3GPP TSG SA WG3 Security — S3#10 **S3-000042**
19-21 January, 2000
Antwerpen, Belgium

CHANGE REQUEST No : *Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.*

Technical Specification GSM / UMTS: 03.20 Version: 7.1.0

Submitted to SMG #32 ? *list SMG plenary meeting no. here ↑* for approval **X** for information ; without presentation ("non-strategic") ; with presentation ("strategic") **X**

PT SMG CR cover form. Filename: crf26_3.doc

Proposed change affects: *(at least one should be marked with an X)* SIM ; ME **X** Network **X**

Work item: GPRS

Source: SMG10 **Date:**

Subject: GPRS encryption

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

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

Release:

Phase 2	
Release 96	
Release 97	
Release 98	**X**
Release 99	**X**
UMTS	

Reason for change: The current recommendation does not reflect clearly enough the fact that the encryption of all transaction is mandatory for GPRS

Clauses affected: Annex D – Section 4

Other specs Affected:

Other releases of same spec	→ List of CRs:	04.08
Other core specifications	→ List of CRs:	
MS test specifications / TBRs	→ 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.

Annex D (normative): Security related network functions for General Packet Radio Service

This annex is only applicable if GPRS is supported.

D.1 General

This annex gives an overview of the different security related services and functions for General Packet Radio Service (GPRS) which is described in GSM 02.60 and GSM 03.60. They are grouped as follows:

- Subscriber identity confidentiality;
- Subscriber identity authentication;
- Confidentiality of user information and signalling between MS and SGSN;
- Security of the GPRS backbone.

It shall be possible to introduce new authentication and ciphering algorithms during the systems lifetime. The fixed part of the network may support more than one authentication and ciphering algorithm.

The security procedures include mechanisms to enable recovery in the event of signalling failures. These recovery procedures are designed to minimise the risk of a breach in the security of the system.

In this annex, the terms GPRS-Kc and GPRS-CKSN are introduced to provide a clear distinction from the ciphering parameters (Kc and CKSN) used for circuit switched. The GPRS-Kc is the ciphering key used for GPRS, and GPRS-CKSN is the corresponding Ciphering Key Sequence Number used for GPRS. The use of these parameters is described in clause D.4.

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. All the MS-SGSN signalling or user information exchanges must be systematically ciphered, except for a few messages listed in GSM 04.08 (e.g., Routing Area Update Request) which may be sent unciphered.

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.

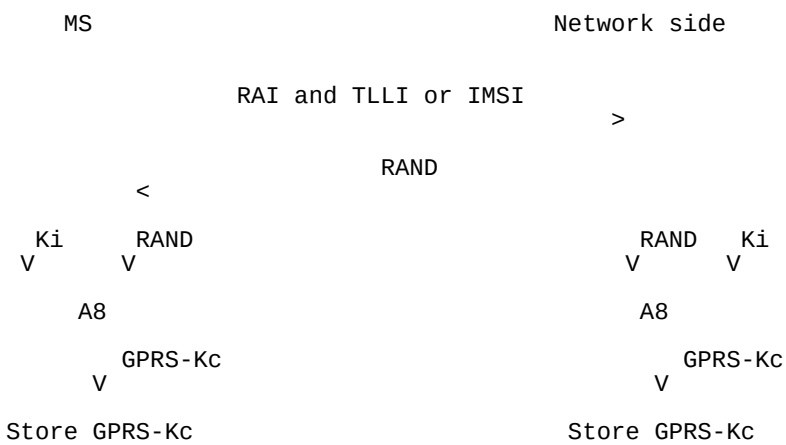

Figure D.4.1: Key setting

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~~ which GPRS encryption algorithm shall be used in the Authentication and Ciphering Request message. ~~If ciphering is used,~~ ~~t~~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.

When receiving a Routing Area Update Request with a valid GPRS-CKSN number, the network shall also immediately start encryption, using either the above described combined authentication and start of encryption method, or the following alternative method, which does not require sending any Authentication and Ciphering Request message to start encryption : ~~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~~ 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 frame containing another type of signalling message or traffic data shall be systematically encryted, both at the MS and SGSN sides. Independent encryption control processes at the MS side and at the SGSN side must ensure that no other frame is sent or received unencrypted~~,~~ If any other frame~~s sent~~ is received unciphered by the MS or the SGSN, the receiving party shall ~~be~~ delete~~d~~ it and immediately release the connection. 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.

