3GPP TSG SA WG3 Security ó S3#36 **S3-0401075**
Shenzhen, China, 23th ñ 26th October 2004

CR-Form-v7.1

CHANGE REQUEST

⌘ **43.020** **CR** **003** ⌘ **rev** **2** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: | UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Clarifying the support of algorithms within mobile stations
Source:	⌘	SA WG3
Work item code:	⌘	SECGKYV
Date:	⌘	17/11/2004
Category:	⌘	**C**
Release:	⌘	*Rel-6*

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Since the publication of the Barkan-Biham-Keller attack, the A5/2 algorithm is not considered safe anymore. Therefore it should not be supported in Rel-6 mobile stations. It is also considered appropriate to mandate A5/3 support in Rel-6 mobile stations and to mandate GEA2 and GEA3 support. The mandatory support of other algorithms that are currently implemented in mobile stations is made more explicit. It is also specified that other undefined A5 or GEA algorithms should not be supported since these could open up opportunities for attack.
Summary of change:	⌘	Clarify the support of A5 and GEA algorithms within mobile stations.
Consequences if not approved:	⌘	Attacks which exploit A5/2 weaknesses will persist for Rel-6 UEs. Opportunities are missed to take advantage of new algorithms implemented in networks.

Clauses affected:	⌘	New clause 4.9, new clause D.4.9

		Y	N		
Other specs affected:	⌘		×	Other core specifications	⌘
			×	Test specifications	
			×	O&M Specifications	

Other comments:	⌘	The intention is to phase out A5/2 within GSM networks by the end of 2005.

*** Begin of change ****

4 Confidentiality of signalling information elements, connectionless data and user information elements on physical connections

4.1 Generality

In GSM 02.09, some signalling information elements are considered sensitive and must be protected.

To ensure identity confidentiality (see clause 2), the Temporary Subscriber Identity must be transferred in a protected mode at allocation time and at other times when the signalling procedures permit it.

The confidentiality of connection less user data requires at least the protection of the message part pertaining to OSI layers 4 and above.

The user information confidentiality of user information on physical connections concerns the information transmitted on a traffic channel on the MS-BSS interface (e.g. for speech). It is not an end-to-end confidentiality service.

These needs for a protected mode of transmission are fulfilled with the same mechanism where the confidentiality function is a OSI layer 1 function. The scheme described below assumes that the main part of the signalling information elements is transmitted on DCCH (Dedicated Control Channel), and that the CCCH (Common Control Channel) is only used for the allocation of a DCCH.

Four points have to be specified:

- the ciphering method;
- the key setting;
- the starting of the enciphering and deciphering processes;
- the synchronization.

4.2 The ciphering method

The layer 1 data flow (transmitted on DCCH or TCH) is ciphered by a bit per bit or stream cipher, i.e. the data flow on the radio path is obtained by the bit per bit binary addition of the user data flow and a ciphering bit stream, generated by algorithm A5 using a key determined as specified in subclause 4.3. The key is denoted below by Kc, and is called "Ciphering Key".

For multislot configurations (e.g. HSCSD) different ciphering bit streams are used on the different timeslots. On timeslot "n" a ciphering bit stream, generated by algorithm A5, using a key Kcn is used. Kcn is derived from Kc as follows:

> Let BN denote a binary encoding onto 64 bits of the timeslot number "n" (range 0-7). Bit "i" of Kcn, Kcn(i), is then calculated as Kc(i) xor (BN<<32(i)) ("xor" indicates: "bit per bit binary addition" and "<<32" indicates: "32 bit circular shift"), the number convention being such that the lsb of Kc is xored with the lsb of the shifted BN.

Deciphering is performed by exactly the same method.

Algorithm A5 is specified in annex C.

4.3 Key setting

Mutual key setting is the procedure that allows the mobile station and the network to agree on the key Kc to use in the ciphering and deciphering algorithms A5.

A key setting is triggered by the authentication procedure. Key setting may be initiated by the network as often as the network operator wishes.

Key setting must occur on a DCCH not yet encrypted and as soon as the identity of the mobile subscriber (i.e. TMSI or IMSI) is known by the network.

The transmission of Kc to the MS is indirect and uses the authentication RAND value; Kc is derived from RAND by using algorithm A8 and the Subscriber Authentication key Ki, as defined in annex C.

As a consequence, the procedures for the management of Kc are the authentication procedures described in subclause 3.3.

The values Kc are computed together with the SRES values. The security related information (see subclause 3.3.1) consists of RAND, SRES and Kc.

The key Kc is stored by the mobile station until it is updated at the next authentication.

