TSG-SA WG3 (Security) meeting #17 **S3-010088**
Göteborg, Sweden, 28th – 2nd March 2001

Agenda Item: 9.2

Source: Ericsson

Title: LCS for GPRS and the BSS+ Solution

Document for: Information and Advice

---

1 Introduction

In 3GPP TSG GERAN there is a work-item (Work Item Description for Building block: Location Services (LCS) for GERAN in A/Gb Mode, Tdoc GP-010390) for developing “LCS for GPRS” utilizing the Gb interface between the CN and the GERAN. There is also another work-item for LCS for GERAN in Iu Mode, this contribution is not related to it and the Iu Mode work item will not be further discussed in this contribution.

In “LCS for GPRS” work, several proposals have been made for how to best design this feature. This contribution explains a bit about the background to this feature and the ciphering issue related to it.

This contribution also highlights the Ericsson BSS+ proposal and asks for feed-back on it.

2 Background

2.1 LCS Architecture

LCS for GSM (see GSM 03.71) allows for two possible architectures, the BSS based where the SMLC is connected via the Lb interface to the BSC and the NSS based where the SMLC is connected via the Ls interface to the MSC. Also see figure 1 below.

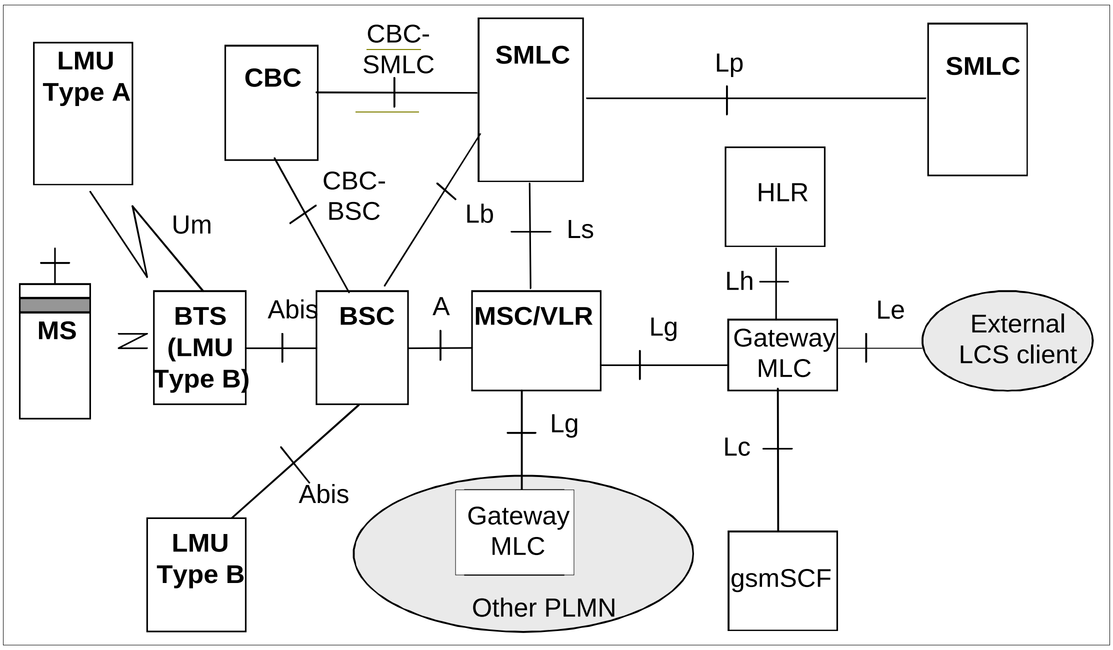

Figure 1: Generic LCS Logical Architecture

2.2 GPRS Architecture

In GPRS (Gb mode) the MS communicates with the SGSN via the BSS (see figure 2). The LLC protocol (see figure 3) is used for point-to-point communication between the MS and the SGSN.

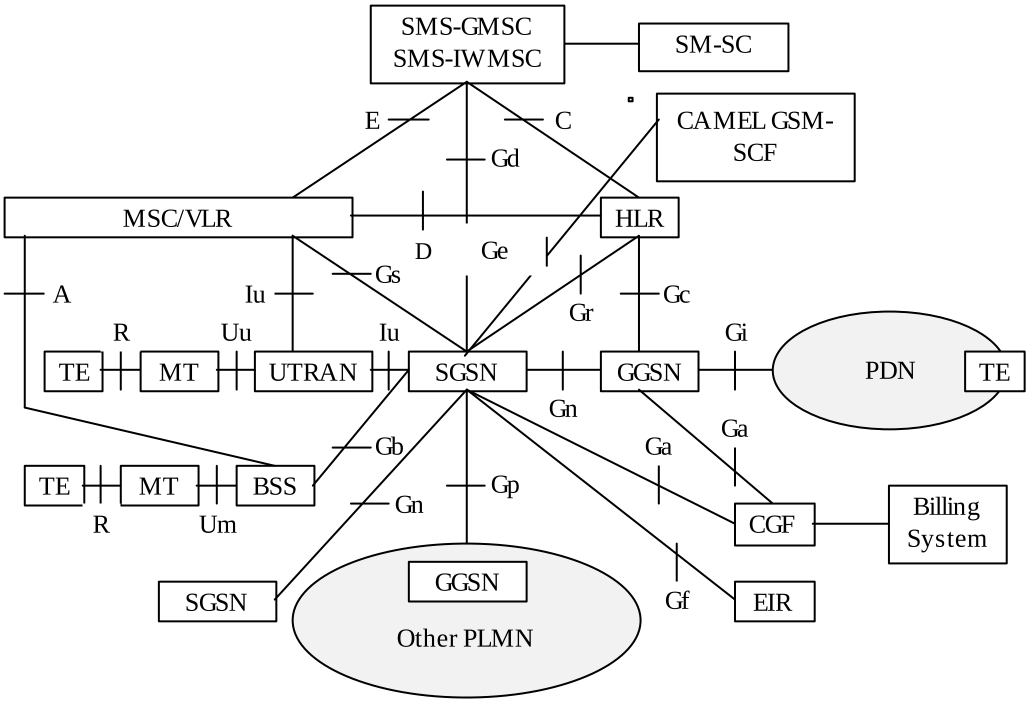

Figure 2: Overview of the Packet Domain Logical (GPRS) Architecture

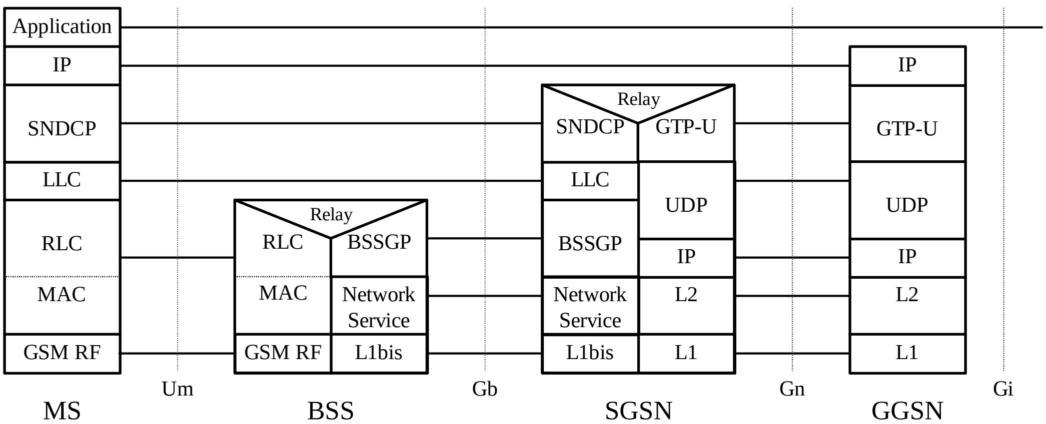

Figure 3: User Plane for GPRS/GSM

2.3 Ciphering Issue

Because the ciphering in GPRS for Gb mode is done in the LLC layer (not in the physical layer) between the SGSN and the MS and the BSS based architecture connects the SMLC to the BSC, there is an issue to consider as far as how to cipher LCS messages for LCS in GPRS. More details can be found in Tdoc GAHL-000009.

