3GPP TSG-SA WG2#22   **Tdoc S2-020316**
14.-18.1.2002, Phoenix, Arizona, U.S.A.

Source:	**Editor (Nokia)**
Title:	**Version 1.1.0 of TR 23.871 Enhanced user privacy in location services**
Document for:	**Combined output from SA1 LCS SWF (chapter 5) and SA2#22 LCS session**

This version 1.1.0 of the **TR 23.871, Enhanced user privacy in location services** contains changes and additions from the agreed contributions in SA1 LCS SWG (Introduction and chapter 5) and SA2#22 LCS session on TR 23.871, i.e. tdocs S1-020291 and S2-020132, -206, -207, -212, -224, -300 and -302 with the additional changes recorded in the LCS drafting session meeting report, S2-020319. There should be no need to confirm the changes with e-mail approval, because the TR is expected to be further revised in the next SA1 and SA2 meetings. The intention is to make TR 23.871 approvable for Release 5 in the March SA Plenary if possible.

TR 23.871 contributions for the next SA1 and SA2 meetings should be based on this version 1.1.0 of TR 23.871.

3GPP TR 23.871

V1.1~~0~~.0 (2002-1)

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

3GPP

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~~ unwelcome 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 subscribers' ~~and~~ location information should anyhow be protected against unwelcome location requests.

In order to protect the UE against the unwelcome location requests, the LCS shall support the screening function which denies the unwelcome accesses to UE The current LCS specification only supports the screening mechanism using the external identity of the LCS client and there is a need to enhance the screening mechanism e.g. using "Allowed Requestor List" or "Codeword".

Japanese national regulatory guideline recommends supporting the screening function based on "Codeword".

~~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

Codeword: Target Subscriber defined access code, which must be provided by requestor in order not to get the location request rejected. The codeword is privacy information.

Privacy profile register (PPR): a ~~data base~~ database 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 are~~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.

It is emphasized that the service types offered by a certain LCS Client is to be part of the LCS Client service profile, which shall be known by the GMLC. An LCS client is hence not able to claim to offer services that are not included in its profile. The service type can also only be conveyed between PLMNs with valid roaming agreements.

The LCS Server (PLMN) shall map the service identity given by the LCS client to a service type, as described below. The operator defines to what service type the given service identity belongs to.

For the benefit of roaming users it is vital to standardize a set of service types that can be used globally in all PLMNs. It shall be possible for the network operator/service provider to define additional service types that need not be globally unique.

Annex C of the LCS stage 1 specification 22.071 lists the attributes of specific location based services as determined by the GSM Alliance Services Working Group. The standardized Service Types to be used in privacy checking are listed in table 5.1 and are based on the services listed in 22.071, Annex C. Some of the services given in Annex C are included as examples of non-standardized Service Types in table 5.1.

It should be noted that only the name and identity (number) of the Service Types is standardized.

Note: In the home PLMN some non-standard service types may be used but this is out of the scope of 3GPP, so it is possible that it is not necessary to include any mentioning of non-standardized service types in TS 22.071.

5.1.1 Standardized Service Types

Location based services categories	Standardized Service Types	Examples of non-standar-dized Service Types
Public Safety Services	Emergency Services *) See Note 1	
	Emergency Alert Services	
Location Sensitive Charging		Home-Zone Billing
Tracking Services	Person Tracking	
	Fleet Management.	
	Asset Management	
		Pet Tracking
Traffic Monitoring	Traffic Congestion Reporting	
Enhanced Call Routing	Roadside Assistance	
	Routing to Nearest Commercial Enterprise	
Location Based	Navigation	

Information Services	City Sightseeing	
	Localized Advertising	
	Mobile Yellow Pages	
Service Provider Specific Services		Network Planning
		Dynamic Network Control

Note 1: It should not be possible for the target UE subscriber to block the emergency services Service Type, so maybe this Service Type is not needed, this is FFS.

Table 5.1, *Standardized Service Types*

5.1.2 Non-Standardized Service Types

It shall be possible for the network operator/service provider to define additional service types that need not be globally unique.

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 and in 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 1: 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 requestor 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 2: Other security aspects of the Requestor functionality should be further studied.

