2	O	T~~L~~V	~~16-20~~17

9.2.2.1 Authentication Parameter AUTN

This IE shall be present if and only if the authentication challenge is a UMTS authentication challenge. The presence or absence of this IE defines- in the case of its absence- a GSM authentication challenge or- in the case of its presence- a UMTS authentication challenge.

9.2.3 Authentication response

This message is sent by the mobile station to the network to deliver a calculated response to the network. See table 9.2.4/TS 24.008.

Message type: AUTHENTICATION RESPONSE

Significance: dual

Direction: mobile station to network

Table 9.2.4/TS 24.008: AUTHENTICATION RESPONSE message content

IEI	Information element	Type / Reference	Presence	Format	Length
	Mobility management protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	Authentication Response message type	Message type 10.4	M	V	1
	Authentication Response parameter	Auth. Response parameter 10.5.3.2	M	V	4
21	Authentication Response Parameter (extension)	Auth. Response parameter 10.5.3.2.1	O	TLV	3-14

9.2.3.1 Authentication Response Parameter

This IE contains the SRES, if it was a GSM authentication challenge, or the RES (all or just the 4 most significant octets of) if it was a UMTS authentication challenge (see also 9.2.3.2).

9.2.3.2 Authentication Response Parameter (extension)

This IE shall be included if and only if the authentication challenge was a UMTS authentication challenge and the RES parameter is greater than 4 octets in length. It shall contain the least significant remaining bits of the RES (the four most significant octets shall be sent in the Authentication Response Parameter IE (see 9.2.3.1))

9.2.3a Authentication Failure

This message is sent by the mobile station to the network to indicate that authentication of the network has failed. See table 9.2.4a/TS 24.008.

Message type: AUTHENTICATION FAILURE

Significance: dual

Direction: mobile station to network

Table 9.2.4a/TS 24.008: AUTHENTICATION FAILURE message content

IEI	Information element	Type / Reference	Presence	Format	Length
	Mobility management Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	Authentication Failure Message type	Message type 10.4	M	V	1
	Reject Cause	Reject Cause 10.5.3.6	M	V	1
22	Authentication Failure parameter	Authentication Failure parameter 10.5.3.2.2	O	T~~L~~V	~~14 - 18~~15

9.2.3a.1 Authentication Failure parameter

This IE shall be sent if and only if the reject cause was 'Synch failure.' It shall include the response to the authentication challenge from the SIM, which is made up of the AUTS parameter (see TS 33.102).

10.5.3.1.2 Authentication Parameter AUTN (UMTS authentication challenge only)

The purpose of the *Authentication Parameter AUTN* information element is to provide the MS with a means of authenticating the network.

The *Authentication Parameter AUTN* information element is coded as shown in figure 10.5.75.1/TS 24.008 and table 10.5.89.1/TS 24.008.

The *Authentication Parameter AUTN* is a type 4 information element with a ~~minimum~~ length of 16 octets. ~~and a maximum of 20 octets length.~~

Figure 10.5.75.1/TS 24.008 *Authentication Parameter AUTN* information element (UMTS authentication challenge only)

8 7 6 5 4 3 2 1	
Authentication Parameter AUTN IEI	octet 1
~~Length of AUTN contents~~	~~octet 2~~
AUTN	Octet ~~3~~2 octet ~~20~~17

Table 10.5.89.1/TS 24.008 *Authentication Parameter AUTN* information element (UMTS authentication challenge only)

```
+-------------------------------------------------------+
• AUTN value (octets ~~3~~ 2 to ~~20~~17)                      •
•                                                       •
• The AUTN consists of (SQN xor AK)||AMF||MAC           •
•                     =~~(32 to 64)~~48+16+64 bits        •
•                      (see TS 33.102)                  •
•                                                       •
+-------------------------------------------------------+
```

10.5.3.2.1 Authentication Response Parameter (extension) (UMTS authentication challenge only)

This IE is included if the authentication response parameter RES is longer than 4 octets (UMTS only) and therefore does not fit in the Authentication Response Parameter field (see 10.5.3.2).

The Authentication Response parameter (extension) IE is coded as shown in figure 10.5.76.1/TS 24.008 and table 10.5.90.1/TS 24.008.

The Authentication Response parameter (extension) IE is a type 4 information element with a minimum length of 3 octets and a maximum length of 14 octets.