2.4 Existing Proposals in TSG GERAN for "LCS for GPRS"

Three major proposals exist so far for how to design the "LCS for GPRS" feature:

- Use LLC between SMLC and MS via the BSS (See Tdocs GAHL-000008 and GAHL-000026)
- Connect the SMLC to the SGSN via the new interface Ln and tunnel SMLC to MS messages through the SGSN (See Tdoc GAHL-000032)
- Connect the SMLC to the BSC via the Lb interface, but still utilize the LLC layer between the SGSN and the MS for SMLC to MS messages (BSS+ Solution, see this document and Tdoc GAHL-010013)

This contribution will describe the later proposal (BSS+ Solution) in more detail.

3 Description of Enclosed Tdocs

This list describes all the enclosed Tdocs and how they relate to LCS in GPRS.

Tdoc	Title	Description
GAHL-000009	Ciphering White Paper	This document describes the ciphering issue for "LCS for GPRS".
GAHL-000026	Protocol layering to support LCS on GPRS protocols in GERAN (Release 4)	Describes the "LLC to SMLC" proposal
GAHL-000032	Protocol Architecture to support LCS in GPRS	Describes the "Tunneling via SGSN" (Ln interface) proposal.
GP-010390	Work Item Description for Building block: Location Services (LCS) for GERAN in A/Gb Mode	This is the official work-item description for "LCS in GPRS".

4 BSS+ Architecture Proposal

The BSS+ proposal is in line with the wishes from the last TSG GERAN meeting about finding a "BSS centric" solution. The network reference architecture for the BSS+ proposal is shown in the figure below.

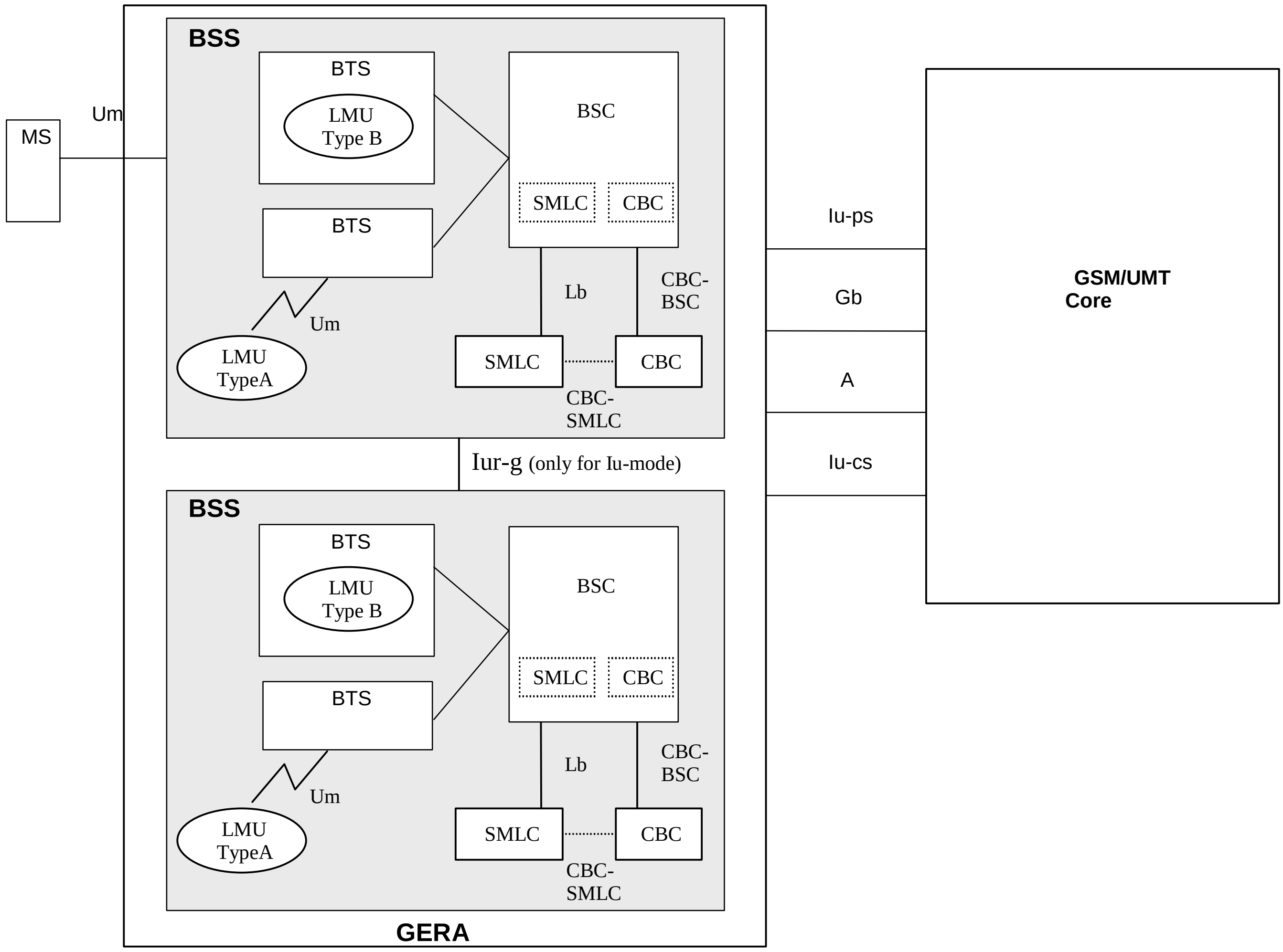

Figure 4: Network Reference Model for BSS+

5 Message Flows for the BSS+ Solution

The proposed message flow for the BSS+ solution (for PS-MT-LR) is described below.

5.1 Packet Switched Mobile Terminating Location Request (PS-MT-LR)

Figure 2 illustrates the general network positioning for LCS clients external to the PLMN for packet switched services. In this scenario, it is assumed that the target MS is identified using an MSISDN, PDP address or IMSI.