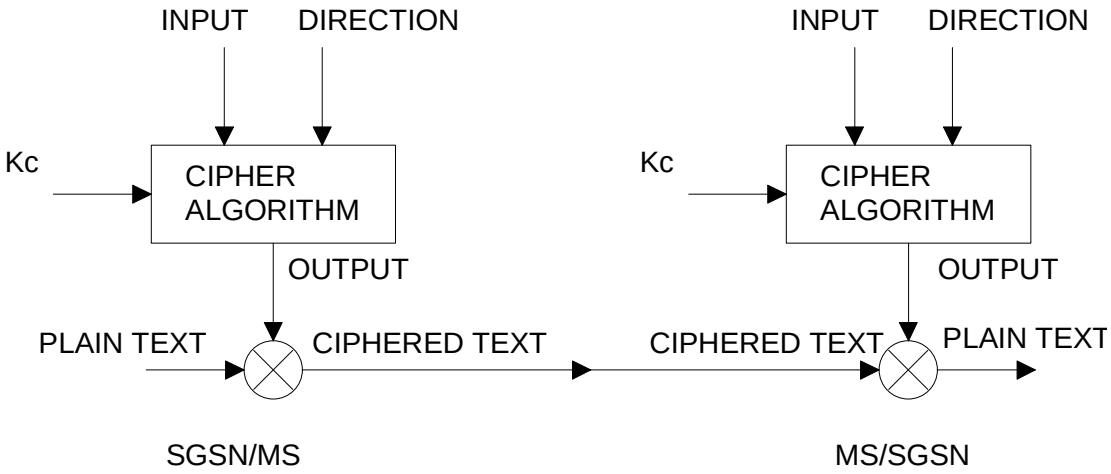

Figure D.4.2: Use of the INPUT parameter

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

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.

D.5 Synthetic summary

Figure D.5.1 shows in a synopsis a routing area updating procedure with all elements pertaining to security functions, i.e. to TLLI management, authentication and GPRS-Kc management.

