3GPP TSG GERAN Meeting   **TSG 000769**
Norrtälje, Sweden 6-10 November 2000

Source: **3GPP TSG GERAN**

To: **3GPP TSG SA WG3**

CC: **3GPP TSG SA2, 3GPP TSG GERAN**

Title: **Liaison Statement to SA WG3 regarding ciphering of RRLP messages between the SMLC and MS in GPRS**

Contact: **3GPP TSG GERAN**

Margaret Livingston (LCS Rapporteur)   **Veijo Vänttinen**
Nokia   **Nokia Research Center**
+1 972 894 5740   **+ 358 40 703 8140**
margaret.livingston@nokia.com   **veijo.vanttinen@nokia.com**

Support for Location Services in GPRS will be in 3GPP, Release 4 standards. The plan is to use RRLP protocol for communication between SMLC and MS in Circuit Switched (CS) and Packet Switched (PS) mode. In CS mode, ciphering is based on the conventional means (GSM CS ciphering); no LCS specific ciphering is needed for point to point messages. In GPRS this is different, the scope of ciphering is between the MS and SGSN for packet data and layer 3 signaling. This creates a problem: RRLP messages in GPRS can not be ciphered by traditional means because the SMLC is a radio network element and the SGSN is not involved in communication between the SMLC and MS.

The GERAN LCS ad-hoc meeting has noticed the problem and two possible approaches to solve this ciphering issue were considered.
1) Employ an instance of LLC layer in SMLC to accomplish ciphering of RRLP messages, using the same ciphering algorithm as in GPRS with either the same or different ciphering key. This proposal is described in Annex A, (copy of tdoc GAHL-000009).
2) Enhance GPRS RLC/MAC protocol to include ciphering of RRLP messages. This enhancement should be in line with the emerging ciphering mechanism in GERAN real time protocols.

This liaison statement is sent to SA WG3 for ciphering experts to consider the problem and express their view on it. TSG GERAN LCS group would like SA WG3 to consider if these two possible approaches are appropriate from a security point of view. In addition, for option 1, we would like to hear opinions from SA WG3 experts which ciphering key to use to cipher messages: the same ciphering key (Kc) used in GPRS, or a separate key (Kc_{SGSN}). .

With Kind Regards,

3GPP TSG GERAN

SOURCE: NOKIA

TITLE: CIPHERING WHITE PAPER

Problem Description

Security services is an essential feature in GSM and UMTS. The use of radio resources for communication between the MS and the access network is particularly important but also sensitive for security attacks. Hence, it is necessary to have mechanisms against:

1)   Misuse of resources by unauthorized persons,
2)   Eavesdropping on the information being exchanged on the radio path.

As a means to protect the system against the former includes, MS authentication and access control. The means to protect the system against eavesdropping are related to **user information confidentiality**. The purpose of this property is to provide for confidentiality of user data including layer 3 signaling messages. This property is accomplished by ciphering. The scope of ciphering is different in GSM Circuit Switched (CS), UMTS and 2G GPRS domains. This is illustrated in Figure 1.
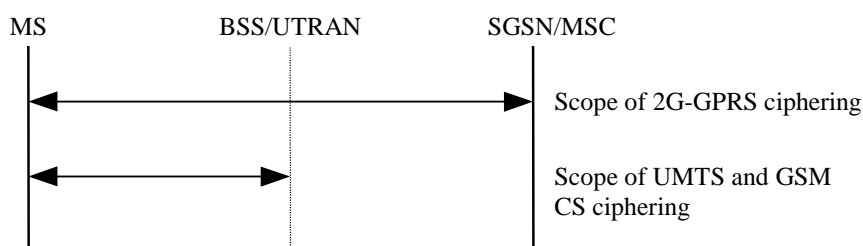

Figure 1 Scope of ciphering

When introducing LoCation Services in GPRS creates a problem for ciphering. Currently, ciphering is accomplished by SGSN and MS, the result is that the LCS specific layer 3 signalling messages in the radio network can not be ciphered by traditional means. In particular, sensitive information within RRLP protocol needs to be ciphered when such information is sent between MS and SMLC in PS mode. The goal in standardization is to support LCS on existing GPRS protocols in LCS release 4 specifications. This contribution considers this problem and proposes a ciphering concept for point-to-point communication in LCS GPRS radio protocols.