Figure 10.5.76.1/TS 24.008 Authentication Response Parameter (extension) information element (UMTS only)

8 7 6 5 4 3 2 1	
Authentication Response (extension) IEI	octet 1
Length of Authentication Response contents	octet 2
RES (all but 4 most significant octets) : :	octet 3 octet 14

Table 10.5.90.1/TS 24.008: *Authentication Response Parameter (extension)* information element (RES)

```
+------------------------------------------------------+
• RES (extension) value (octet 3 to 14)                •
•                                                      •
• This contains all but the 4 most significant octets  •
•  of RES                                              •
•                                                      •
+------------------------------------------------------+
```

10.5.3.2.2 Authentication Failure parameter (UMTS authentication challenge only)

The purpose of the *Authentication Failure parameter* information element is to provide the network with the necessary information to begin a re-authentication procedure (see TS 33.102) in the case of a ‘Synch failure’, following a UMTS authentication challenge.

The Authentication Failure parameter IE is coded as shown in figure 10.5.76.2/TS 24.008 and table 10.5.90.2/TS 24.008.

The Authentication Failure parameter IE is a type 4 information element with a ~~minimum ~~length of 14 octets and~~ a maximum length of 18 octets~~.

Figure 10.5.76.2/TS 24.008 Authentication Failure parameter information element (UMTS authentication challenge only)

8 7 6 5 4 3 2 1	
Authentication Failure parameter IEI	octet 1
~~Length ofAuthentication Failure parameter contents~~	~~octet 2~~
Authentication Failure parameter : :	octet ~~3~~2
	octet ~~18~~15

Table 10.5.90.2/TS 24.008: Authentication Failure parameter information element

•Authentication Failure parameter value (octet ~~3 ~~2 to~~••18~~ 15)
This contains AUTS (see TS 33.102)

4.7.7 Authentication and ciphering procedure

4.7.7a Authentication and ciphering procedure used for UMTS authentication challenge.

The purpose of the authentication and ciphering procedure is fourfold (see TS 33.102):

- to permit the network to check whether the identity provided by the MS is acceptable or not~~, see TS 33.102)~~;
- to provide parameters enabling the MS to calculate a new GPRS UMTS ciphering key and a new GPRS UMTS integrity key.
- to let the network set the GSM ciphering mode (ciphering /no ciphering) and GSM ciphering algorithm; and
- to permit the mobile station to authenticate the network.

In UMTS, and in the case of a UMTS authentication challenge, the authentication and ciphering procedure can be used for authentication only.

The cases in which the authentication and ciphering procedure shall be used are defined in TS 33.102 and GSM 02.09 [5].

The authentication and ciphering procedure is always initiated and controlled by the network. However, in the case of a UMTS authentication challenge, there is the possibility for the MS to reject the network.

UMTS authentication challenge shall be supported by a ME supporting GSM or UMTS radio access.

The authentication and ciphering procedure can be used for either:

- authentication only;
- setting of the GSM ciphering mode and the GSM ciphering algorithm only; or
- authentication and the setting of the GSM ciphering mode and the GSM ciphering algorithm.

~~In GSM, t~~The network should not send any user data during the authentication and ciphering procedure.

A UMTS security context is established in the MS and the network when a UMTS authentication challenge is performed in GSM or in UMTS. After a successful UMTS authentication, the GPRS UMTS ciphering key and~~,~~ the GPRS UMTS integrity key~~, the GPRS GSM ciphering key~~ and the GPRS ciphering key sequence number~~,~~ are stored both in the network and the MS. In addition, the MS may store a GPRS GSM ciphering key, if the SIM supports GSM. The network may derive the GPRS GSM ciphering key from the GPRS UMTS ciphering/integrity keys when it is needed or at any time before and also store it.

4.7.7b Authentication and ciphering procedure used for GSM authentication challenge

The purpose of the authentication and ciphering procedure is threefold (see GSM 03.20):

- to permit the network to check whether the identity provided by the MS is acceptable or not~~, see GSM 03.20 [13])~~;
- to provide parameters enabling the MS to calculate a new GPRS GSM ciphering key; and
- to let the network set the GSM ciphering mode (ciphering/no ciphering) and GSM ciphering algorithm.

The authentication and ciphering procedure can be used for either:

- authentication only;
- setting of the GSM ciphering mode and the GSM ciphering algorithm only; or
- authentication and the setting of the GSM ciphering mode and the GSM ciphering algorithm.

The cases in which the authentication and ciphering procedure shall be used are defined in GSM 02.09 [5].