Note 3: It is seen that when the requestors are authenticated by the LCS client, the LCS client should not use the same requestor identityname for several requestors, when the requestors are authenticated by GMLC the GMLC should not use the same requestor identity for several requestors. On the other hand, the requestor identityname could be the identitya name of a closed user group, that could be used by and for different requestors, 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, Requestors and Codewords. The mechanisms for user control are FFS.

5.5 Codeword

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

The location request from the LCS client/Requestor may include the codeword for the target subscriber. The PLMN compares the codeword sent from the LCS client/requestor with the codeword, which is registered to the PLMN in advance. If the comparison of the codeword is successful, then the location request is not rejected. If the comparison fails, the PLMN judges that the location request shall be rejected. After the codeword is checked and the check is successful, the privacy setting in the current specification will be checked. The privacy setting in the current specification is not overridden even if codeword check is successful. The codeword is registered in the PLMN is set and managed by the subscriberUE. The subscriber may register multiple codeword. In this case, the location request is not rejected if the received codeword is included in the codeword list of the subscriber. The subscriberuser of the UE is responsible to distribute his/her codeword to such requestors, whom the subscriber hasuser it is allowed to request his/her location. Once the codeword has been set and properly distributed, the subscriberUE is protected against the location request from a third party that does not know his codeword.

[Optionally, the subscriber may specify that the codeword is not checked in the PLMN, but instead be passed to the subscriber as additional information to be used by the subscriber to determine whether or not the location request should be authorized. This option is for further study and needs to be endorsed by SA1.]

The mechanism for distribution and registration of the codeword is outside the scope of 3GPP.

The codeword is applicable to the value added services only.

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 1~~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)