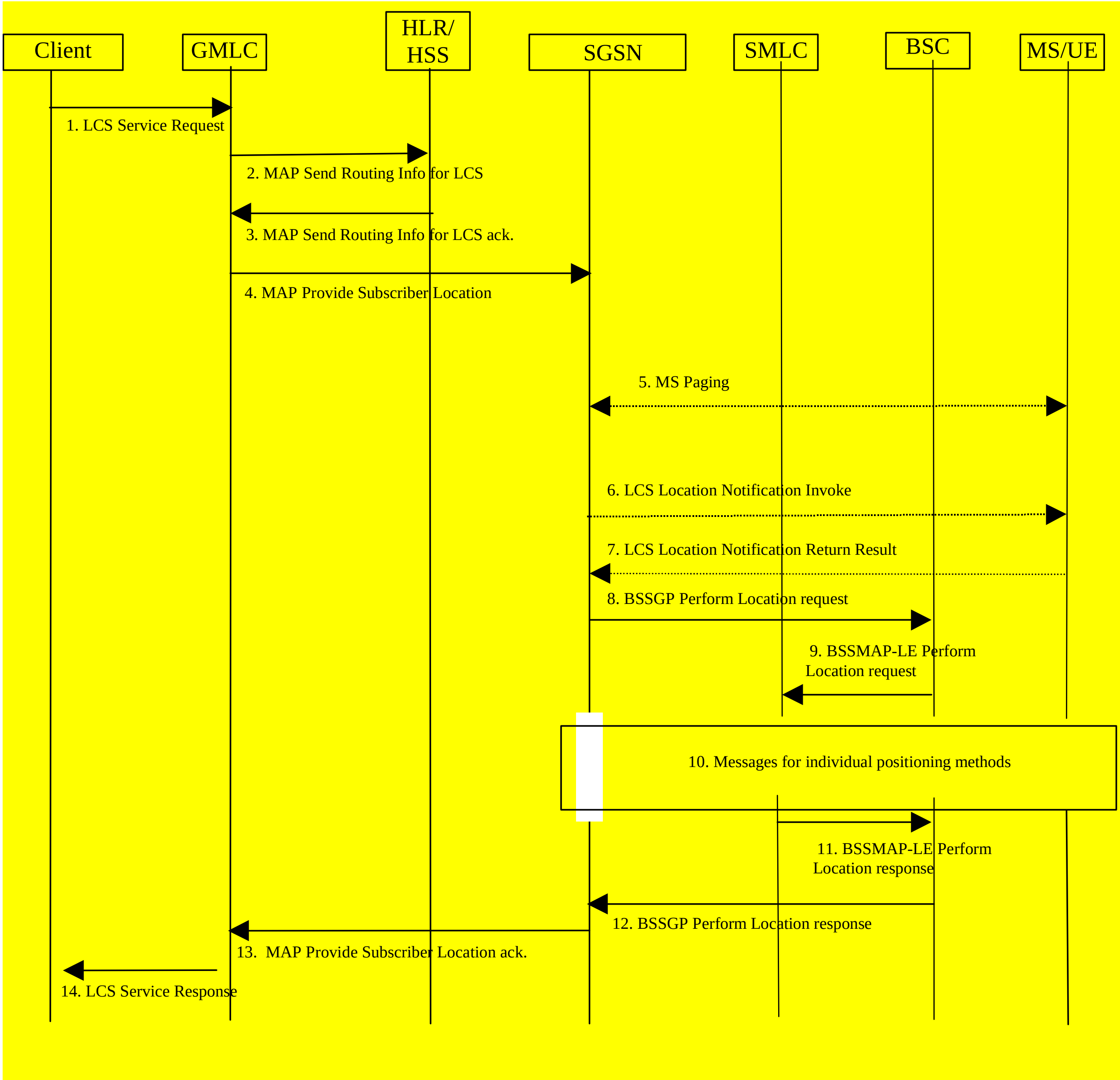

Figure 5: General Network Positioning for Packet Switched PS-MT-LR

Step 10 is the step where air-interface communication is utilized and it is described more in detail below.

5.2 Signalling for Individual Positioning Methods for GPRS

5.2.1 A-GPS and E-OTD Positioning in PS Domain

This signaling flow is generic for all MS based or assisted location methods (MS Based E-OTD, MS Assisted E-OTD, GPS and Assisted GPS). The RRLP message is transported from the SMLC to the BSC in a BSSMAP Connection Oriented Information message. The BSC forwards it in a BSSGP Position Command message. Finally the SGSN delivers it to the MS in a LLC UI frame.

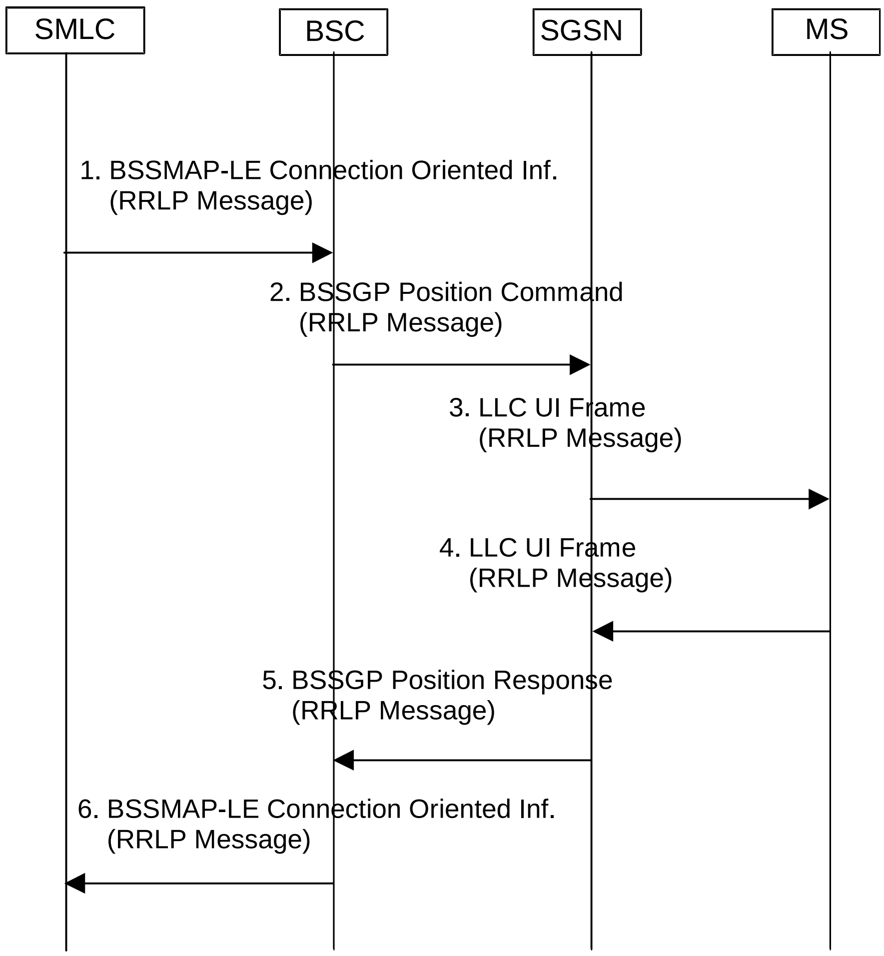

Figure 6: E-OTD/GPS Positioning Procedure in PS Domain

6 Protocol Stacks for BSS+ Solution

This architecture would give allow us to define the following protocol models.

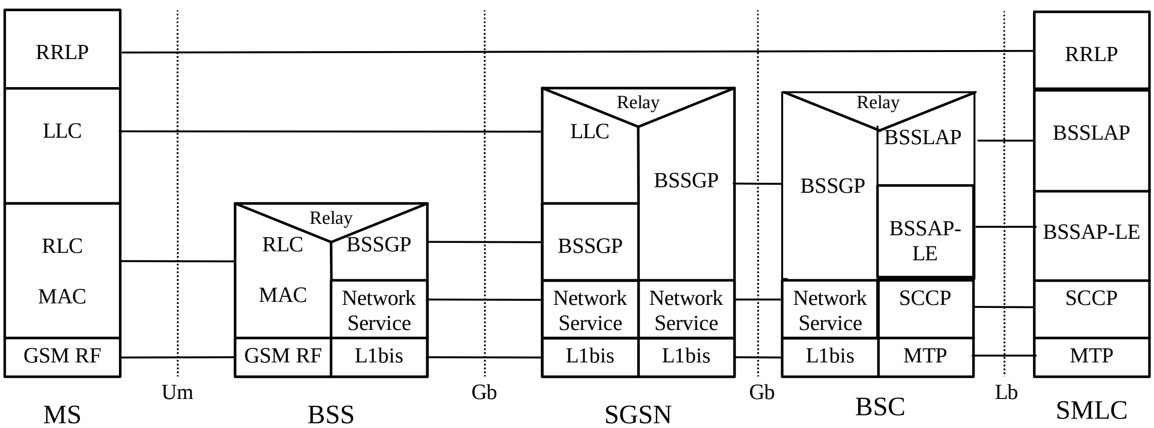

Figure 7: Protocols for SMLC to MS communication

7 Conclusion

The BSS+ proposal solves the ciphering issue by utilizing the LLC protocol between the SGSN and the MS. This means that all air-interface communication for LCS in GPRS can be ciphered. The Gb and Lb interfaces would not be ciphered, which is in line with UMTS and GSM circuit services where the A, Lb, and Iu interfaces are not ciphered. We would very much like to get the SA3 feedback and comments on the BSS+ proposal.

3GPP TSG GERAN LCS Ad-Hoc#1 **GAHL-000009**

Irving, Texas **Agenda item 3.3**

24-27 October 2000

SOURCE: NOKIA

TITLE: CIPHERING WHITE PAPER

1. 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 signalling 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.