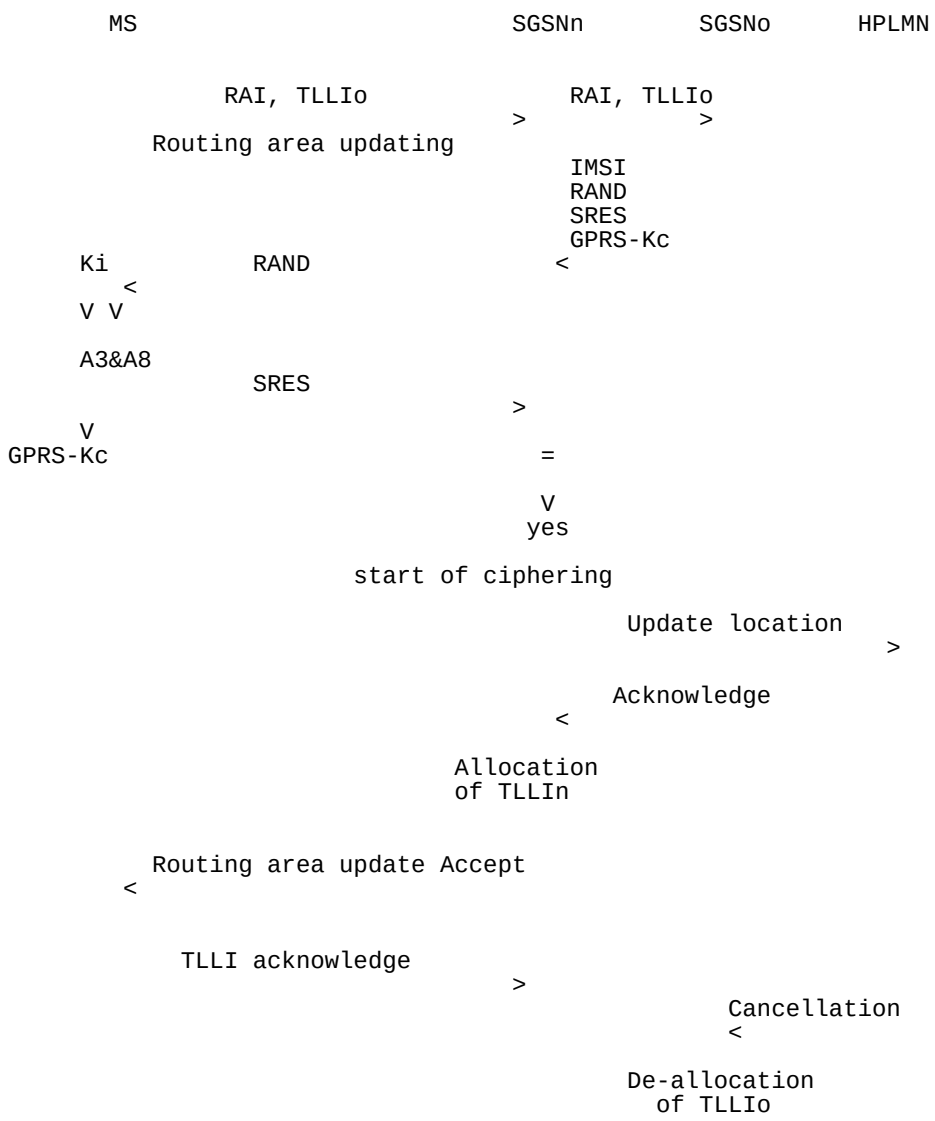

Figure D.5.1: Routing area updating procedure

D.6 Security of the GPRS backbone

The operator is responsible for the security of its own Intra-PLMN backbone which includes all network elements and physical connections. The operator shall prevent unauthorised access to its Intra-PLMN backbone. A secure Intra-PLMN backbone guarantees that no intruder can eavesdrop or modify user information and signalling in the Intra-PLMN backbone.

The GPRS architecture utilises GPRS tunnelling and private IP addressing within the backbone to restrict unauthorised access to the backbone. User traffic addressed to a network element shall be discarded. Firewall functionality may provide these means at the access points (Gi reference point and Gp interface) of the Intra-PLMN backbone.

The Inter-PLMN links shall be negotiated between operators as part of the roaming agreement. They shall ensure that the Inter-PLMN links are secure providing integrity and confidentiality. For example, secure links can be achieved by point to point links, private Inter-PLMN backbones or encrypted tunnels over the public Internet.

Operators shall be able to determine the origin of packets coming from the inter-PLMN backbone. One example is to use a Frame Relay PVC between two operators.

C.1 Specifications for Algorithm A5

C.1.1 Purpose

As defined in GSM 03.20, Algorithm A5 realizes the protection of both user data and signalling information elements at the physical layer on the dedicated channels (TCH or DCCH).

Synchronization of both the enciphering and deciphering (especially at hand-over) must be guarantied.

C.1.2 Implementation indications

Algorithm A5 is implemented into both the MS and the BSS. On the BSS side description below assumes that one algorithm A5 is implemented for each physical channel (TCH or DCCH).

The ciphering takes place before modulation and after interleaving (see GSM 05.01); the deciphering takes place after demodulation symmetrically. Both enciphering and deciphering need Algorithm A5 and start at different times (see clause 4).

As an indication, recall that, due to the TDMA techniques used in the system, the useful data (also called the plain text in the sequel) are organized into blocks of 114 bits. Then, each block is incorporated into a normal burst (see GSM 05.02) and transmitted during a time slot. According to GSM 05.03, the useful information bits into a block are numbered e0 to e56 and e59 to e115 (the flag bits e57 and e58 are ignored). Successive slots for a given physical channel are separated at least by a frame duration, approximately 4.615 ms (see GSM 05.01).

In the case of EDGE (Enhanced Data rate for GSM Evolution) the useful data are organized into longer blocks than 114 bits. According to GSM 05.03 the useful information in a block is included in 116 symbols which are numbered E(0) to E(115). Each symbol contains 3 bits, hence a block contains 348 useful information bits. See C.1.5 for changes in A5 due to use of EDGE.

For ciphering, Algorithm A5 produces, each 4.615 ms, a sequence of 114 encipher/decipher bits (here called BLOCK) which is combined by a bit-wise modulo 2 addition with the 114-bit plain text block. The first encipher/decipher bit produced by A5 is added to e0, the second to e1 and so on. As an indication, the resulting 114-bit block is then applied to the burst builder (see GSM 05.01).

For each slot, deciphering is performed on the MS side with the first block (BLOCK1) of 114 bits produced by A5, and enciphering is performed with the second block (BLOCK2). As a consequence, on the network side BLOCK1 is used for enciphering and BLOCK2 for deciphering. Therefore Algorithm A5 must produce two blocks of 114 bits (i.e. BLOCK1 and BLOCK2) each 4.615 ms.

