Technical Specification Group Services and System Aspects ***TSGS#14(01)0717***
Meeting #14, Kyoto, Japan, 17-20 December 2001

Source: **TSG SA WG2**
Title: **TR 23.871 on " Enhanced support for User Privacy in location services"**
Agenda Item: **7.2.3**

The attached Rel-5 Technical Report 23.871 ‘Enhanced support for user privacy in location services’ provides some indications on how to enhance the privacy mechanisms provided for Location Services to support the increasing number of LCS clients and the varying privacy requirements for location services.

It identifies and describes the service requirements for enhanced user privacy in location services (LCS) and the corresponding functional requirements.
The first part of the TR describes the corresponding stage 1 type of service requirements and may be moved to the LCS Stage 1 specification TS 22.071, as seen feasible by TSG SA1.
The second part of the TR describes the stage-2 type of functional requirements for enhancing user privacy in location services and may be moved to the LCS Stage 2 specification TS 23.271, as seen feasible by TSG SA2.

3GPP TR 23.871 V1.0.0 (2001-12)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects
System Aspects;

Technical Report
Enhanced support for User Privacy in location services
(Release 5)

Keywords

UMTS, service, multicast

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

There is a need to enhance the privacy mechanisms provided for Location Services to support the increasing number of LCS clients and the varying privacy requirements for location services. It should also be possible for the subscriber to set or change the location related privacy parameters in the home network. There are some limitations in support for user privacy in the current LCS specifications in 3GPP and there is a need to enhance the privacy mechanisms e.g. for roaming subscribers.

In current Specifications only limited screening for privacy is possible. The screening is based on the “LCS client ID” parameter of MAP Provide Subscribe Location message used by GMLC to request the subscriber’s location from SGSN or MCS. MSC/VLR maps the received LCS client ID to subscriber’s Privacy parameters (e.g. list of allowed LCS clients) to screen out the unwanted location requests. In practise, there is a need to have more detailed service type screening e.g. to differentiate between “where am I” type of services and games or entertainment services.

Additionally, it will be difficult for a subscriber to use local location based services when roaming. The subscriber does not have proper means to add local LCS clients to the allowed LCS client list in the Home environment HLR. Furthermore, the privacy parameters are defined with quite a narrow scope in the HLR, which may make it difficult for the subscriber to set additional and varying privacy parameters per LCS client.

According to the current specifications, the subscriber cannot receive any information regarding who originally asked for the location of the subscriber. Subscribers should be notified about the Requestor identity and it should be possible to allow the location information to be given only to those requestors, who are entitled to have it. All subscriber and location information should anyhow be protected according to privacy requirements in the national regulations.

In order to fulfil Japanese national regulatory guidelines, the LCS shall support the codeword functionality as an optional function. This codeword functionality enables UE to limit unwelcome LCS access from a third party.

1. Scope

This Technical Report for Rel-5 identifies and describes the service requirements for enhanced user privacy in location services (LCS) and the corresponding functional requirements. The first part of the TR describes the corresponding stage 1 type of service requirements and may be moved to the LCS Stage 1 specification TS 22.071, as seen feasible by TSG SA1. Stage one is the set of requirements which shall be supported for the provision of enhanced user privacy in location services, seen primarily from the subscriber's and service providers' points of view. The TR describes some possible enhancements to the privacy mechanisms provided for Location Services to support the increasing number of LCS clients and the varying privacy requirements for location services.

The second part of the TR describes the stage-2 type of functional requirements for enhancing user privacy in location services and may be moved to the LCS Stage 2 specification TS 23.271, as seen feasible by TSG SA2.

This TR defines the service requirements and functional requirements for the enhanced support of user privacy in location services regarding:

- General description of enhanced user privacy in location services
- Definition of enhanced user privacy in location services capabilities
- Service requirements
- Charging aspects
- Security aspects
- Roaming, service availability and continuity
- Relation between privacy issues in Presence and Location services.