~~In GSM, t~~The authentication and ciphering procedure is always initiated and controlled by the network. It shall be performed in a non ciphered mode because of the following reasons:

- the network cannot decipher a ciphered AUTHENTICATION AND CIPHERING RESPONSE from an unauthorised MS and put it on the black list; and
- to be able to define a specific point in time from which on a new GPRS GSM ciphering key should be used instead of the old one.

GSM authentication challenge shall be supported by a ME supporting GSM or UMTS radio access.

~~In GSM, t~~The network should not send any user data during the authentication and ciphering procedure.

A GSM security context is established in the MS and the network when a GSM authentication challenge is performed in GSM or in UMTS. After a successful GSM authentication challenge, the GPRS GSM ciphering key and the GPRS ciphering key sequence number, are stored both in the network and the MS.

4.7.7.1 Authentication and ciphering initiation by the network

The network initiates the authentication and ciphering procedure by transferring an AUTHENTICATION AND CIPHERING REQUEST message across the radio interface and starts timer T3360. The AUTHENTICATION AND CIPHERING REQUEST message shall contain all parameters necessary to calculate the response parameters when authentication is performed (see GSM 03.20 [13] and TS 33.102).

If authentication is requested, then the AUTHENTICATION AND CIPHERING REQUEST message shall contain either:

- ~~—~~In a GSM authentication challenge, the GPRS ciphering key sequence number, allocated to the GPRS GSM ciphering key and the RAND~~, or~~. The network shall mark the used GSM authentication challenge as "used". GSM authentication challenges should not be re-used; they may be re-used under the strict conditions described in GSM 02.09.
- In a UMTS authentication challenge, the GPRS ciphering key sequence number, allocated to the GPRS UMTS ciphering and GPRS UMTS integrity keys, the RAND and the AUTN. The network shall retain the used RAND and AUTN for re-synchronisation and retransmission when the timer T3360 expires. Apart of these retrans-missions, UMTS authentication challenges shall not be re-used by the network.

In GSM, if authentication is not requested, then the AUTHENTICATION AND CIPHERING REQUEST message shall not contain neither the GPRS ciphering key sequence number, the RAND nor the AUTN.

In GSM, if ciphering is requested, in a GSM authentication challenge or in a UMTS authentication challenge, then the AUTHENTICATION AND CIPHERING REQUEST message shall indicate the GPRS GSM ciphering algorithm.

The network includes the A&C reference number information element in the AUTHENTICATION AND CIPHERING REQUEST message. Its value is chosen in order to link an AUTHENTICATION AND CIPHERING REQUEST in a RA with its RESPONSE. The A&C reference number value might be based on the RA Colour Code value.

Additionally, the network may request the MS to include its IMEISV in the AUTHENTICATION AND CIPHERING RESPONSE message.

4.7.7.2 Authentication and ciphering response by the MS

In GSM, a MS that is attached to GPRS shall be ready to respond upon an AUTHENTICATION AND CIPHERING REQUEST message at any time.

In UMTS, an MS that is attached to GPRS shall be ready to respond upon an AUTHENTICATION AND CIPHERING REQUEST message at any time whilst a PS signalling connection exists.

In a GSM authentication challenge, if the AUTHENTICATION AND CIPHERING REQUEST message includes the authentication parameters RAND and GPRS CKSN, then upon receipt of the message, the MS processes the challenge information and sends an AUTHENTICATION AND CIPHERING RESPONSE message to the network. The value of the received A&C reference number information element shall be copied into the A&C reference number information element in the AUTHENTICATION AND CIPHERING RESPONSE message. A GSM authentication challenge will result in the SIM passing a SRES and a GPRS GSM ciphering key to the ME. The new GPRS GSM ciphering key calculated from the challenge information shall overwrite the previous one and any previously stored GPRS UMTS ciphering and GPRS UMTS integrity keys shall be deleted. The calculated GSM ciphering key shall be stored on the SIM together with the GPRS ciphering key sequence number before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted.