Key setting is schematized in figure 4.1.

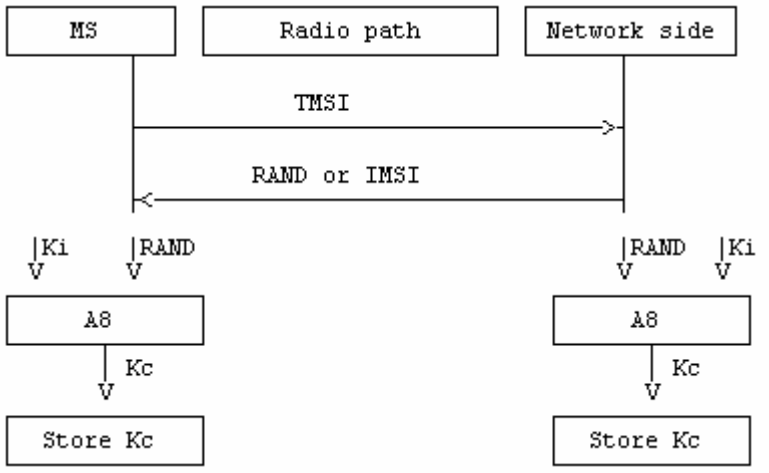

Figure 4.1: Key setting

4.4 Ciphering key sequence number

The ciphering key sequence number is a number which is associated with the ciphering key Kc and they are stored together in the mobile station and in the network.

However since it is not directly involved in any security mechanism, it is not addressed in this specification but in GSM 04.08 instead.

4.5 Starting of the ciphering and deciphering processes

The MS and the BSS must co-ordinate the instants at which the enciphering and deciphering processes start on DCCH and TCH.

On DCCH, this procedure takes place under the control of the network some time after the completion of the authentication procedure (if any), or after the key Kc has been made available at the BSS.

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

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

The starting of enciphering and deciphering processes is schematized in figure 4.2.

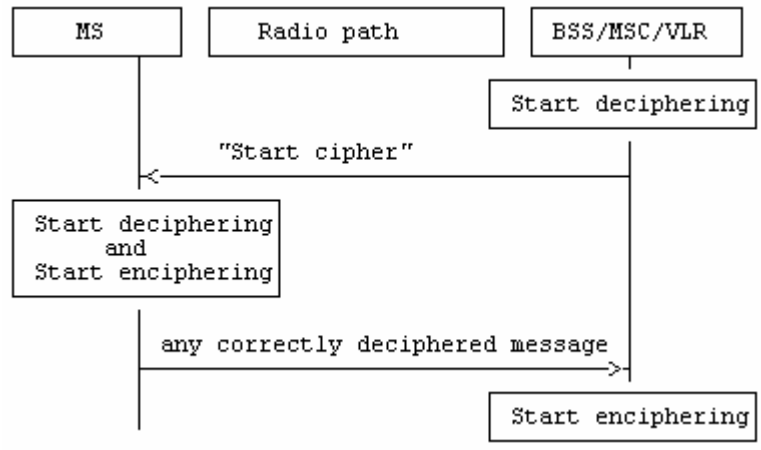

Figure 4.2: Starting of the enciphering and deciphering processes

When a TCH is allocated for user data transmission, the key used is the one set during the preceding DCCH session (Call Set-up). The enciphering and deciphering processes start immediately.

4.6 Synchronization

The enciphering stream at one end and the deciphering stream at the other end must be synchronized, for the enciphering bit stream and the deciphering bit streams to coincide. The underlying Synchronization scheme is described in annex C.

4.7 Handover

When a handover occurs, the necessary information (e.g. key Kc, initialization data) is transmitted within the system infrastructure to enable the communication to proceed from the old BSS to the new one, and the Synchronization procedure is resumed. The key Kc remains unchanged at handover.

4.8 Negotiation of A5 algorithm

Not more then 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 of the seven versions of the A5 algorithm it supports. The network shall not provide service to an MS which indicates that it does not support the ciphering algorithm(s) required by GSM 02.07.

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

1) If the MS and the network have no versions of the A5 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 A5 algorithm in common, then the network shall select one of the mutually acceptable versions of the A5 algorithm for use on that connection.

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

4.9 Support of A5 Algorithms in MS

It is mandatory for A5/1, A5/3 and non encrypted mode (i.e.A5/0) to be implemented in mobile stations. It is prohibited to implement A5/2 in mobile stations. No other A5 algorithms shall be supported in mobile stations.

