3GPP TSG SA WG3 Security — S3#12 **S3-000219**

11-14 April, 2000

Stockholm, Sweden

Source: **CN WG1/SMG3**
Title: **Reply to LS on "Introduction of rejection of non ciphered calls for GPRS"**
Document for: **Discussion**
Agenda Item:

3GPP TSG-CN-WG1, Meeting #11 *Tdoc N1-000539*
28. February - 03.March. 2000
Umea, Sweden

To: TSG-S3/SMG10

cc: TSG-T2, SMG9

Source: TSG-N1/SMG3

Title: Reply to LS on "Introduction of rejection of non ciphered calls for GPRS"

Contact: Roland Gruber, Siemens AG
E-mail: roland.gruber@mch.siemens.de
phone: +49 89 722 46392

N1 thanks S3 for their LS on "Introduction of rejection of non ciphered calls for GPRS" (S3-00 0206). N1 has discussed the topic and came to the conclusion, that S3 is asking for the introduction of a complex new feature that requires work to be done by several TSG working groups, which should be covered by a separate new work item. N1 assumes that S3 would be the best group to initiate and control the work item.

As the R99 and all older releases are already functionally frozen N1 do not see a possibility that, at least for the needed changes to the specifications under its responsibility, caused by this requirement can be completed for R97, 98 or 99.

N1 see that changes to the specifications under its responsibility will be needed if a new R00 work item is approved.

N1 has also discussed the attached CR (S3-000058/ N1-000287) for 04.08/ R98/ GPRS with the result that this CR is rejected by N1.

ETSI SMG10
Helsinki
7-9th December, 1999

Tdoc S3-000058

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: 04.08 Version: 7.2.0

Submitted to SMG #30 *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: Sections 4.7.1 and 4.7.7

Other specs affected:

Other releases of same spec	→ List of CRs:	
Other core specifications	→ List of CRs:	03.20
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.

4.7 Elementary mobility management procedures for GPRS services

4.7.1 General

This section describes the basic functions offered by the mobility management (GMM) sublayer at the radio interface (reference point U_m). The functionality is described in terms of timers and procedures. During GMM procedures, session management procedures, see chapter 6, are suspended.

4.7.1.1 Lower layer failure

The LLC sublayer shall indicate a logical link failure or an RR sublayer failure to the GMM sublayer. The failure indicates an error that cannot be corrected by the lower layers.

4.7.1.2 Ciphering of messages

The GMM sublayer provides a systematic encryption of all the user traffic and of all signalling messages ~~If ciphering is to be applied on a GMM context, all GMM messages shall be ciphered~~ except the following messages, which may be transmitted unciphered :

-- ATTACH REQUEST;

-- ATTACH REJECT;

-- AUTHENTICATION AND CIPHERING REQUEST;

-- AUTHENTICATION AND CIPHERING RESPONSE;

-- AUTHENTICATION AND CIPHERING REJECT;

-- IDENTITY REQUEST;

-- IDENTITY RESPONSE;

-- ROUTING AREA UPDATE REQUEST; and

-- ROUTING AREA UPDATE REJECT.

4.7.1.3 P-TMSI signature

The network may assign a P-TMSI signature to an MS in an attach, routing area update, or P-TMSI reallocation procedure. Only in combination with a valid P-TMSI, this P-TMSI signature is used by the MS for authentication and identification purposes in the subsequent attach or routing area update procedure. If the MS has no valid P-TMSI it shall not use the P-TMSI signature in the subsequent attach or routing area update procedure. Upon successful completion of the subsequent attach or routing area update procedure the used P-TMSI signature shall be deleted.

4.7.1.4 Radio resource sublayer address handling

While a packet TMSI (P-TMSI) is used in the GMM sublayer for identification of an MS, a temporary logical link identity (TLLI) is used for addressing purposes at the RR sublayer. This section describes how the RR addressing is managed by GMM. For the detailed coding of the different TLLI types and how a TLLI can be derived from a P-TMSI, see GSM 03.03 [10].