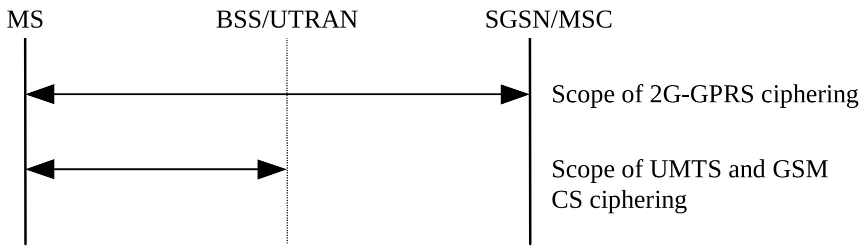

Figure 1 Scope of ciphering

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.

2. 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 minimun amount of changes to the 3GPP specifications

- Ciphering should be implementable to the system with minimum amount of impacts

3. 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).

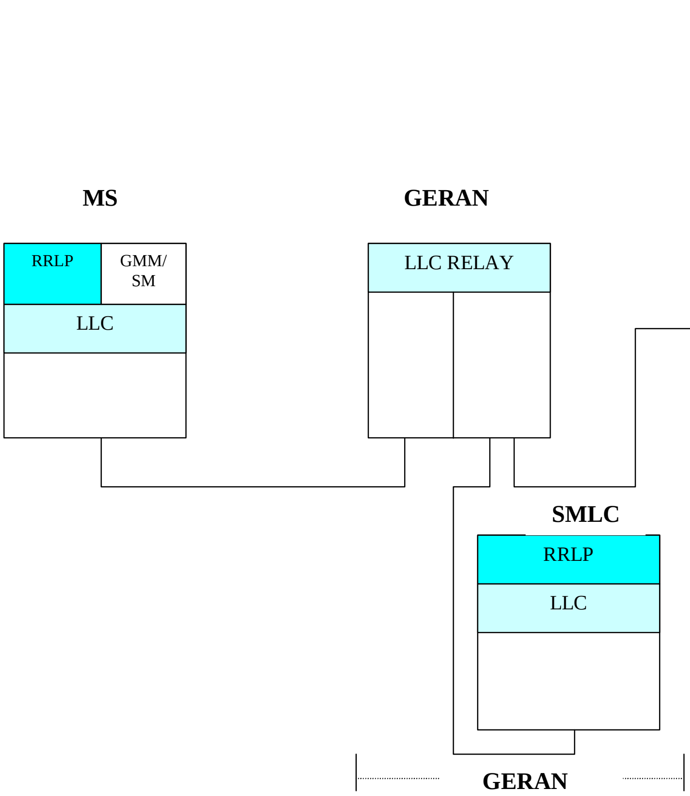

Figure 2 Deployment of the RRLP protocol and split of LLC between SGSN and SMLC in GERAN architecture

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

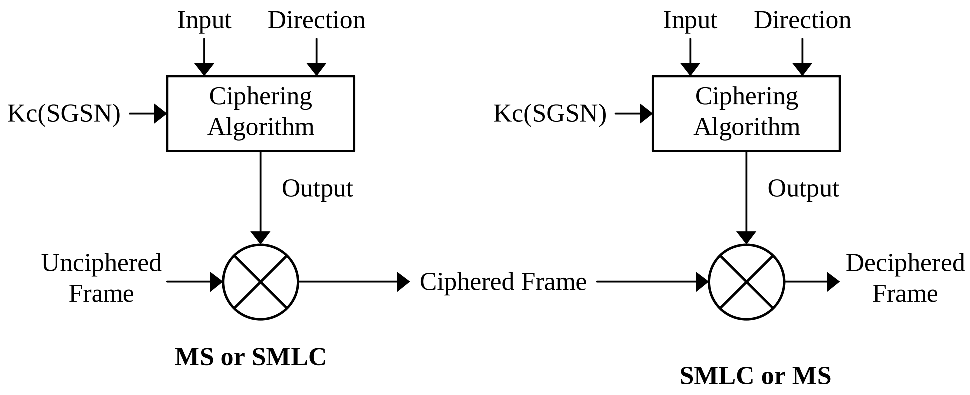

Figure 3 LCS ciphering environment

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.

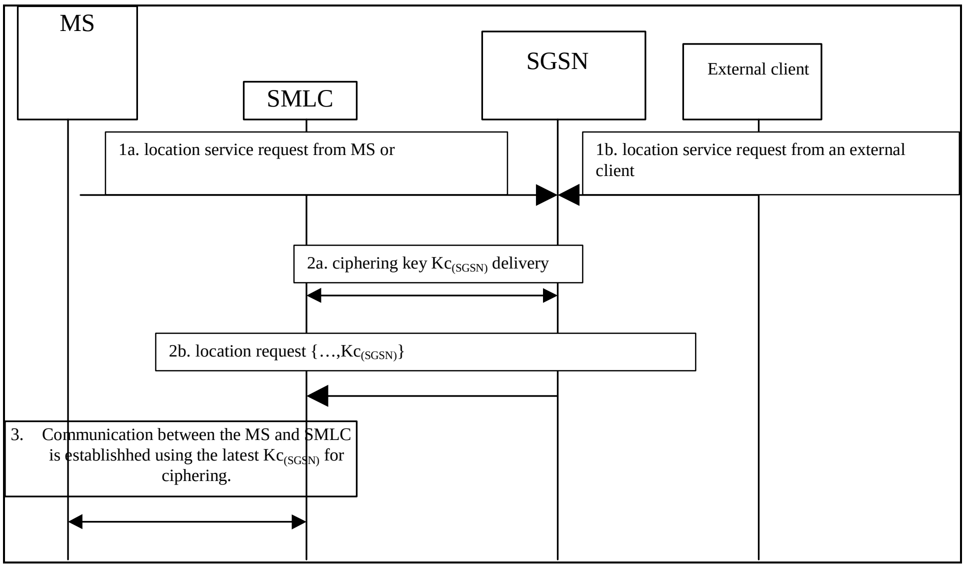

Figure 4 Delivery of ciphering key and ciphering in LCS context

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".

Source: **Nokia**
Title: **Protocol layering to support LCS on GPRS protocols in GERAN (Release 4)**

Summary

This change request adds contents to Chapter 6 in LCS Stage 2 description, TS 43.059. These enhancements are related to protocol layers to support LCS on GPRS protocols in release 4 standards.

Proposal

It is proposed that 3GPP TSG GERAN LCS ad-hoc agrees these updates to be added into Stage 2 specification TS 43.059.

6.2 Protocol Layering in PS Domain

6.2.1 Generic Signalling Model for LCS in PS Domain

Figure 1~~Figure 11~~ shows the generic signalling model applicable to LCS for signalling interaction in release 4 architecture in which an SMLC forms at least one of the signalling end points in the packet switched domain.