In a UMTS authentication challenge, if the AUTHENTICATION AND CIPHERING REQUEST message includes the UMTS authentication parameters GPRS CKSN, RAND and AUTN, then upon receipt of the message, the MS verifies the AUTN parameter and if this is accepted, the MS processes the challenge information and sends an AUTHENTICATION AND CIPHERING RESPONSE message to the network. The value of the received A&C reference number information element shall be copied into the A&C reference number information element in the AUTHENTICATION AND CIPHERING RESPONSE message. A UMTS authentication challenge will result in the SIM passing a RES, a GPRS UMTS ciphering key, a GPRS UMTS integrity key ~~and a GPRS GSM ciphering key~~ to the ME. In addition, a UMTS authentication challenge may result in the SIM passing a GSM ciphering key to the ME. The new GPRS UMTS ciphering key, GPRS UMTS integrity key and GPRS GSM ciphering key calculated from the challenge information shall overwrite the previous ones. The new GPRS UMTS ciphering key, GPRS UMTS integrity key and GPRS GSM ciphering key shall be stored on the SIM together with the GPRS ciphering key sequence number before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted.

In UMTS, an MS capable of UMTS only shall ignore the Ciphering Algorithm IE in the AUTHENTICATION AND CIPHERING REQUEST message. An MS capable of both UMTS and GSM shall store the received value in the Ciphering Algorithm IE in the AUTHENTICATION AND CIPHERING REQUEST message in order to be used at an inter system change from UMTS to GSM.

If the AUTHENTICATION AND CIPHERING REQUEST message does not include neither the GSM authentication parameters (RAND and GPRS CKSN) nor the UMTS authentication parameters RAND, AUTN and GPRS CKSN), then upon receipt of the message, the MS replies by sending an AUTHENTICATION AND CIPHERING RESPONSE message to the network.

In GSM, the GMM layer shall notify the LLC layer if ciphering shall be used or not and if yes which GSM ciphering algorithm and GPRS GSM ciphering key that shall be used (see GSM 04.64 [76]).

4.7.7.3 Authentication and ciphering completion by the network

Upon receipt of the AUTHENTICATION AND CIPHERING RESPONSE message, the network stops the timer T3360 and checks the validity of the response (see GSM 03.20 [13] and TS 33.102). For this, it may use the A&C reference number information element within the AUTHENTICATION AND CIPHERING RESPONSE message to determine whether the response is correlating to the last request that was sent. If authentication failes, i.e., if the response is not valid, see 4.7.7.5 (GSM authentication challenge) or 4.7.7.5a (UMTS authentication challenge).

In GSM, the GMM layer shall notify the LLC sublayer if ciphering shall be used or not and if yes which algorithm and GPRS GSM ciphering key that shall be used (see GSM 04.64 [76]).

Upon receipt of the AUTHENTICATION AND CIPHERING FAILURE message, the network stops the timer T3360.

In MAC failure case, ~~the procedural behaviour is ffs.~~ the network considers whether the MS has used the P-TMSI or the IMSI for identification.

If the P-TMSI has been used, the network may decide to initiate the identification procedure. If the IMSI given by the MS differs from the one the network had associated with the P-TMSI, the authentication should be restarted with the correct parameters. If the IMSI provided by the MS is the expected one (i.e. authentication has really failed), the network should proceed as described in 4.7.7.5a.

In Synch failure case, the ~~core~~ network shall send the user's HLR/AuC a request for new quintets, include an indication of synchronisation failure, and include the random challenge RAND and the re-synchronisation token AUTS. The procedures at the radio side are ffs. ~~may renegotiate with the HLR/AuC and provide the MS with new authentication parameters.~~

4.7.7.4 GPRS ciphering key sequence number

The security parameters for authentication and ciphering are tied together in sets. In a GSM authentication challenge, from a challenge parameter RAND both the authentication response parameter SRES and the GPRS GSM ciphering key can be computed given the secret key associated to the IMSI. In a UMTS authentication challenge, from a challenge parameter RAND, the authentication response parameter RES and the GPRS UMTS ciphering key and the GPRS UMTS integrity key can be computed given the secret key associated to the IMSI. In addition, a GPRS GSM ciphering key can be computed from the UMTS ciphering key and UMTS integrity key by means of an unkeyed conversion function. The computation of a GPRS GSM ciphering key is optional.

In order to allow start of ciphering on a logical link without authentication, GPRS ciphering key sequence numbers are introduced.

The GPRS ciphering key sequence number is managed by the network such that the AUTHENTICATION AND CIPHERING REQUEST message contains the GPRS ciphering key sequence number allocated to the GPRS GSM ciphering key (in case of a GSM authentication challenge) or the GPRS UMTS ciphering key and the GPRS UMTS integrity key (in case of a UMTS authentication challenge) which may be computed from the RAND parameter carried in that message.