General Security Requirements

The following generic requirements should be taken into account when defining a solution for ciphering LCS messages:

- LCS ciphering mechanism should be in line with those in GSM and UMTS
- Security should be at least as good as in current GSM
- Ciphering should be standardized with minimum amount of changes to the 3GPP specifications
- Ciphering should be implementable to the system with minimum amount of impacts

Proposal for Solution

The proposal for ciphering of MS – SMLC communication is based on the following assumptions:

- RRLP protocol is used in GPRS for communication between MS and SMLC.
- An instance of LLC layer is positioned in SMLC directly below the RRLP and ciphering is accomplished by LLC layer.
- Same ciphering algorithm as in GPRS is adopted, ciphering key is different.
- Key management shall be handled in an effective and secure way.

3.1   LLC layer

A basic assumption is that LLC protocol is used to accomplish ciphering [3]. This requires that LLC is split from SGSN and there is another instance of LLC in the GERAN. The following Figure depicts the proposed protocol architecture. Note that SMLC can be either a separate logical entity or integrated functionality in the GERAN(BSC).
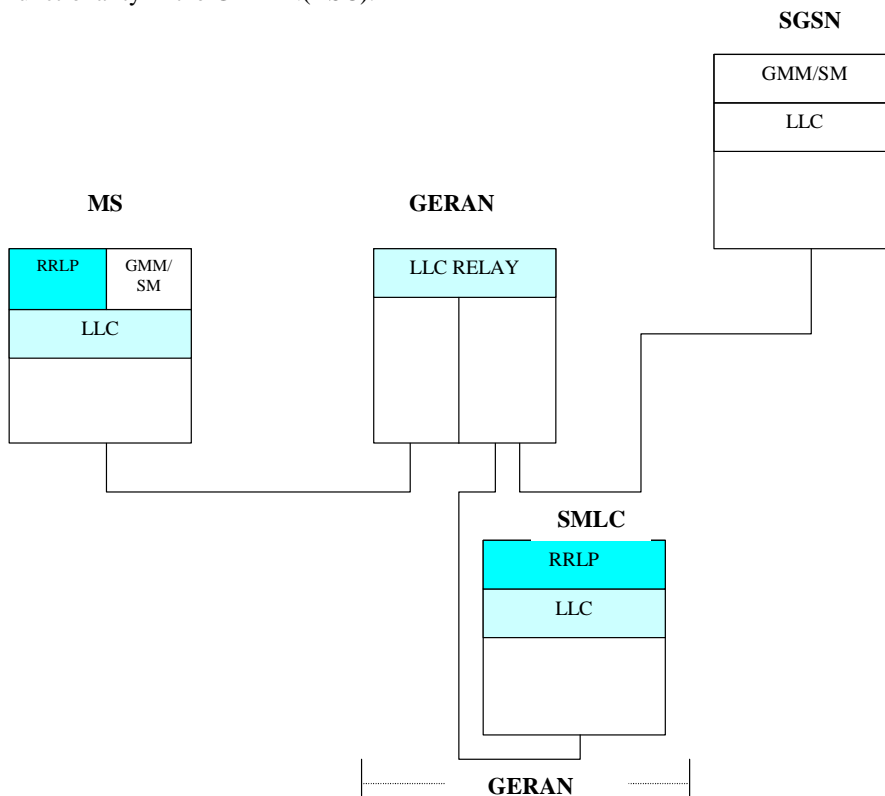

Figure 2 Deployment of the RRLP protocol and split of LLC between SGSN and SMLC in GERAN architecture

Moreover, it is up to the LLC relay function to route LLC frames in uplink direction towards either SGSN or SMLC. This can be done by indicating the destination by a Service Access Point Identifier (SAPI) in the header of each LLC frame. From radio protocols point of view (RLC/MAC) LLC frames are just normal frames and there is no need to handle them differently.