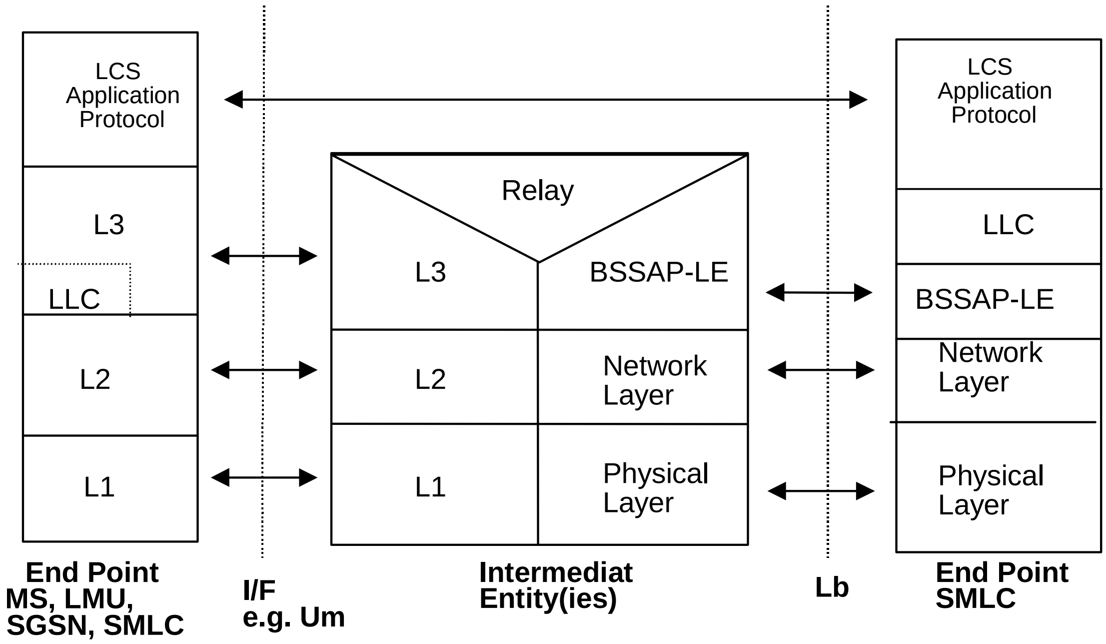

Figure 1~~1~~ Generic Model for LCS Signalling to an SMLC for PS domain

The functions performed by each protocol layer are the same as defined in chapter 6.1.1 with the following additions:

a) LCS application protocol: the same application protocols are used in CS and PS modes on Lb interface in release 4 standards. The messages may include packet mode specific parameters.
b) BSSAP-LE is used in GPRS to carry LLC frames and LCS application protocol signaling units. The messages may include packet mode specific parameters. This layer supports segmentation of LCS application layer protocols. Segmentation is needed when MTP is used on Lb interface.
c) Network Layer is provided using a combination of MTP and SCCP or IP based transport in release 4 standards.
d) Physical Layer – either SS7 signaling links or IP based connections are supported by the physical layer.
e) L3 – a protocol layer compatible with or the same as BSSAP-LE.
f) L2 – logical link layer for the other endpoint
g) L1 – physical layer for the other end point.
h) LLC – encapsulates higher layer messages in LLC frames and performs ciphering providing signalling confidentiality for communication between MS and SMLC.

…

~~**Generic Model for LCS Signalling to an SMLC in Packet Switched Domain (Gb I/f)**~~

~~**Generic Model for LCS Signalling to an SMLC in Packet Switched Domain (Iu-ps I/f)**~~

~~(FFS) …~~

6.2.~~1~~2 Signalling Between SMLC and SGSN

SMLC can be either a separate logical entity or it can be an integrated functionality in BSC. If the SMLC is a separate logical entity, the LCS signalling between SMLC and SGSN is accomplished through the Gb and Lb interfaces towards 2G-

SGSN~~ and through Iu-ps and Lb interfaces towards 3G-SGSN~~. If the SMLC is integrated functionality in the BSC, the LCS signalling is accomplished through Gb ~~or Iu-ps~~ interfaces.

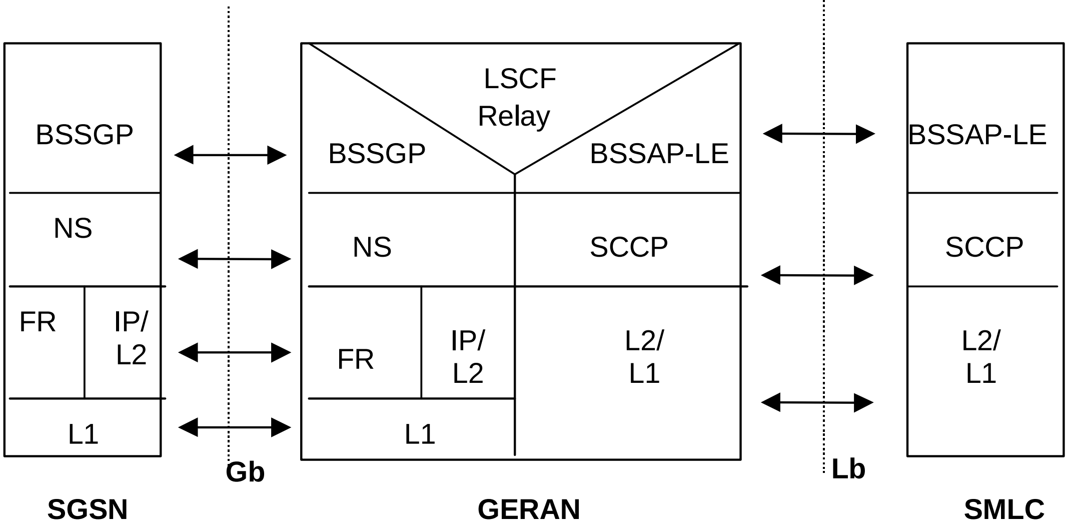

Figure 2~~2~~2 Signalling between an SMLC and SGSN through Gb and Lb interfaces in release 4 protocol architecture

6.2.~~2~~3 Signaling between SMLC and MS

SMLC Signalling to a target MS is accomplised through the Um interface. Figure 3~~Figure 33~~ shows the protocol layers used to support signaling between an SMLC and target MS.

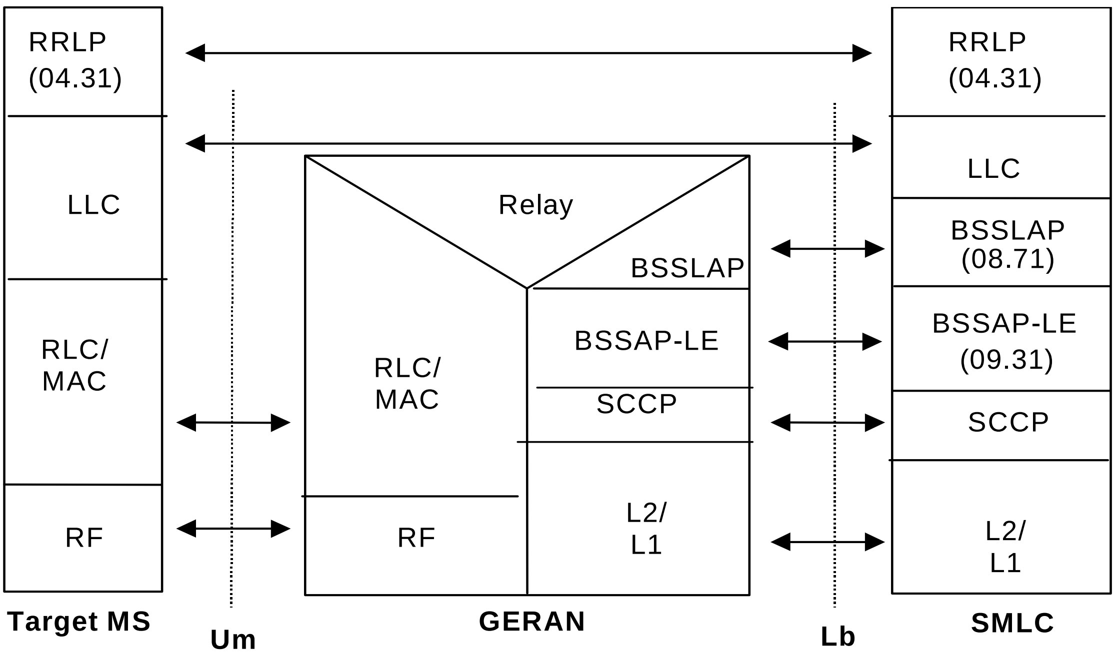

Figure 3~~3~~3 Signalling between an SMLC and Target MS in release 4 protocol architecture

~~FFS~~

~~6.2.3~~6.2.4 SMLC Signalling to a Type A LMU

FFS

~~6.2.4~~6.2.5 SMLC Signalling to a Type B LMU

~~FFS~~

The protocol layers employed to enable signaling between the SMLC and a type B LMU are shown in **Figure 4~~Figure 44~~**.