The ~~MS~~ ME and the SIM store~~s~~ the GPRS ciphering key sequence number with the GPRS GSM ciphering key (in case of a GSM authentication challenge) and the GPRS UMTS ciphering key and the GPRS UMTS integrity key (in case of a UMTS authentication challenge), and includes the corresponding GPRS ciphering key sequence number in the ROUTING AREA UPDATE REQUEST , SERVICE REQUEST and ATTACH REQUEST messages.

If the GPRS ciphering key sequence number is deleted, the associated GPRS GSM ciphering key, GPRS UMTS ciphering key and GPRS UMTS integrity key shall be deleted (i.e. the established GSM security context or the UMTS security context is no longer valid).

In UMTS, the network may choose to start ciphering and integrity checking with the stored GPRS UMTS ciphering key and the stored GPRS UMTS integrity key (under the restrictions given in GSM 02.09 and TS 33.102) if the stored GPRS ciphering key sequence number and the one given from the MS are equal.

In GSM, the network may choose to start ciphering with the stored GPRS GSM ciphering key (under the restrictions given in GSM 02.09) if the stored GPRS ciphering key sequence number and the one given from the MS are equal and the previously negotiated ciphering algorithm is known and supported in the network. When ciphering is requested at GPRS attach, the authentication and ciphering procedure shall be performed since the MS does not store the ciphering algorithm at detach.

Upon GPRS attach, if ciphering is to be used, an AUTHENTICATION AND CIPHERING REQUEST message shall be sent to the MS to start ciphering.

If the GPRS ciphering key sequence number stored in the network does not match the GPRS ciphering key sequence number received from the MS in the ATTACH REQUEST message, then the network should authenticate the MS.

In GSM, the MS starts ciphering after sending the AUTHENTICATION AND CIPHERING RESPONSE message. The network starts ciphering when a valid AUTHENTICATION AND CIPHERING RESPONSE is received from the MS.

In UMTS, the MS starts ciphering and integrity checking according to the conditions specified in specification TS 25.331.

In GSM, as an option, the network may decide to continue ciphering without sending an AUTHENTICATION AND CIPHERING REQUEST message after receiving a ROUTING AREA UPDATE REQUEST message with a valid GPRS ciphering key sequence number. Both the MS and the network shall use the latest ciphering parameters. The network starts ciphering when sending the ciphered ROUTING AREA UPDATE ACCEPT message to the MS. The MS starts ciphering after receiving a valid ciphered ROUTING AREA UPDATE ACCEPT message from the network.

NOTE: In some specifications the term KSI (Key Set Identifier) is used instead of the term GPRS ciphering key sequence number.

4.7.7.5 GSM Authentication not accepted by the network

If authentication and ciphering fails, i.e. if the response is not valid, the network considers whether the MS has used the P-TMSI or the IMSI for identification.

- If the P-TMSI has been used, the network may decide to initiate the identification procedure. If the IMSI given by the MS differs from the one the network had associated with the P-TMSI, the authentication should be restarted with the correct parameters. If the IMSI provided by the MS is the expected one (i.e. authentication has really failed), the network should proceed as described below.
- If the IMSI has been used, or the network decides not to try the identification procedure, an AUTHENTICATION AND CIPHERING REJECT message should be transferred to the MS.

Upon receipt of an AUTHENTICATION AND CIPHERING REJECT message, the MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED and shall delete the P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number stored. If available, also the TMSI, LAI and ciphering key sequence number shall be deleted and the update status shall be set to U3 ROAMING NOT ALLOWED. The SIM shall be considered as invalid until switching off or the SIM is removed.

If the AUTHENTICATION AND CIPHERING REJECT message is received, the MS shall abort any GMM procedure, shall stop the timers T3310 and T3330 (if running) and shall enter state GMM-DEREGISTERED.

4.7.7.5 UMTS Authentication not accepted by the network

In the followign cases:

- If the MS returns an AUTHENTICATION AND CIPHERING RESPONSE with an invalid response;
- If the MS returns an AUTHENTICATION AND CIPHERING FAILURE with an indication of MAC failure and the MS has been identified by means of the IMSI or the network decides not to try the identification procedure;

the network sends the MS an AUTHENTICATION AND CIPHERING REJECT message.