3.2 Ciphering algorithm

The ciphering algorithm proposed is similar to the ciphering in GPRS. Both LLC specific I and UI frames need to be ciphered in GERAN. The following figure 3 depicts the LCS related ciphering procedure
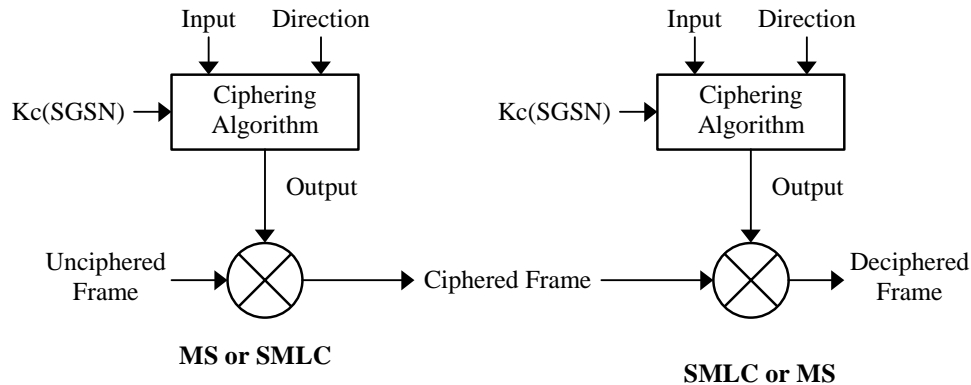

Figure 3 LCS ciphering environment

There are three input parameters: the ciphering key $Kc_{(SGSN)}$, the frame-dependent input (Input), and the transfer direction (Direction). The ciphering algorithm has one output parameter: Output. Minor changes for parameter values are proposed.

- $Kc_{(SGSN)}$ is a ciphering key which is generated by the SGSN from Kc using a one-way function. This function may well be publicly known and it does not require any keys. The essential result of the use of one-way function is the fact that knowing $Kc_{(SGSN)}$ does not give advantage when trying to guess $Kc_{(AuC)}$. The length of $Kc_{(SGSN)}$ is 128 bits.

- $Kc = Kc_{(AuC)}$, $Kc_{(AuC)}$ is a ciphering key provided by the Authentication Center.

- IOV-I/IOV-UI = is a 32 bit random value which is used to calculate the frame-dependent Input value. This parameter is generated by the SMLC

- Other parameters are used as is defined in GPRS ciphering algorithm (see appendix 1)

3.3 Key management

A basic assumption is that LCS ciphering key $Kc_{(SGSN)}$ is not the same as the normal ciphering key Kc in GPRS. $Kc_{(SGSN)}$ is generated from Kc using a one-way function. In the network the key is generated by the SGSN from Kc which is delivered from the authentication center. On the MS side, Kc is generated inside the SIM card. This is delivered to the ME. The one-way function by which the key $Kc_{(SGSN)}$ can be derived may be implemented in the ME. Alternatively, $Kc_{(SGSN)}$ could be implemented in the SIM. There may be a need to specify a procedure for the ME to request a Kc from the SIM card. This could be based on the SIM Toolkit.

A valid $Kc_{(SGSN)}$ should be available at the SMLC and MS in advance a RRLP communication procedure. This means that $Kc_{(SGSN)}$ should be delivered to SMLC either within a location request message from the SGSN or in a separate message prior to the location request. The following Figure depicts the signalling flow.
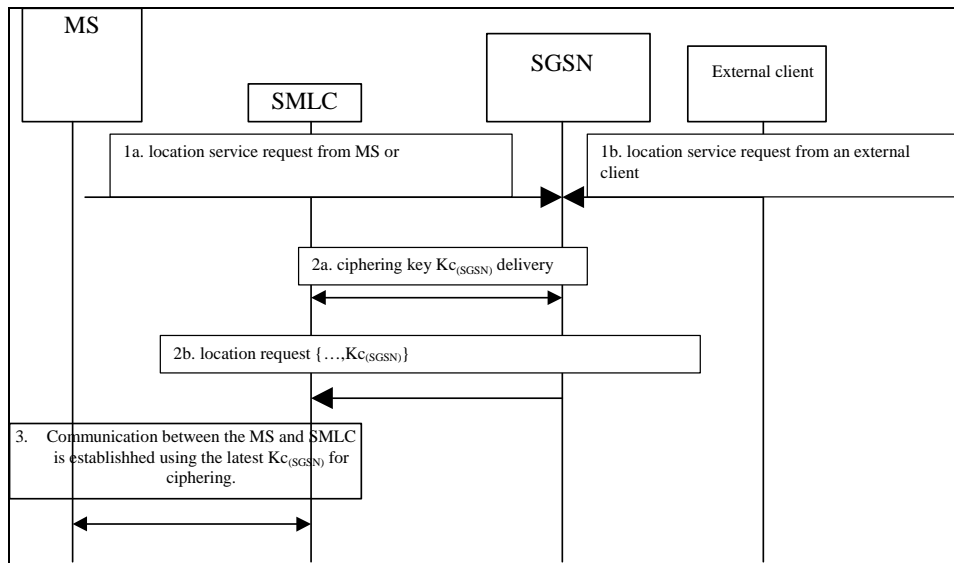
Figure 4 Delivery of ciphering key and ciphering in LCS context