(Note 1)*: Abis interface is beyond the scope of this document.

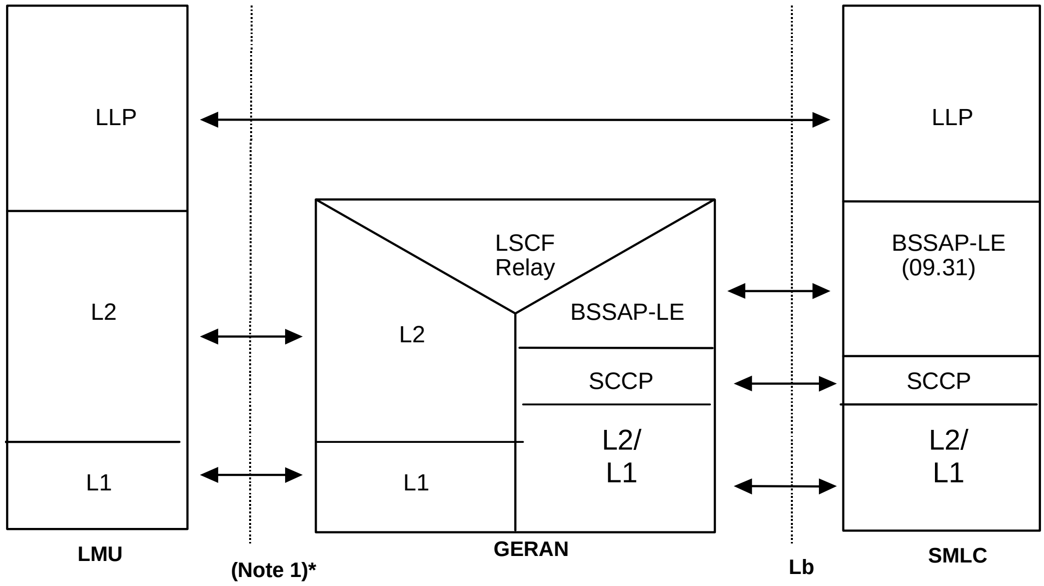

Figure 4~~4~~4: Signalling between an SMLC and Type B LMU

~~6.2.5~~6.2.6 GERAN SMLC Signalling to a peer GERAN SMLC

The Iur-g interface is used to communicate between the LCS functional entities associated with the BSC or SMLC to another GERAN BSC or SMLC. This interface is FFS.

3GPP TSG GERAN LCS AdHoc #2 **Tdoc GAHL-000032**
Orlando, FL, USA **Agenda item x.x.x.x**
December 12th – 14th, 2000

Source: Ericsson

Protocol Architecture to support LCS in GPRS

1 Introduction

In Tdocs GAHL-000008, GAHL-000009, GAHL-000010, and GAHL-000013 various ideas for how to design the protocol architecture for LCS in GPRS should be done. This contribution further explores some possibilities for this architecture.

2 Issues with the Current Proposals

All the current proposals for suffer from some drawbacks. They are related to the fact that the SMLC is connected to the BSS. This means that the BSS has to communicate to two “upstream” entities instead of the one (SGSN) that the architecture was originally designed for.

2.1 Ciphering

One of those issues is the ciphering issue (as identified in GAHL-000009). In short, the problem is that in GPRS there is no ciphering on the BTS to MS interface, instead the ciphering is done end-to-end between the SGSN and the MS in the LLC layer. Therefore, for the current LCS architecture, a new ciphering method is needed somewhere along the link between the SMLC and the MS. With the SMLC connected to the BSS, this either impacts the SMLC new requiring the SMLC to support ciphering, or it impacts the PCU to support a new ciphering mechanism. Finally, whatever solution that may be found, there is an impact on the MS to support the new ciphering.

2.2 Ciphering Key Management

In the contribution GAHL-000009 it is suggested to use a new key, $Kc_{(SGSN)}$, for ciphering of LCS in GPRS.

The management of the $Kc_{(SGSN)}$ is not trivial. Consider the following cases:

- The $Kc_{(AuC)}$ might change during a GPRS attach session. The SGSN orders the MS to change $Kc_{(AuC)}$ (and implicitly $Kc_{(SGSN)}$). The SMLC must also be informed about the new $Kc_{(SGSN)}$ via the SGSN-SMLC interface.

- Shall there be only one SMLC per PLMN? One SMLC per SGSN? One SMLC per BSS? If there are several SMLC per PLMN how shall "inter-SMLC-change be done", the new SMLC will not know the history of number of sent and received LLC-frames between MS and old-SMLC. The input vector to the algorithm is dependent of previous number of sent/received LLC frames. In other words a similar reset-mechanism (to inter-SGSN-RA-update) between MS and new-SMLC must be defined.

- The same problem exist if the MS is allowed to roam between PLMNs without performing a new GPRS attach.

2.3 Flow Control

Another issue with the current proposal is how to handle scheduling and flow control of the two streams of data coming from the SGSN and the SMLC towards the MS.

From the perspective of the BSSGP in the BSS, the current flow control mechanism is based on the following model:

- there is a downlink buffer for each BVC (cell), as identified by a BVCI, in a BSS;

- the transfer of BSSGP UNITDATA PDUs for an MS from the SGSN is controlled by the BSS;

The principle of the BSSGP flow control procedures is that the BSS sends flow control parameters to the SGSN, which allow the SGSN to locally control its transmission output in the SGSN to BSS direction. The SGSN shall perform flow control on each BVC and on each MS.

The BSS shall control the flow of BSSGP UNITDATA PDUs to its BVC buffers by indicating to the SGSN the maximum allowed throughput in total for each BVC. The BSS shall control the flow of BSSGP UNITDATA PDUs to the BVC buffer for an individual MS by indicating to the SGSN the maximum allowed throughput for a certain TLLI.

With the SMLC to BSS connection, a new stream of data from the SMLC to the BSS would now have to be flow controlled. This creates additional complexity in the BSS. This would have to be handled per cell and per MS.

2.4 Scheduling and Quality of Service

In the “pre-LCS” GPRS model, there is only one source for downstream packet-data towards the BSS, the SGSN.

The SGSN can provide a BSS with information related to ongoing user data transmission. The information related to one MS is stored in a BSS context. The BSS may contain BSS contexts for several MSs. A BSS context contains a number of BSS packet flow contexts. Each BSS packet flow context is identified by a packet flow identifier assigned by the SGSN. A BSS packet flow context is shared by one or more activated PDP contexts with identical or similar negotiated QoS profiles. The data transmission related to PDP contexts that share the same BSS packet flow context constitute one packet flow.

Three packet flows are pre-defined, and identified by three reserved packet flow identifier values. The BSS shall not negotiate BSS packet flow contexts for these pre-defined packet flows with the SGSN. One pre-defined packet flow is used for best-effort service, one is used for SMS, and one is used for signalling.

The combined BSS QoS profile for the PDP contexts that share the same packet flow is called the aggregate BSS QoS profile. The aggregate BSS QoS profile is considered to be a single parameter with multiple data transfer attributes as defined by the Quality of Service Profile. It defines the QoS that must be provided by the BSS for a given packet flow between the MS and the SGSN, i.e., for the Um and Gb interfaces combined. The aggregate BSS QoS profile is negotiated between the SGSN and the BSS.

With the introduction of the SMLC to BSS connection for LCS in GPRS, there is now another source for a data stream towards the MS and the scheduling and QoS handling of this new stream must be integrated with the existing mechanisms in BSS.

2.5 LLC Sniffing in BSS

In at least some earlier proposals (see GAHL-000009), it has been proposed to let the BSS look into the LLC frames. This is done in order to determine whether an uplink LLC frame is supposed to be sent to the SGSN or sent to the SMLC. This violates the current GPRS architecture where the LLC protocol layer is fully transparent for the BSS and only the MS and the SGSN needs to understand the LLC protocol.