Upon receipt of an AUTHENTICATION AND CIPHERING REJECT message, the MS shall set the GPRS update status to GU3 ROAMING NOT ALLOWED and shall delete the P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number stored. If available, also the TMSI, LAI and ciphering key sequence number shall be deleted and the update status shall be set to U3 ROAMING NOT ALLOWED. The SIM shall be considered as invalid until switching off or the SIM is removed.

If the AUTHENTICATION AND CIPHERING REJECT message is received, the MS shall abort any GMM procedure, shall stop the timers T3310 and T3330 (if running) and shall enter state GMM-DEREGISTERED.

4.7.7.5.1 Authentication not accepted by the MS

In a UMTS authentication challenge, the authentication procedure is extended to allow the MS to check the authenticity of the core network. Thus allowing, for instance, detection of false base station.

Following a UMTS authentication challenge, the MS may reject the core network, on the grounds of an incorrect AUTN parameter (see TS 33.102). This parameter contains two possible causes for authentication failure:

a) MAC code failure

If the MS considers the MAC code (supplied by the core network in the AUTN parameter) to be invalid, it shall send a AUTHENTICATION AND CIPHERING FAILURE message to the network, with the failure cause 'MAC failure'~~ and parameters provided by the SIM (see TS 33.102)~~.

b) SQN failure

If the MS considers the SQN (supplied by the core network in the AUTN parameter) to be out of range, it shall send a AUTHENTICATION AND CIPHERING FAILURE message to the network, with the failure cause 'Synch failure' and ~~parameters~~ the re-synchronisation token AUTS provided by the SIM (see TS 33.102).

~~Note: Actions might vary according to the presence/absence of an integrity protected connection to a different core network node.~~

4.7.7.6 Abnormal cases on the network side

The following abnormal cases can be identified:

a) Lower layer failure

Upon detection of a lower layer failure before the AUTHENTICATION AND CIPHERING RESPONSE is received, the network shall abort the procedure.

b) Expiry of timer T3360

The network shall, on the first expiry of the timer T3360, ~~retransmit the AUTHENTICATION AND CIPHERING REQUEST and shall reset and start timer T3360. This retransmission is repeated four times, i.e. on the fifth expiry of timer T3360,~~ the procedure shall be aborted and the used UMTS authentication challenges shall be deleted~~.~~

c) Collision of an authentication and ciphering procedure with a GPRS attach procedure

If the network receives an ATTACH REQUEST message before the ongoing authentication procedure has been completed and no GPRS attach procedure is pending on the network (i.e. no ATTACH ACCEPT/REJECT message has to be sent as an answer to an ATTACH REQUEST message), the network shall abort the authentication and ciphering procedure and proceed with the new GPRS attach procedure.

d) Collision of an authentication and ciphering procedure with a GPRS attach procedure when the authentication and ciphering procedure has been caused by a previous GPRS attach procedure

If the network receives an ATTACH REQUEST message before the ongoing authentication procedure has been completed and a GPRS attach procedure is pending (i.e. an ATTACH ACCEPT/REJECT message has still to be sent as an answer to an earlier ATTACH REQUEST message), then:

- If one or more of the information elements in the ATTACH REQUEST message differs from the ones received within the previous ATTACH REQUEST message, the network shall not treat the authentication any further and proceed with the GPRS attach procedure ; or
- If the information elements do not differ, then the network shall not treat any further this new ATTACH REQUEST.

Collision of an authentication and ciphering procedure with a GPRS detach procedure

GPRS detach containing cause "power off":

If the network receives a DETACH REQUEST message before the ongoing authentication and ciphering procedure has been completed, the network shall abort the authentication and ciphering procedure and shall progress the GPRS detach procedure.

GPRS detach containing other causes than "power off":

If the network receives a DETACH REQUEST message before the ongoing authentication and ciphering procedure has been completed, the network shall complete the authentication and ciphering procedure and shall respond to the GPRS detach procedure as described in section 4.7.4.

e) Collision of an authentication and ciphering procedure with a routing area updating procedure

If the network receives a ROUTING AREA UPDATE REQUEST message before the ongoing authentication procedure has been completed, the network shall progress both procedures.