2. References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1] 3GPP TS 22.071

[2] 3GPP TS 23.271

3. Definitions, symbols and abbreviations

3.1 Definitions

Privacy profile register (PPR): a data base containing subscriber privacy information for location services

Requestor: the originating entity which has requested the location of the target UE from the LCS client.

Requestor Identity: This identifier is identifying the Requestor and can be e.g. MSISDN or logical name.

Service Type: [The definition of Service Type is to be included.] The privacy setting may be different depending on which Service Types are offered to the target UE or requested by the target UE.

Service Identity: Identity of the service under certain LCS Clients

User: The subscriber and user of the target UE

3.2 Abbreviations

4. General description

5. Service Requirements (this chapter should be handled by SA1)

5.1 Service Type Privacy

The user may wish to differentiate between privacy requirements even with one LCS Client, depending on which service is requested by the user from this LCS client or which service is offered to the user by this LCS Client.

The LCS client requests location information for a target UE from GMLC. Currently the location request contains only the identity of the LCS client and the identity of the target UE. The LCS client request is screened by GMLC using the identity of the LCS client. The screening mechanism is enough for the basic type of location requests, but there is a need to enhance the functionality of the mechanism because one single LCS client may offer or support several or a multitude of different services. It is clear that the target UE user will have different privacy demands for different services even when only one LCS client offers the services.

The enhanced mechanism should enable the users to allow their location information to be given to all LCS clients providing an indicated type of service. The user could e.g. allow all dating type services to get location information. The location request message issued by the LCS client to GMLC could be enhanced to include a service identity which would then be interpreted by GMLC to indicate what services belong to a certain Service Type category. The subscriber should be able to define and set privacy rules based on service type, so that services under that service type can be handled according to the corresponding service type privacy setting.

The service type functionality would allow subscribers to use location services more easily while roaming.
The service type could be seen as an attribute of the LCS client and the LCS client name could contain the service type.
The service type shall be defined in a useful way and it shall be possible to verify that the service type indicated by the LCS client is correct.

Note: There are opposite views regarding:

- whether the service type check may be done in the network or only by the target user
- whether it is necessary to standardize the actual service type or not, i.e. should the service type (coding) be globally unique?
- whether it is necessary to specify the service type within 3GPP scope or not, i.e. could the service type be handled on application level?

Service type checking by the target would be a “looser” way of defining services, and allowing users and client more freedom in defining services, while service type checking by the network would require some standardization, but would allow the network to control “spamming” towards the target.

Service type checking on application level avoids unnecessary signaling in core network, i.e. filters out the Location requests that anyway is going to be rejected.
In addition application/content providers can start offering (if not already done?) this kind of service without waiting for Rel5 of 3GPP.

5.2 Support for enhanced privacy checking

It is seen that the current way to handle the privacy related settings in the network is probably too limited to support the increasing number of LCS clients and the varying privacy requirements for location services. It should also be possible for the user to set or change the location related privacy parameters in the home environment. In order to support additional privacy settings for location services architectural changes may be needed, see chapter 7.

For compatibility reasons to Rel-4 the MSC/SGSN and HLR privacy functionality has to be kept (notification/verification).

5.3 Requestor

In the current 3GPP LCS specifications only the LCS client is identified and authorized when a location based application is requesting the position of a target UE andin the original LCS specifications the LCS client itself was the originator, i.e requestor, of the location information. The GMLC may store an “Authorized UE List”, which holds MSISDNs or groups of MSISDN for which the LCS Client may issue a location request [2].

Within 3GPP scope there is no mechanism for the target UE user to activate a certain application with a known LCS client, but still be able to restrict who are allowed to get position information regarding the target UE. A simple example of this type of service is a “Friends finder” application. Currently there is only a relation between the LCS client and the MSISDNs it is allowed to issue location request for, but there is no relation between the originating requestor and the target UE. This prevents the target UE user from authorizing the originating requestor.