2.6 SMLC Impacts

In at least some earlier proposals (see for example GAHL-000008 and GAHL-000009), it has been proposed to add the LLC protocol to the SMLC. This is a rather large and complicated protocol. This would mean a large impact to the SMLC. In addition to the protocol itself, the ciphering mechanism would have to be implemented in the SMLC. This is another big impact on the SMLC.

3 Architecture Proposal

To avoid all the problems described above that are a result of connecting the SMLC to the BSS for LCS in GPRS, an alternative solution should be chosen. This alternative is described in figure 1. The Lb interface is used for CS LCS signaling and the Ln interface for PS LCS signaling. This proposal significantly simplifies the development of LCS in GPRS.

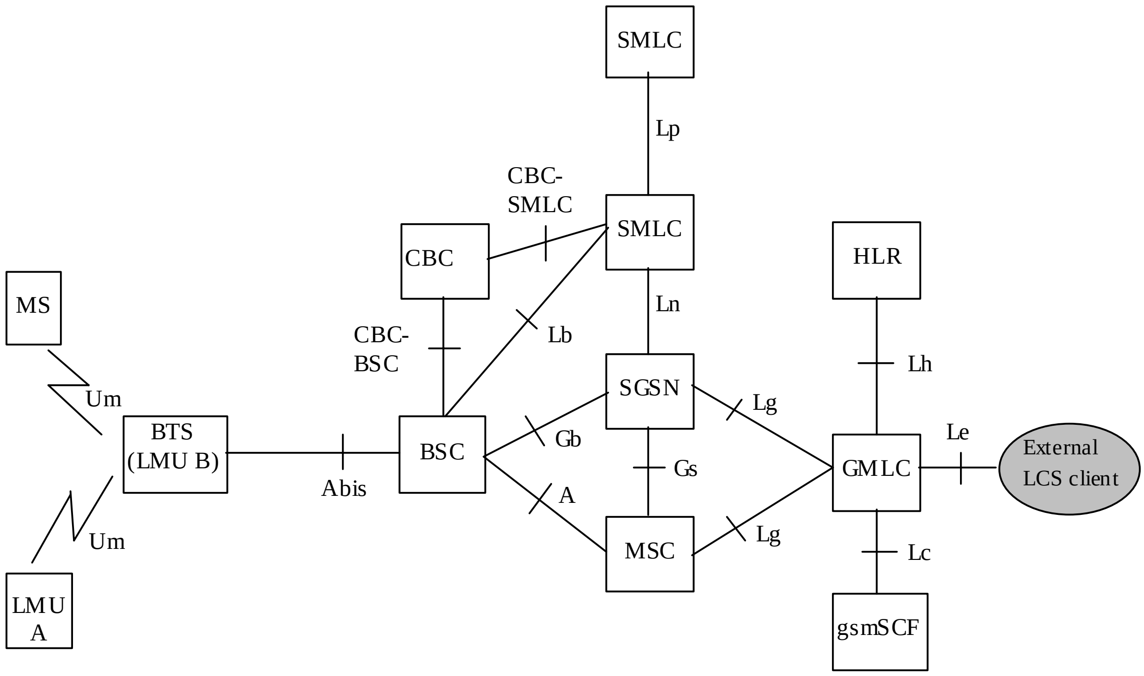

Figure 1: Network Reference Model for LCS in GPRS

This architecture would give allow us to define the following protocol models.

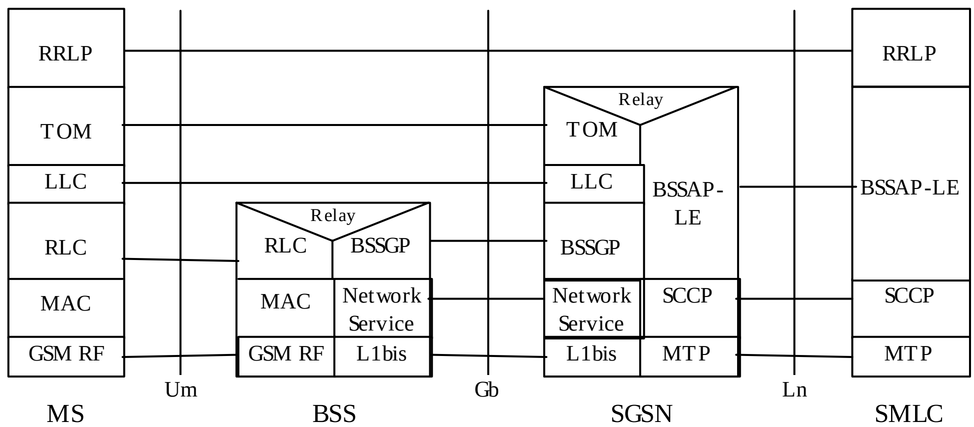

Figure 2: Protocols for SMLC to MS communication

The BSSAP-LE and TOM protocols would need to be modified for this communication. Both would need to be updated to be able carry RRLP messages.

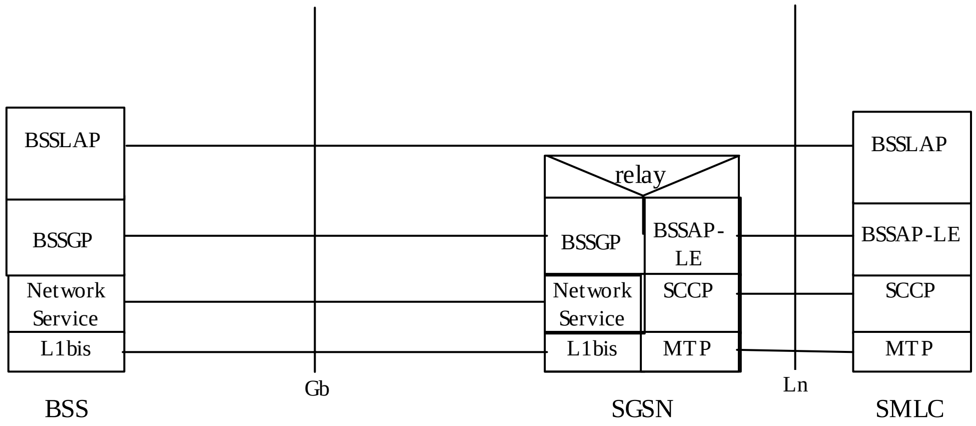

Figure 3: Protocols for SMLC to BSS communication

The BSSGP protocol need to be modified to add messages that carries BSSLAP messages. The BSSLAP protocol would probably need to be modified to support packet data (FFS).

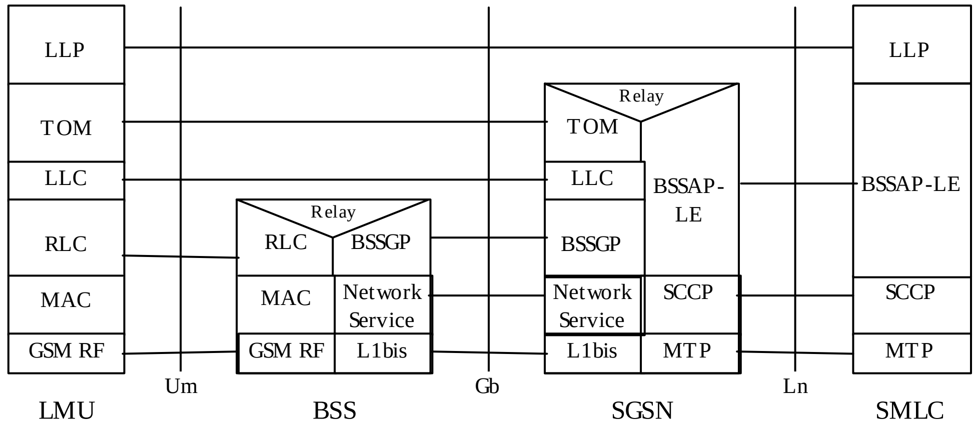

Figure 4: Protocols for SMLC to Type A LMU communication

The TOM protocol would need to be modified to be able to carry the LLP protocol. Notice that BSSAP-LE is already able to carry the LLP protocol.