It is not feasible to store the $Kc_{(SGSN)}$ at the MS because it is already derived from the Kc. This also prevents the possibility to unsynchronized versions of ciphering keys. When the MS starts a Mobile Originated Location Request (PS-MO-LR), a ciphering key has to be produced. In Mobile Terminated Location Request (PS-MT-LR), the MS should be notified in advance about the coming RRLP layer communication in order to produce the ciphering key in advance. If the MS is in idle or standby mode, this notification could easily be made by indicating it in a paging message. If the MS is in ready state, it still could be paged. Alternatively, a special notification message could be sent by the SGSN, informing a need to create a ciphering key. As the MS has a valid $Kc_{(SGSN)}$ when LLC frames from SMLC are received, the decryption of the messages can be started immediately without any delay.

3.4 Case studies

This chapter refers to PS-MO-LR and PS-MT-LR procedures in TS 23.271 and points out the issues that are related to ciphering.

3.4.1 Mobile Originated Location Request

- Service request is sent from MS to SGSN and MS generates a $Kc_{(SGSN)}$ based on a valid Kc.
- SGSN sends a location request to SMLC including the $Kc_{(SGSN)}$.
- SMLC starts communicating with MS using the previously generated $Kc_{(SGSN)}$
- MS identifies from the SAPI in LLC header that a LLC message from SMLC is coming and deciphers it using the $Kc_{(SGSN)}$.

3.4.2 Mobile Terminated Location Request

- Location request comes from GMLC to SGSN
- In the case where the mobile is in idle or standby state, then the MS is paged (with a cause value "paging for LCS"). If MS is in ready state, then one of the options should be standardized
  a) page anyway
  b) send a special message to warn about the coming location request
  c) do not send any notification (= do nothing)

- SGSN generates the $Kc_{(SGSN)}$ and sends it to SMLC within Location Request
- SMLC starts communicating with MS using the new $Kc_{(SGSN)}$

- MS receives LLC frame from SMLC, if the MS was LCS paged or notified, then a pre-generated $Kc_{(SGSN)}$ is taken into use, if not then $Kc_{(SGSN)}$ is immediately generated when the MS notices that LLC frame comes from SMLC.

4. summary

LCS support in GPRS will, alone, bring a need to introduce layer 3 signalling in GPRS radio network. Unfortunately, there are currently no procedures to cipher such messages. This proposal is to reside LLC protocol in SMLC to accomplish ciphering. The ciphering algorithm is proposed to be the same as in GPRS.

RRLP protocol is used for communication between SMLC and MS. It is proposed to have the RRLP protocol reside on top of packet protocol stack in SMLC. RRLP messages should be ciphered using LLC services.

A specific LCS ciphering key $Kc_{(SGSN)}$ is generated by the SGSN and ME. A ciphering key needs to be different from Kc for security reasons. The ciphering key needs to be delivered to the SMLC and a notification sent to the MS before a RRLP communication is started between the entities. This is accomplished by including $Kc_{S(SGSN)}$ in a location request message or creating a key exchange procedure between SGSN and SMLC. In mobile terminated location request, the MS should be informed in advance about the RRLP communication by sending a LCS page or by a specific notification message sent to the MS by the SGSN.

5. KEY WORDS

LoCation Services (LCS), Ciphering, Encryption, Decryption.

REFERENCES

[1] GSM 04.31:"Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Mobile Station (MS) – Serving Mobile Location Center (SMLC); Radio Resource LCS Protocol (RRLP)."

[2] 3GPP TS 23.271, Functional Stage 2 description of Location Services

[3] GSM 04.64: "Logical Link Control (LLC) layer specification".