Note: It is FFS if the relation between the originating requestor and the target UE could be handled by the application. Applications like the “Friends finder” typically already today provide this kind of relation.

A new service requirement is hence identified, that the Location Request issued by the LCS client to GMLC should be enhanced to optionally include also the identity of the originator of the location request, i.e. the Requestor, not only the identity of the LCS client. The scenario is developed such, that the requstor is connected to the LCS client as a separate entity, with its own identity and name. Because of this, also the requestor must be authenticated by the LCS client and/or the network.

Note 1: Other security aspects of the Requestor functionality should be further studied.

Note 2: It is seen that the LCS client should not use the same requestor name for several requestors. On the other hand, the requestor name could be a name of a closed user group, that could be used by and for different requstors, but this is for further study

The identity of the Requestor shall be included in the privacy interrogation request, when this is sent to the target UE and shown to the user.

This functionality should possibly be introduced already in Rel-5.

5.4 User Control

The target user must have full control regarding who can get his or her location information. The current LCS stage 1 specification 22.071 contains the following text on user control:

"The user shall be able to change the following settings in the privacy exception list.

- the LCS Client and/or group of LCS Clients list

- the target UE user notification setting (with/without notification)
- the default treatment, which is applicable in the absence of a response from the target UE for each LCS client identifiers"

In addition the user should also be able to change privacy settings for the service types. The mechanisms for user control are FFS.

5.5 Codeword

The codeword is an optional function that shall be handled according to the national regulatory guidelines option for LCS location services to protect UE against monitoring his/her location from the third party access.

The codeword is set and managed by the UE. The user of the UE is responsible to distribute his/her codeword to whom the user it is allowed to request his/her location. Once codeword has been set and properly distributed, UE is protected against the location request from a third party that does not know his codeword.

Note1: It should be clarified if this codeword should be limited to value added services only. The codeword functionality may not be applicable to emergency or lawful intercept services.

Note2: It should be studied what is the relation between this new codeword functionality and the 5 privacy setting alternatives in the current specifications. (The privacy setting alternatives are listed in chapter 7.)

6. Stage 2 description of service type privacy

LIF has defined a 'Service Identity' information element which is used to identify the services offered by the LCS client. The LCS client shall forward the service identity information in the LCS Service Request on the Le interface from the LCS client to the GMLC. It is for further study whether the GMLC or PPR shall map the received service identity to a specific Service Type when the service is provisioned in GMLC. If GMLC only receives the LCS client identity but not the service identity, the GMLC may report an error to the LCS client, or in case the LCS Client is explicitly so authorized, proceed with the request. The service type information may be included in HLR/HSS and in the Privacy Profile Register. Also the the Provide Subscriber Location MAP message sent by GMLC on the Lg interface to MSC and SGSN may contain the Service Type information.
The service type can be defined in a similar way as Annex C in TS 22.071, which describes the attributes for specific services.

The service type privacy setting could be the same as the 5 privacy settings listed in Annex A of 23.271, but in addition it may be necessary to define some new privacy settings according to service type.

7. Stage 2 description of enhanced privacy checking

LCS Stage 2 specification TS 23.271 defines only limited set of privacy options in chapter 9.5.3 consisting mainly of five different privacy settings:

- positioning not allowed;
- positioning allowed without notifying the UE user (default case);
- positioning allowed with notification to the UE user;
- positioning requires notification and verification by the UE user; positioning is allowed only if granted by the UE user or if there is no response to the notification;
- positioning requires notification and verification by the UE user; positioning is allowed only if granted by the UE user.

These settings in the network are probably too limited to support the increasing number of LCS clients and the varying privacy requirements for location services especially for roaming subscribers.

It should be possible to have variable privacy settings, e.g. according to time of day, day of week and according to the location of the target UE. However, for compatibility reasons to Rel-4 the MSC/SGSN and HLR privacy functionality has to be kept (notification/verification).