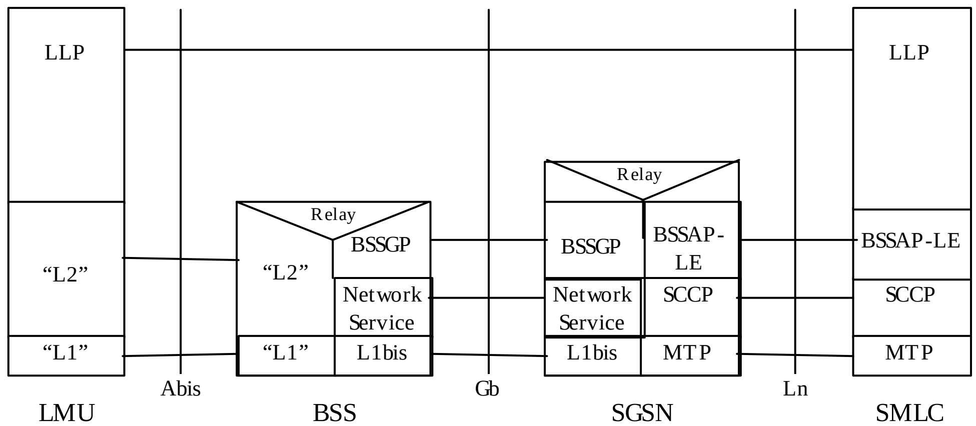

Figure 5: Protocols for SMLC to Type B LMU communication

No standards modifications would be needed for this, but a proprietary L1 and L2 protocol between the BSS and the LMU.

4 Conclusions

In light of the discussion in section 2, it is recommended that the architecture described in section 3 be adopted for the LCS in GPRS work item.

TSG GERAN #3~~2~~
Boston, MA~~Norrtälje, Sweden~~
15-19 Jan 2001~~06-10 Nov 2000~~

Source: LCS Rapporteur
Title: Work Item Description for Building block: Location Services (LCS) for GERAN in A/Gb Mode
Document for: Approval

Work Item Description

Title

Location Services (LCS) for GERAN in A/Gb Mode

1 3GPP Work Area

X	Radio Access
X	Core Network
X	Services

2 Linked work items

LCS work items for Release 4 and Release 5 ~~R2000~~ in TSG-SA, TSG-CN, TSG-RAN

3 Justification

LoCation Services (LCS) provide the mechanisms to support mobile location services for operators, subscribers and third party service providers. Currently GSM LoCation Services (LCS) Release 98 and 99 supports only circuit switched case. In order to provide same services for packet switched case support for Packet Switched (PS) LCS domain should be included in the 3GPP GERAN LCS Release 5~~4~~. Other enhancements will be considered in later 3GPP GERAN Releases. The alignment of GERAN LCS Release 5~~4~~ with UMTS LCS in Release 4 is required, e.g. due to the common Core Network.

4 Objective

The purpose of this work item is to enhance GERAN LCS, i.e. to implement GERAN LCS Release 5~~4~~. This includes introduction of LCS in packet switched GERAN including similar services that are available in circuit switched GSM, with reasonably small amount of changes to the existing GPRS specifications. Backward compatibility with GSM LCS R'98 & '99 BSS architecture is required. LCS support for GERAN also includes the support for circuit switched and packet switched modes (i.e. GPRS), which are not covered in GSM LCS R'98 & R'99. The LCS Stage 1 description TS 22.071 already includes this requirement but should be further elaborated regarding LCS support in the packet switched domain. The three positioning mechanisms supported by GERAN LCS are Timing Advance (TA), Enhanced Observed Time Difference (E-OTD), and Global Positioning System (GPS).
There are two main efforts that can be identified for LCS in 3GPP TSG GERAN.

1. Support LCS in A/Gb mode: LCS support on packet-data channels and over the A/Gb interface.
2. Support LCS in Iu mode: LCS support over the Iu-ps, Iu-cs, Iur-g interfaces.

This building block describes support for LCS in GERAN for A/Gb mode.

In order to progress the LCS work, efficiently, emphasis on development of "LCS in A/Gb mode" work should be completed for the GERAN specifications by June 2001.~~April 2001~~.

The following work tasks are identified as high priority items:

- GERAN LCS Stage Two (first release)
- Gb interface support for LCS
- ~~A interface changes for LCS~~
- Broadcast of LCS data on packet channels
- RLC/MAC protocol support for LCS
- L3 protocol support for LCS
- Timing Advance based positioning on packet channels
- Class A and Dual Transfer Mode (DTM) MS impact (i.e. Air-interface impacts)
- Updates to existing protocols (RRLP, LLP, SMLCPP, BSSLAP, etc.) due to GPRS
- Ciphering of LCS in GPRS
- Lb interface support for LCS in GPRS
- Miscellaneous impacts from the new LCS Stage Two (23.271)

5 Service Aspects

- Provision of Velocity
- Privacy Control
- Location of All Mobiles in Geographical Area (LAMGA). This means that a LCS application can request locations and possibly identities of all mobiles in a certain geographical area. More exact definition of LAMGA is FFS.
- The Common LCS Stage 1 mentions Defined Geographical Areas (DEGA). For example it may be possible to identify and report when the user's terminal enters or leaves a specified geographic area. Also certain services might be available to mobiles within specified areas. Defined Geographical Areas should be specified in more detail in Stage 1 first. (FFS)
- Event Based Location Request - FFS

6 MMI-Aspects

None

7 Charging Aspects

None

8 Security Aspects

None

9 Impacts

Affects:	SIM	ME	AN	CN	Others
Yes		X	X	X	
No	X				
Don't know					

10 Expected Output and Time scale (to be updated at each plenary)

New specifications						
Specification No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
43.059	Functional Stage 2 Description of Location Services in GERAN	GERAN				This specification describes the LCS support in GERAN for both Circuit Switched and Packet Switched services.
23.271	Functional stage 2 description of LCS [based on 23.171 and System and core network aspects from 03.71 +new features]	SA 2				This specification describes the system and core network aspects of LCS and is common to GSM and UMTS

Affected existing specifications				
Specification No.	CR	Subject	Approved at plenary#	Comments
44.018		Mobile radio interface layer 3 specification, Radio Resource Control Protocol		
44.031		Mobile Station (MS) Serving Mobile Location Centre (SMLC) Radio Resource LCS Protocol (RRLP)		
44.035		Broadcast Network Assistance for Enhanced Observed Time Difference (E-OTD) and Global Positioning System (GPS) Positioning Methods		
44.060		R adio Link Control/ Medium Access Control		
44.064		LLC specification GPRS		
44.071		Mobile radio interface layer 3 Location Services (LCS) specification;		
45.005 ~~V4.01~~		Radio transmission and reception		
45.008 ~~V4.01~~		Radio subsystem link control		
45.010		Radio subsystem synchronization		
45.050		Background for Radio Frequency (RF) requirements		
48.008		MSC-BSS interface; Layer 3 A i/f		
48.018		BSS GPRS protocol		
29.002		Mobile Application Part (MAP) Specification		
29.031		Base Station System Application Part LCS Extension (BSSAP-LE)		
22.071		3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Location Services (LCS); Service description, Stage 1		This specification is common to GSM and UMTS (/GERAN and UTRAN)

24.008		Mobile Radio Interface Layer 3 Specification		

11 Work item rapporteur

Nokia – Margaret Livingston

12 Work item leadership

GERAN

13 Supporting Companies

Nokia, Motorola, Ericsson, Siemens, Qualcomm, T-Mobil

14 Classification of the WI (if known)

	Feature (go to 14a)
X	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

14b The WI is a Building Block: parent Feature

Location Service (UMTS)

14c The WI is a Work Task: parent Building Block

(one Work Item identified as a building block)