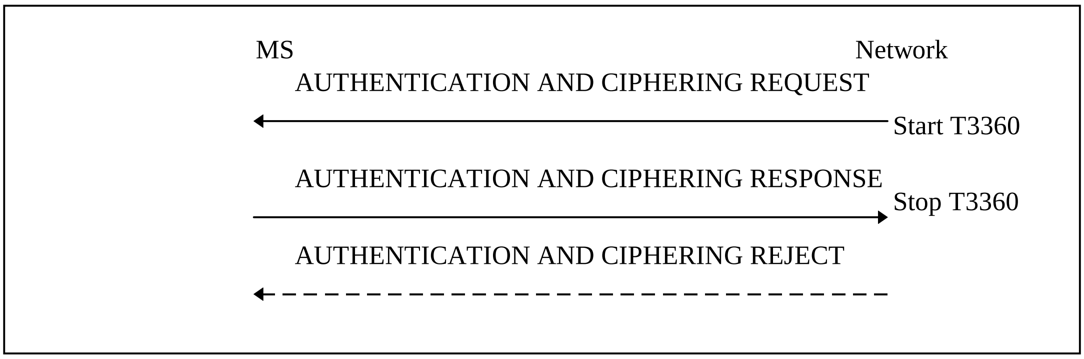
MS
Network
AUTHENTICATION AND CIPHERING REQUEST
Start T3360
AUTHENTICATION AND CIPHERING RESPONSE
Stop T3360
AUTHENTICATION AND CIPHERING REJECT

Figure 4.7.7/1 TS 24.008: Authentication and ciphering procedure

4.7.7.7 Use of established security contexts

In GSM, in the case of an established GSM security context, the GPRS GSM ciphering key shall be taken into use by the MS before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted.

In GSM, in the case of an established UMTS security context, the GPRS GSM ciphering key shall be taken into use by the MS before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted. The network shall derive a GPRS GSM ciphering key from the GPRS UMTS ciphering key and the GPRS UMTS integrity key, by using the conversion function named "c3" defined in TS 33.102.

In UMTS, in the case of an established GSM security context, the ME shall derive a GPRS UMTS ciphering key and a GPRS UMTS integrity key from the GPRS GSM ciphering key by using the conversion functions named "c4" and "c5" defined in TS 33.102. The derived GPRS UMTS ciphering key and GPRS UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating PS domain is received during an RR connection (the definition of a valid SECURITY MODE COMMAND message is given in TS 25.331). The network shall derive a GPRS UMTS ciphering key and a GPRS UMTS integrity key from the GPRS GSM ciphering key by using the conversion functions named "c4" and "c5" defined in TS 33.102.

In UMTS, in the case of an established UMTS security context, the GPRS UMTS ciphering key and the GPRS UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating PS domain is received during an PS signalling connection (the definition of a valid SECURITY MODE COMMAND message is given in TS 25.331).

NOTE: In UMTS, during an ongoing, already ciphering/integrity protected PS signalling connection, the network might initiate a new Authentication and ciphering procedure in order to establish a new GSM/UMTS security context. The new GPRS UMTS ciphering key and GPRS UMTS integrity key are taken into use by the MS, when a new valid SECURITY MODE COMMAND indicating PS domain is received during the PS signalling connection.

4.7.7.8 Handling of keys at intersystem change from UMTS to GSM

At an intersystem change from UMTS to GSM, ciphering may be started (see GSM 04.64 [76]) without any new authentication and ciphering procedure. Deduction of the appropriate security key for ciphering in GSM, depends on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GPRS GSM ciphering key according to Table 4.7.7.8.1.

Before any initial GMM message is sent in the new cell in GSM, the GMM layer in the MS shall notify the LLC layer if ciphering shall be used or not. If yes, the GPRS GSM ciphering key and the applicable ciphering algorithm according to the stored *Ciphering Algorithm IE* in the MS shall also be indicated to the LLC layer (see GSM 04.64 [76]).

Table 4.7.7.8.1/TS 24.008: Intersystem change from UMTS to GSM

Security context established in MS and network in UMTS	At intersystem change to GSM:
GSM security context	An ME shall apply the GPRS GSM cipher key received from the GSM security context residing in the SIM.
UMTS security context	An ME shall apply the GPRS GSM cipher key derived by the SIM from the GPRS UMTS cipher key and the GPRS UMTS integrity key.

NOTE A SIM with UMTS security context, passes the GPRS UMTS ciphering key, the GPRS UMTS integrity key and the derived GPRS GSM ciphering key to the ME independent on the current radio access being UMTS or GSM. (The derivation of a GSM ciphering key is optional.)