Note 1: Privacy check according Rel-4 (privacy check in MSC/SGSN) and the additional "privacy check" of GMLC/PPR (as proposed in TR) may lead to different results, so it is for further study how to combine the different results.

Note 2: The problem of roaming subscriber may need further discussion and may cause additional changes of the architecture proposed in this TR.

Note 3: It is FFS if these additional privacy settings could be handled by the User Profile services as specified in 3GPP.

7.1. Architecture alternative with privacy profile register (PPR)

In order to support additional privacy settings for location services the HLR/HSS may indicate that the subscribers additional privacy information for location services is available in an external data base, e.g. the Privacy Profile Register (PPR). The PPR may contain additional privacy settings, e.g. according to time of day, day of week and according to the location of the target UE. In case the PPR have executed the additional privacy check and given the result back to GMLC, then GMLC will in case of positive result from PPR forward the Location Request to MSC/SGSN as specified in 23.271 or in case of negative result from PPR immediately return the response back to LCS Client. The PPR is accessible from the GMLC via the Lr interface. This is illustrated in figure 7.1.

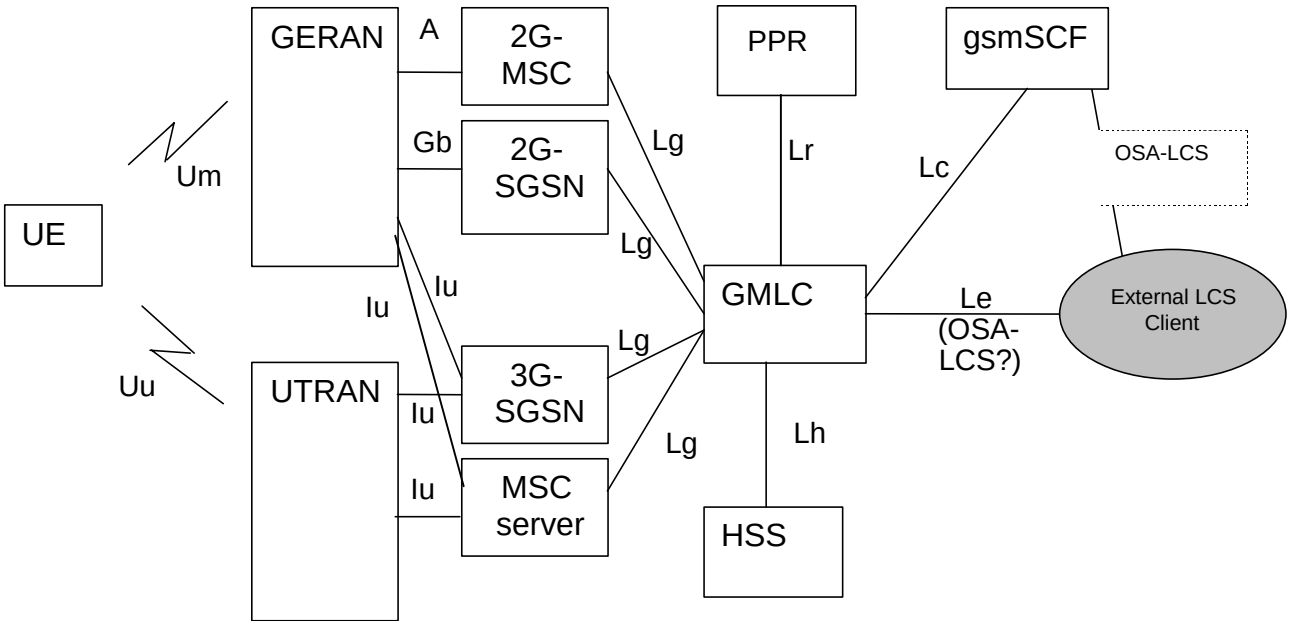

Figure 7.1; LCS architecture alternative with PPR attached to GMLC

Note 1: It is for further study could PPR be outside the core network, e.g. in the UE, but there may be some limitations in such an approach.