Synchronization is guarantied by driving Algorithm A5 by an explicit time variable, COUNT, derived from the TDMA frame number. Therefore each 114-bit block produced by A5 depends only on the TDMA frame numbering and the ciphering key Kc.

COUNT is expressed in 22 bits as the concatenation of the binary representation of T1, T3 and T2. It is an input parameter of Algorithm A5. The coding of COUNT is shown in figure C.1.

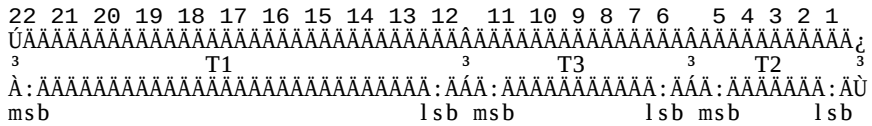

Figure C.1: The coding of COUNT

Binary representation of COUNT. Bit 22 is the most significant bit (msb) and bit 1 the least significant bit (lsb) of COUNT. T1, T3 and T2 are represented in binary. (For definition of T1, T3 and T2, see GSM 05.02).

Figure C.2 summarizes the implementation indications listed above, with only one enciphering/deciphering procedure represented (the second one for deciphering/enciphering is symmetrical).

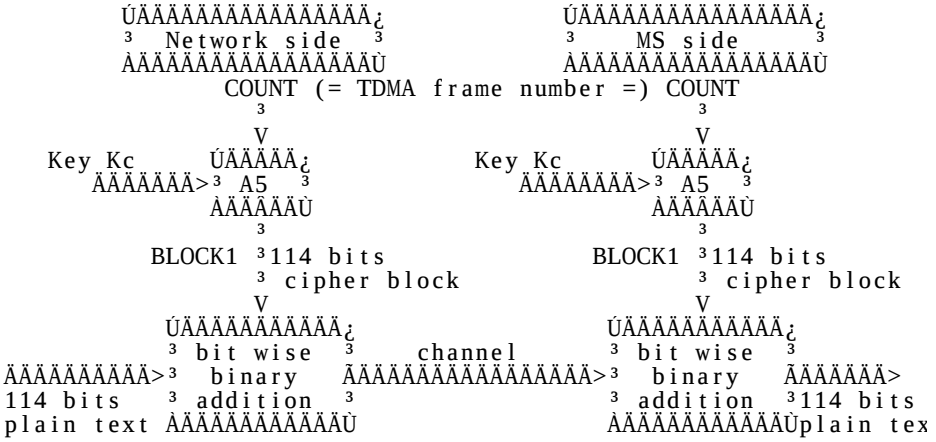

Figure C.2: Deciphering on the MS side

C.1.3 External specifications of Algorithm A5

The two input parameters (COUNT and Kc) and the output parameters (BLOCK1 and BLOCK2) of Algorithm A5 shall use the following formats:

- length of Kc: 64 bits;
- length of COUNT: 22 bits;
- length of BLOCK1: 114 bits;
- length of BLOCK2: 114 bits.

Algorithm A5 shall produce BLOCK1 and BLOCK2 in less than a TDMA frame duration, i.e. 4.615 ms.

NOTE: If the actual length of the ciphering key is less than 64 bits, then it is assumed that the actual ciphering key corresponds to the most significant bits of Kc, and that the remaining a~~n~~d less significant bits are set to zero. It must be clear that for signalling and testing purposes the ciphering key Kc is considered to be 64 unstructured bits.

C.1.4 Internal specification of Algorithm A5

The internal specification of Algorithm A5 is managed under the responsibility of GSM/MoU; it will be made available to in response to an appropriate request.

C.1.5 A modification of A5 for EDGE

In EDGE the block size is greater than 114 bits. With EDGE a modification of A5 algorithm is used which produces BLOCK 1 and BLOCK2 which each contain 348 bits. The other parameters are not modified anyhow. The modified algorithm produces both blocks during a TDMA frame duration, i.e. 4.615 ms. The blocks are combined by bitwise modulo 2 addition with the plaintext data as explained in C.1.2.

It is possible in EDGE that the plaintext data block for either uplink or downlink is shorter than 348 bits. In this case only the first part of the corresponding output parameter BLOCK is used in the bit-wise adition and the rest of the bits are discarded.

The necessary modifications are reflected in the internal specifications of Algorithm A5.