Two cases can be distinguished:

- a valid P-TMSI is available in the MS; or

- no valid P-TMSI is available in the MS

NOTE: For anonymous access, the RR address assignment is handled by the SM sublayer as described in section 6.1.1.1.

i) valid P-TMSI available

If the MS has stored a valid P-TMSI, the MS shall derive a foreign TLLI from that P-TMSI and shall use it for transmission of the:

- ATTACH REQUEST message of any GPRS combined/non-combined attach procedure; and
- ROUTING AREA UPDATE REQUEST message of a combined/non-combined RAU procedure if the MS has entered a new routing area, or if the GPRS update status is not equal to GU1 UPDATED.

Any other GMM message is transmitted using a local TLLI derived from the stored P-TMSI. This includes a ROUTING AREA UPDATE REQUEST message that is sent within a periodic routing area update procedure.

ii) no valid P-TMSI available

When the MS has not stored a valid P-TMSI, i.e. the MS is not attached to GPRS, the MS shall use a randomly selected random TLLI for transmission of the:

- ATTACH REQUEST message of any combined/non-combined GPRS attach procedure.

The same randomly selected random TLLI value shall be used for all message retransmission attempts and for the cell updates within one attach attempt.

Upon receipt of an ATTACH REQUEST message, the network assigns a P-TMSI to the MS, derives a local TLLI from the assigned P-TMSI, and transmits the assigned P-TMSI to the MS.

Upon receipt of the assigned P-TMSI, the MS shall derive the local TLLI from this P-TMSI and shall use it for addressing at lower layers.

In both cases, the MS shall acknowledge the reception of the assigned P-TMSI to the network. After receipt of the acknowledgement, the network shall use the local TLLI for addressing at lower layers.

4.7.1.5 P-TMSI handling

If a new P-TMSI is assigned by the network the MS and the network shall handle the old and the new P-TMSI as follows:

Upon receipt of a GMM message containing a new P-TMSI the MS shall consider the new P-TMSI and new RAI and also the old P-TMSI and old RAI as valid in order to react to paging requests and downlink transmission of LLC frames. For uplink transmission of LLC frames the new P-TMSI shall be used.

The MS shall consider the old P-TMSI and old RAI as invalid as soon as an LLC frame is received with the local TLLI derived from the new P-TMSI.

Upon the transmission of a GMM message containing a new P-TMSI the network shall consider the new P-TMSI and new RAI and also the old P-TMSI and old RAI as valid in order to be able to receive LLC frames from the MS.

The network shall consider the old P-TMSI and old RAI as invalid as soon as an LLC frame is received with the local TLLI derived from the new P-TMSI.

4.7.1.6 Change of network mode of operation

Whenever an MS moves to a new RA, the procedures executed by the MS depend on the network mode of operation in the old and new routing area.

In case the MS is in state GMM-REGISTERED or GMM-ROUTING-AREA-UPDATING-INITIATED and is in operation mode:

a) A or B (with the exceptions in b and c below), the MS shall execute:

Table 4.7.1.6.1/GSM 04.08: Mode A or B

Network operation mode change	Procedure to execute
I → II or I → III	Normal Location Update(*), followed by a Normal Routing Area Update
II → III or III → II	Normal Location Update (see section 4.2.2), followed by a Normal Routing Area Update
II → I or III → I	Combined Routing Area Update with IMSI attach

b) B which reverts to operation mode C in network operation mode III, the MS shall execute:

Table 4.7.1.6.2/GSM 04.08: Mode B which reverts into mode C in network operation mode III

Network operation mode change	Procedure to execute
I → II	Normal Location Update(*), followed by a Normal Routing Area Update
I → III or II → III	IMSI Detach (see section 4.3.4), followed by a Normal Routing Area Update
II → I or III → I	Combined Routing Area Update with IMSI attach
III → II	IMSI attach (see section 4.4.3), followed by a Normal Routing Area Update

c) B which reverts to IMSI attached for CS services only in network operation mode III, the MS shall execute:

Table 4.7.1.6.3/GSM 04.08: Mode B which reverts into IMSI attached for CS services only in network operation mode III

Network operation mode change	Procedure to execute
I → II	Normal Location Update(*), followed by a Normal Routing Area Update
I → III	Normal Location Update(*), followed by a GPRS Detach with type indicating “GPRS Detach”
II → III	Normal Location Update (see section 4.2.2), followed by a GPRS Detach with detach type indicating “GPRS Detach”
II → I	Combined Routing Area Update with IMSI attach
III → I	Combined GPRS Attach
III → II	Normal Location Update (see section 4.2.2), followed by a Normal GPRS Attach

(*) Intended to remove the Gs association in the MSC/VLR.