Note 2: SA3 will be asked to verify whether the preferred solution alternative is acceptable from security point of view.

Note 3: It should be verified if the MSC/SGSN can trust the privacy setting result sent by GMLC/PPR, also when GMLC is in another country.

8. Stage 2 description of Requestor indication

TS 23.271 defines a LCS Location Notification Invoke message sent to the target UE in a MT-LR both in the CS and the PS domain. This message indicates the type of location request and the identity of the LCS client and whether privacy verification is required. From target UE user point of view this reflects only part of the location request chain, i.e. a possible requesting entity remains unknown to the target UE user. This is considered as a flaw in terms of target UE user privacy.

The identities of the Requestor can be e.g. MSISDNs or logical names.

Editorial note: The requestor identity need perhaps not be globally unique, comp papa and Naomi.

The LCS Location Notification procedure should be enhanced for transferring the Requestor identity to the target UE for a case-by-case authorization by the user.

Functional Requirements:

- The requestor identity should be added as an information element to be carried on the Le, Lg and Lc interfaces.
- Before the LCS client issues a location request on behalf of a requestor, the requestor identity shall be duly authenticated so that the target user can trust the displayed requestor name to be correct.
- The requestor identity should be added to the LCS Location Notification Invoke procedure

Note: Anonymous location request is for further study.