*** End of change ****

*** Next change ****

D.4 Confidentiality of user information and signalling between MS and SGSN

D.4.1 Generality

In GSM 02.09, some signalling information elements are considered sensitive and must be protected.

To ensure identity confidentiality (see clause 2), the new TLLI must be transferred in a protected mode at allocation time.

The confidentiality of user information concerns the information transmitted on the logical connection between MS and SGSN.

These needs for a protected mode of transmission are fulfilled by a ciphering function in the LLC layer. It is not an end-to-end confidentiality service.

Four points have to be specified:

- the ciphering method;
- the key setting;
- the starting of the enciphering and deciphering processes;
- the synchronisation.

D.4.2 The ciphering method

The LLC layer information flow is ciphered by the algorithm GPRS-A5 as described in GSM 01.61.

D.4.3 Key setting

Mutual key setting is the procedure that allows the mobile station and the network to agree on the key GPRS-Kc to use in the ciphering and deciphering algorithms GPRS-A5. This procedure corresponds to the procedure described in subclause 4.3 besides the different confidential subscriber identity. The GPRS-Kc is handled by the SGSN independently from the MSC. If a MS is using both circuit switched and packet switched, two different ciphering keys will be used independently, one (Kc) in the MSC and one (GPRS-Kc) in the SGSN.

A key setting is triggered by the authentication procedure. Key setting may be initiated by the network as often as the network operator wishes. If an authentication procedure is performed during a data transfer, the new ciphering parameters shall be taken in use immediately at the end of the authentication procedure in both SGSN and MS.

Key setting may not be encrypted and shall be performed as soon as the identity of the mobile subscriber (i.e. TLLI or IMSI) is known by the network.

The transmission of GPRS-Kc to the MS is indirect and uses the authentication RAND value; GPRS-Kc is derived from RAND by using algorithm A8 and the Subscriber Authentication key Ki, in the same way as defined in annex C for Kc.

As a consequence, the procedures for the management of GPRS-Kc are the authentication procedures described in subclause D.3.3.

The values GPRS-Kc are computed together with the SRES values. The security related information (see subclause D.3.3.1) consists of RAND, SRES and GPRS-Kc.

The key GPRS-Kc is stored by the mobile station until it is updated at the next authentication.

Key setting is schematised in figure D.4.1.

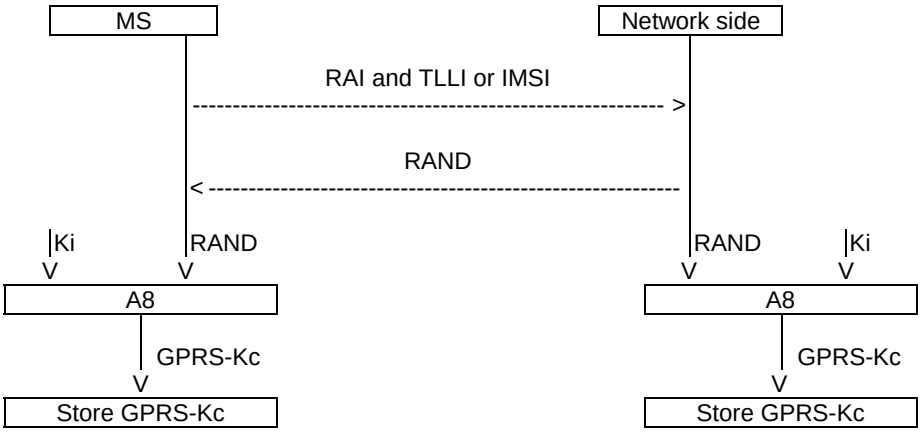

Figure D.4.1: Key setting

D.4.4 Ciphering key sequence number

The GPRS-CKSN (Ciphering Key Sequence Number) is a number which is associated with each ciphering key GPRS-Kc. The GPRS-CKSN and GPRS-Kc are stored together in the mobile station and in the network. It permits the consistency check of the keys stored in the MS and in the network. Two independent pairs, Kc and CKSN (for circuit switched), and GPRS-Kc and GPRS-CKSN (for packet switched) may be stored in the MS simultaneously.

However since it is not directly involved in any security mechanism, it is not addressed in this specification but in GSM 04.08 instead.

D.4.5 Starting of the ciphering and deciphering processes

The MS and the SGSN must co-ordinate the instants at which the ciphering and deciphering processes start. The authentication procedure governs the start of ciphering. The SGSN indicates if ciphering shall be used or not in the Authentication and Ciphering Request message. If ciphering is used, the MS starts ciphering after sending the Authentication and Ciphering Response message. The SGSN starts ciphering when a valid Authentication and Ciphering Response message is received from the MS.