Further details are implementation issues.

4.7.7 Authentication and ciphering procedure

The purpose of the authentication and ciphering procedure is threefold:

- 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 ciphering key; and
- to let the network start ciphering and set the ciphering ~~mode (ciphering/no ciphering) and~~ algorithm.

The authentication and ciphering procedure can be used for either:

~~— authentication only;~~

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

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

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 ciphering key should be used instead of the old one.

The network should not send any user data during the authentication and ciphering procedure.

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]).

If authentication is requested, then the AUTHENTICATION AND CIPHERING REQUEST message shall contain the GPRS ciphering key sequence number, allocated to the GPRS ciphering key and the RAND. If authentication is not requested, then the AUTHENTICATION AND CIPHERING REQUEST message shall contain neither the GPRS ciphering key sequence number nor the RAND.

~~If ciphering is requested, then t~~The AUTHENTICATION AND CIPHERING REQUEST message shall indicate the GPRS 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

An MS that is attached to GPRS shall be ready to respond upon an AUTHENTICATION AND CIPHERING REQUEST message at any time. 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.The new GPRS ciphering key calculated from the challenge information shall overwrite the previous one. It shall be stored and shall be loaded into the ME before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted. The GPRS ciphering key sequence number shall be stored together with the calculated key.

If the AUTHENTICATION AND CIPHERING REQUEST message does not include the authentication parameters RAND and GPRS CKSN, then upon receipt of the message, the MS replies by sending an AUTHENTICATION AND CIPHERING RESPONSE message to the network.

The GMM layer shall notify the LLC ~~layer if ciphering shall be used or not and if yes~~ which algorithm and GPRS 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]). 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.

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

4.7.7.4 GPRS ciphering key sequence number

The security parameters for authentication and ciphering are tied together in sets, i.e. from a challenge parameter RAND both the authentication response SRES and the GPRS ciphering key can be computed given the secret key associated to the IMSI.

In order to allow start of ciphering on a logical link without authentication, GPRS ciphering key sequence numbers are introduced. The sequence number is managed by the network such that the AUTHENTICATION AND CIPHERING REQUEST message contains the sequence number allocated to the key which may be computed from the RAND parameter carried in that message.

The MS stores this number with the key, and includes the corresponding sequence number in the ROUTING AREA UPDATE REQUEST and ATTACH REQUEST messages. If the sequence number is deleted, the associated key shall be considered as invalid.

The network may choose to start ciphering with the stored key (under the restrictions given in GSM 02.09) if the stored 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.

The MS starts ciphering after sending the AUTHENTICATION AND CIPHERING RESPONSE message. The SGSN starts ciphering when a valid AUTHENTICATION AND CIPHERING RESPONSE is received from the MS.

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 SGSN 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.

4.7.7.5 Unsuccessful authentication and ciphering

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, 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.

4.7.7.6 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.

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.

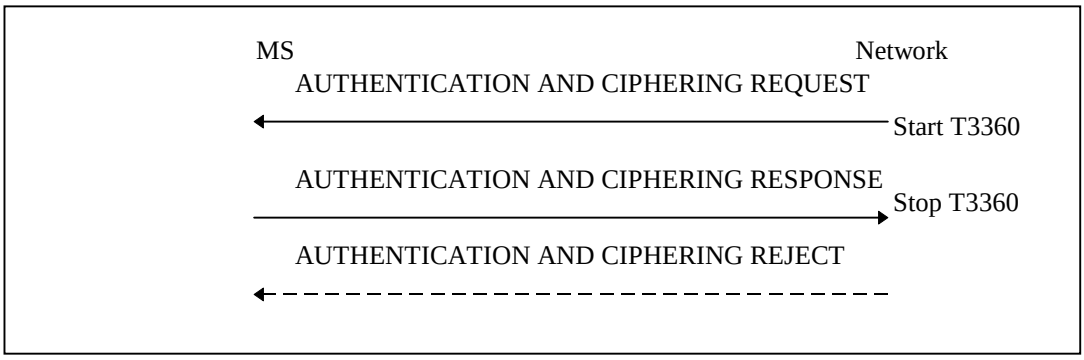

Figure 4.7.7/1 GSM 04.08: Authentication and ciphering procedure