8.1 Architecture alternative with requestor authentication in GMLC

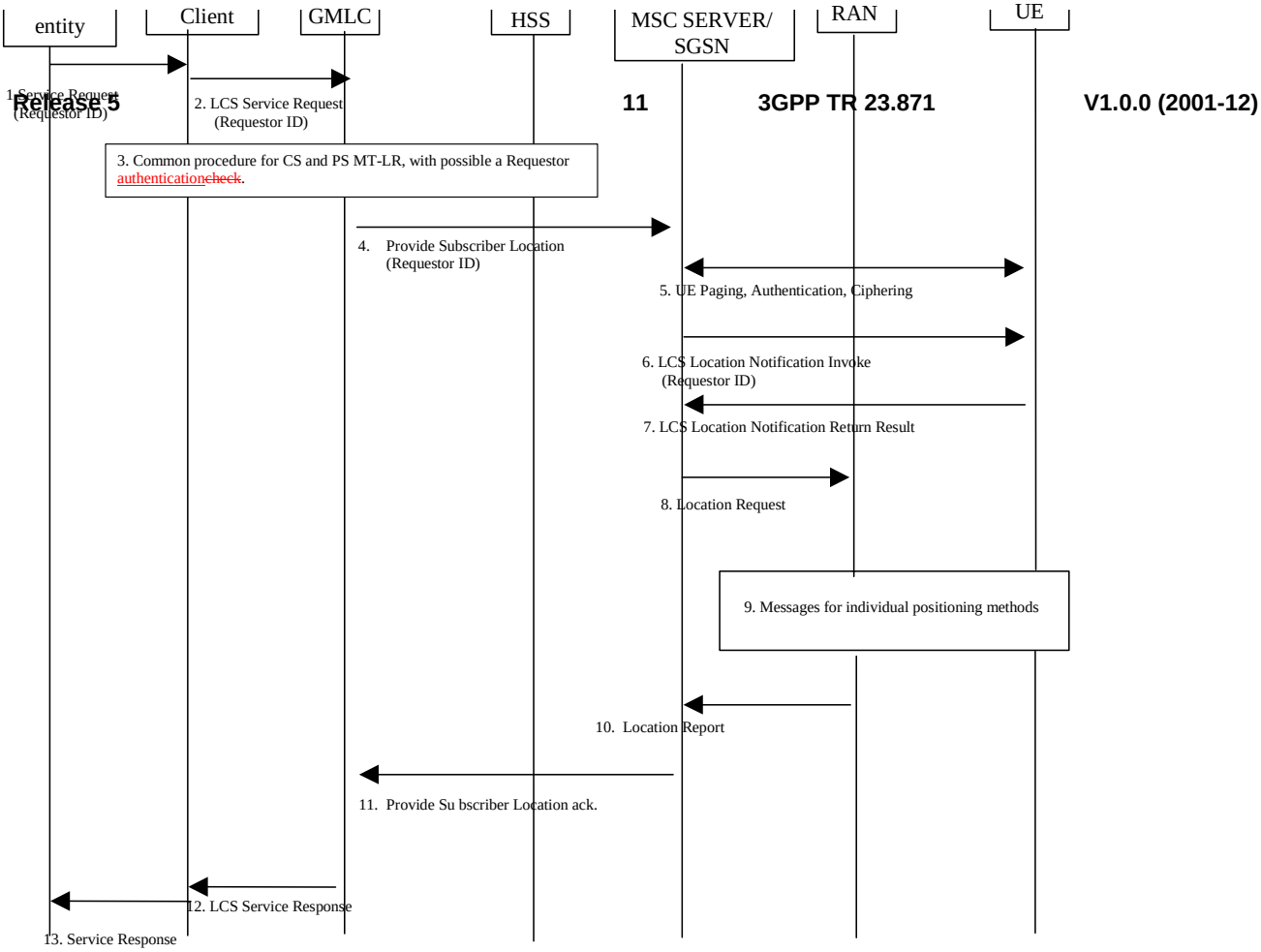

Figure 8.1 illustrates the MT-LR signaling procedure when the requestor identity is authenticated in GMLC.

***Figure 8.1**; MT-LR signaling procedure when the requestor identity is authenticated in GMLC*

1) A requestor entity is accessing an LCS Client requesting a service, which requires the location information of a target UE. [The interface Requestor – LCS client is outside the scope of this TR.] The identity of the Requestor may be added to the service request by the requestor. Another possibility is that the Requestor identity is obtained from the LCS Client as the requestor is authenticated with the LCS Client. In this case the Requestor identity also needs to be provisioned in the privacy profile.

Note: According to this description, the requestor identity may be authenticated both by the LCS client and the GMLC in this case.

2) The LCS Client issues an location request to the GMLC containing the identity of the Requestor.

3) Common PS and CS MT-LR procedure as described in 23.271 section 9.1.1. After the authentication of the LCS Client and checking that the target UE is on the “Authorized UE List”, the “Allowed Requestor List” is checked for authorization of the location request for this Requestor.

Note: More detailed description of steps 4 to 12 can be found in TS 23.271, section 9.1.2 onwards.

4) The GMLC sends a PROVIDE_ SUBSCRIBER _LOCATION message to the MSC/MSC server/SGSN indicated by the HLR/HSS. This message carries also the new Requestor Identity information. If the target UE subscriber profile so indicates, the UE must be notified for privacy verification. The Requestor identity is included in the LCS Location Notification Invoke message together with the LCS Client Id.

5) Described in 23.271 section 9.1.2.

6) If the location request comes from a value added LCS client and the UE subscription profile indicates that the UE must either be notified or notified with privacy verification and the UE supports notification of LCS (according to the UE Capability information), an LCS Location Notification Invoke message is sent to the target UE indicating the type of location request (e.g. current location) and the identity of the LCS client, Requestor identity and whether privacy verification is required.

7) to 12) Described in 23.271 section 9.1.2

13) The LCS Client sends the service response back to the requestor with the location information of the target UE. In case there was an error or the request was denied or not authorized this may be indicated in the service response. However, specification of the service response is outside the scope of this TR.

8.2 Architecture alternative with requestor authentication in the LCS client

Figure 8.2 illustrates the MT-LR signaling procedure when the requestor identity is authenticated in the LCS client.