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-CKSN stored in the network does not match the GPRS-CKSN received from the MS in the Attach Request message, then the network should authenticate the MS.

As an option, the network may decide to continue ciphering without authentication after receiving a Routing Area Update Request message with a valid GPRS-CKSN. Both the MS and the network shall use the latest ciphering parameters. The MS starts ciphering after a receiving a valid ciphered Routing Area Update Accept message from the network. The SGSN starts ciphering when sending the ciphered Routing Area Update Accept message to the MS.

Upon delivery of the Authentication and Ciphering Response message or the Routing Area Update Accept message, the GPRS Mobility and Management entity in both SGSN and MS shall be aware if ciphering has started or not. LLC provides the capability to send both ciphered and unciphered PDUs. The synchronisation of ciphering at LLC frames level is done by a bit in the LLC header indicating if the frame is ciphered or not. Only a few identified signalling messages (e.g., Routing Area Update Request message) described in GSM 04.08 may be sent unciphered, any other frames sent unciphered shall be deleted. Once the encryption has been started, neither the MS nor the network shall go to an unciphered session.

D.4.6 Synchronisation

The enciphering stream at one end and the deciphering stream at the other end must be synchronised, for the enciphering bit stream and the deciphering bit streams to coincide. Synchronisation is guaranteed by driving Algorithm GPRS-A5 by an explicit variable INPUT per established LLC and direction.

These initial INPUT values shall not be identical for the different LLC link. The initial INPUT value shall be determined by the network. It may be identical for uplink and downlink value because the direction is given to the ciphering algorithm as described in GSM 01.61 and illustrated on the figure D.4.2. In a given direction, the INPUT value shall be unique for each frame.

The calculation of the INPUT value is described in GSM. The use of the INPUT value is described in GSM 01.61 and illustrated on the figure D.4.2.

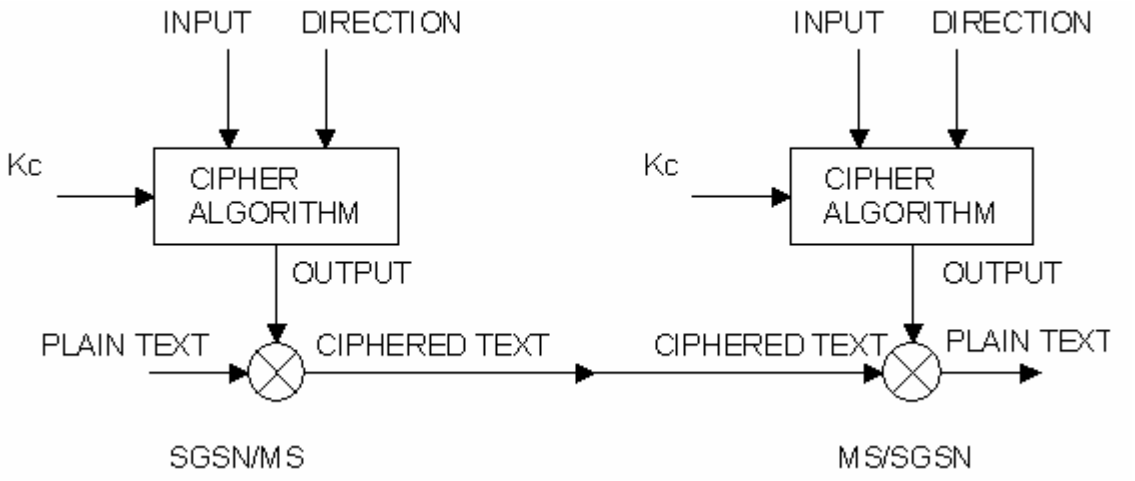

Figure D.4.2: Use of the INPUT parameter

D.4.7 Inter SGSN routing area update

When an Inter SGSN routing area update occurs, the necessary information (e.g. key Kc, INPUT parameters) is transmitted within the system infrastructure to enable the communication to proceed from the old SGSN to the new one, and the Synchronisation procedure is resumed. The key Kc may remains unchanged at Inter SGSN routing area update.

D.4.8 Negotiation of GPRS-A5 algorithm

Not more than seven versions of the GPRS-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) 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) ~~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.

D.4.9 Support of GPRS-A5 Algorithms in MS

It is mandatory for GEA1, GEA2, GEA3 and non encrypted mode (i.e. GEA0) to be implemented in mobile stations. No other GPRS encryption algorithms shall be supported in mobile stations.