4.7.7.9 Handling of keys at intersystem change from GSM to UMTS

At an intersystem change from GSM to UMTS, ciphering and integrity may be started (see TS 25.331) without any new authentication and ciphering procedure. Deduction of the appropriate security keys for ciphering and integrity check in UMTS, depend on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GPRS UMTS cipher key and the GPRS UMTS integrity key according to Table 4.7.7.9.1.

Table 4.7.7.9.1/TS 24.008: Intersystem change from GSM to UMTS

Security context established in MS and network in GSM	At intersystem change to UMTS:
GSM security context	An ME shall derive the GPRS UMTS cipher key and GPRS UMTS integrity key from the GPRS GSM cipher key provided by the SIM. The conversion functions named “c4” and “c5” in TS 33.102 are used for this purpose.
UMTS security context	An ME shall apply the GPRS UMTS ciphering key and the GPRS UMTS integrity key received from the UMTS security context residing in the SIM.

NOTE A SIM with UMTS security context, passes the GPRS UMTS ciphering key, the GPRS UMTS integrity key and the derived GPRS GSM ciphering key to the ME independent on the current radio access being UMTS or GSM. (The derivation of a GSM ciphering key is optional.)

9.4.9 Authentication and ciphering request

This message is sent by the network to the MS to initiate authentication of the MS identity. Additionally, the ciphering mode is set, indicating whether ciphering will be performed or not. See table 9.4.9/GSM 24.008.

Message type: AUTHENTICATION AND CIPHERING REQUEST

Significance: dual

Direction: network to MS

Table 9.4.9/GSM 24.008: AUTHENTICATION AND CIPHERING REQUEST message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip indicator	Skip indicator 10.3.1	M	V	1/2
	Authentication and ciphering request message identity	Message type 10.4	M	V	1
	Ciphering algorithm	Ciphering algorithm 10.5.5.3	M	V	1/2
	IMEISV request	IMEISV request 10.5.5.10	M	V	1/2
	Force to standby	Force to standby 10.5.5.7	M	V	1/2
	A&C reference number	A&C reference number 10.5.5.19	M	V	1/2
21	Authentication parameter RAND	Authentication parameter RAND 10.5.3.1	O	TV	17
8	GPRS ciphering key sequence number	Ciphering key sequence number 10.5.1.2	C	TV	1
28	Authentication parameter AUTN	Authentication parameter AUTN 10.5.3.1.2	O	T~~L~~V	~~16-20~~17

9.4.10 Authentication and ciphering response

This message is sent by the MS to the network in response to an *Authentication and ciphering request* message. See table 9.4.10/TS 24.008.

Message type: AUTHENTICATION AND CIPHERING RESPONSE

Significance: dual

Direction: MS to network

Table 9.4.10/TS 24.008: AUTHENTICATION AND CIPHERING RESPONSE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip indicator	Skip indicator 10.3.1	M	V	1/2
	Authentication and ciphering response message identity	GPRS message type 10.4	M	V	1
	A&C reference number	A&C reference number 10.5.5.19	M	V	1/2
	Spare half octet	Spare half octet 10.5.1.8	M	V	1/2
22	Authentication parameter Response	Authentication Response parameter 10.5.3.2	O	TV	5
23	IMEISV	Mobile identity 10.5.1.4	O	TLV	11
29	Authentication Response parameter (extension)	Authentication Response parameter 10.5.3.2.1	O	TLV	3-14

9.4.10a Authentication and Ciphering Failure

This message is sent by the mobile station to the network to indicate that authentication of the network has failed. See table 9.4.10a/TS 24.008.

Message type: AUTHENTICATION AND CIPHERING FAILURE

Significance: dual

Direction: mobile station to network

Table 9.4.10a/TS 24.008: AUTHENTICATION AND CIPHERING FAILURE message content

IEI	Information element	Type / Reference	Presence	Format	Length
	Mobility management Protocol discriminator	Protocol discriminator 10.2	M	V	1/2
	Skip Indicator	Skip Indicator 10.3.1	M	V	1/2
	Authentication and Ciphering Failure Message type	Message type 10.4	M	V	1
	GMM Cause	GMM Cause 10.5.5.14	M	V	1
30	Authentication Failure parameter	Authentication Failure parameter 10.5.3.2.2	O	T~~L~~V	~~14 – 18~~15

9.4.10a.1 Authentication Failure parameter

This IE shall be sent if and only if the GMM cause was ‘Synch failure.’ It shall include the response to the authentication challenge from the SIM, which is made up of the AUTS parameter (see TS 33.102).