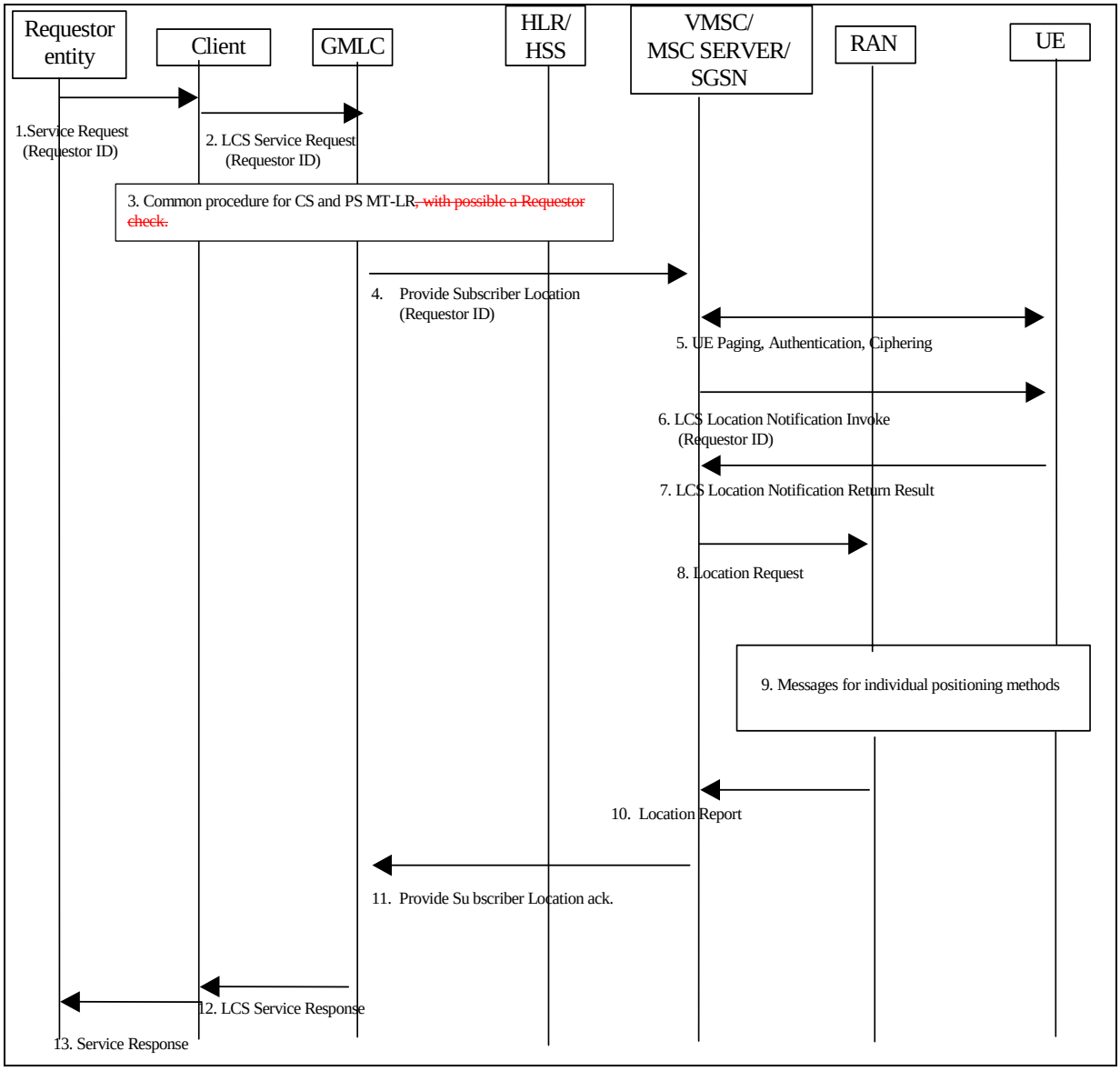

***Figure 8.2**; MT-LR signaling procedure when the requestor identity is authenticated in the LCS client*

1) A requestor entity is accessing an LCS Client requesting a service, which requires the location information of a target UE. [The interface Requestor – LCS client is outside the scope of this TR.] The identity of the Requestor may be added to the service request by the requestor. Another possibility is that the Requestor identity is obtained from the LCS Client as the requestor is authenticated with the LCS Client. In this case the Requestor identity also needs to be provisioned in the privacy profile.

2) The LCS Client issues an location request to the GMLC containing the identity of the Requestor.

3) Common PS and CS MT-LR procedure as described in 23.271 section 9.1.1.

Note: More detailed information of steps 4 to 12 can be found in TS 23.271 section 9.1.2 onwards.

4) The GMLC sends a PROVIDE_ SUBSCRIBER _LOCATION message to the MSC/MSC server/SGSN indicated by the HLR/HSS. This message carries also the new Requestor Identity information. If the target UE subscriber profile so indicates, the UE must be notified for privacy verification. The Requestor identity is included in the LCS Location Notification Invoke message together with the LCS Client Id.

5) Described in 23.271 section 9.1.2.

6) If the location request comes from a value added LCS client and the UE subscription profile indicates that the UE must either be notified or notified with privacy verification and the UE supports notification of LCS (according to the UE Capability information), an LCS Location Notification Invoke message is sent to the target UE indicating the type of location request (e.g. current location) and the identity of the LCS client, Requestor identity and whether privacy verification is required.

7) to 12) Described in 23.271 section 9.1.2

13) The LCS Client sends the service response back to the requestor with the location information of the target UE. In case there was an error or the request was denied or not authorized this may be indicated in the service response. However, specification of the service response is outside the scope of this TR.

8.3 Backward compatibility

MSC, SGSN and UE according to previous releases do not support the requestor functionality.

When a location request is passed through MSC, SGSN or GMLC of previous releases, the requestor identity of the location request may be dropped and UE may not be able to receive the identity.

When a location request, expected to contain the requestor identity, is notified to the UE without requestor identity, Rel-5 UE may judge that the requestor identity was dropped due to the lack of network capability.

As an alternative, the requestor name could be carried as part of the LCS client name but this is for further study.

9. Stage 2 description of the codeword concept

There are several ways to standardize the codeword handling. The following table compares the possible solutions.

	Node where codeword stored	How to update his codeword	Node where codeword is compared	Impacts to the standardization
Alt.1	GMLC	Update without any impact to 3GPP. (Using WAP access as an example)	GMLC	Le interface
Alt.2	HLR	According to the 3GPP standard	GMLC	Le interface and, UE-SGSN/MSC codeword update, SGSN/MSC-HLR codeword update, HLR-GMLC codeword update
Alt.3	UE	In UE internally	UE	Le interface and, Lg interface (GMLC and serving node), 23.030 interface

A solution to be chosen is FFS. It is recommended that a solution be found taking account of the following aspects.

- Roaming
- GMLC located in different PLMN
- Security for codeword handling

10. Charging Aspects

11. Security aspects

12. Roaming, Service Availability and Continuity

Annex A (informative): Change history

Ver. 0.0.1	October 26, 2001	First Draft
Ver. 0.0.2	October 31, 2001	Comments added in SA2 #20 LCS drafting
Ver. 0.0.3	November 1, 2001	Password functionality added
Ver. 0.1.0	November 2, 2001	Version number raised to 0.1.0
Ver. 0.2.0	December 3, 2001	Contributions and comments added in SA2#21
Ver. 0.3.0	December 10, 2001	e-mail comments added
Ver. 0.4.0	December 11, 2001	Siemens' e-mail comments added
Ver.1.0.0	December 16, 2001	For information to SA#14. Same technical content as v.0.4.0

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**