7.1.1 Architecture

In order to support additional privacy settings for location services the HLR/HSS may indicate that the subscriber's additional privacy information for location services is available in an external data ~~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.
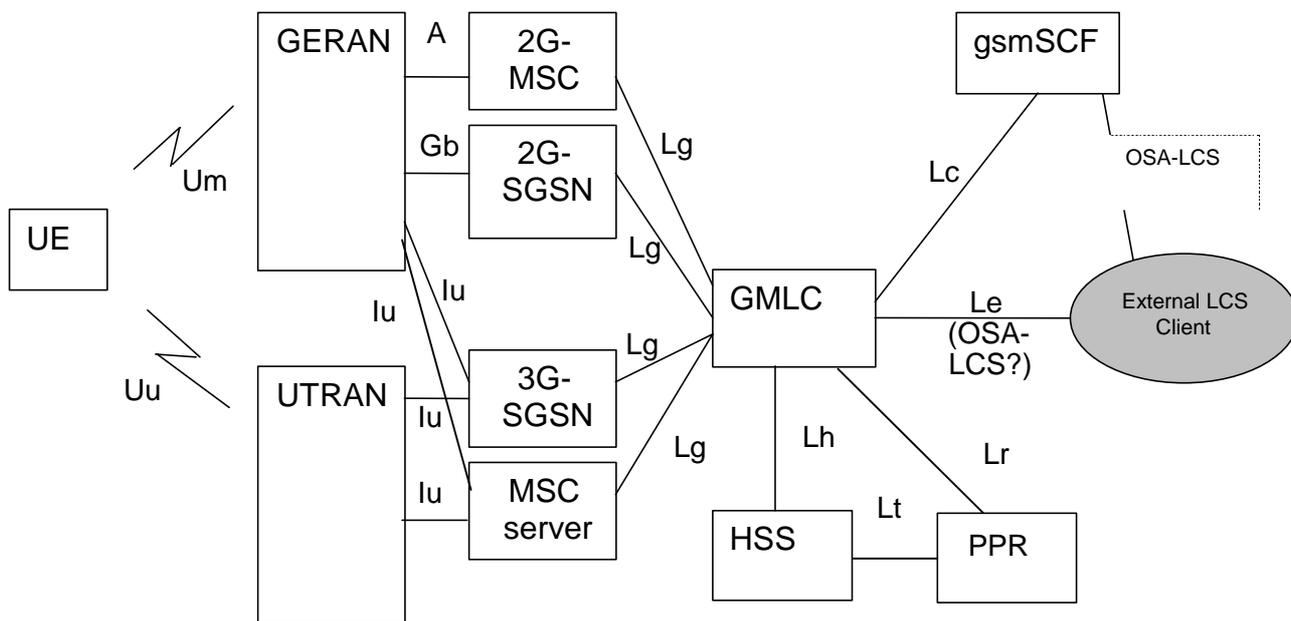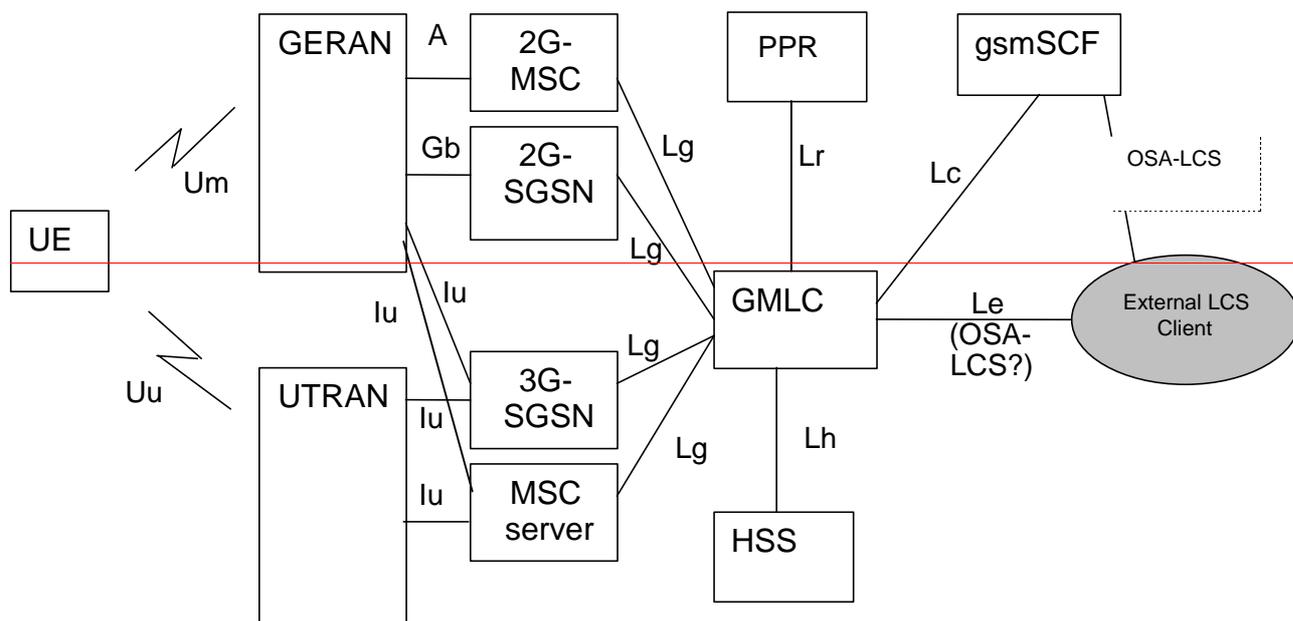
Figure 7.1; LCS architecture alternative with PPR attached to GMLC

The PPR is normally managed by the PLMN operator and there is trusted signaling between GMLC and PPR. When the request has to be delivered via an unsecured network, (i.e. public IP-network) the PPR server needs to be authenticated and the traffic has to be secured.

The PPR could be located outside the operator's core network, but this type of architecture is outside the scope of 3GPP.

Privacy check according to Rel-4 (privacy check in MSC/SGSN) and the additional "privacy check" of GMLC/PPR (as proposed in TR) may lead to different results

PPR always sends a result for the privacy check request it received from the GMLC that will be sent to MSC/SGSN. If the privacy check was approved by the PPR it will report to GMLC whether the subscriber wants to be notified, verified or is the request allowed without notification. GMLC will use this result and pass it on to the MSC/SGSN as an additional "result" field in the PSL message on the Lg interface. There are 3 alternatives how to combine the PPR result with the privacy checking in MSC (Rel-5):

1. MSC shall check as specified in, whether the subscriber has blocked all LCS services, in which case the PPR result shall be rejected. In all other cases the PPR result shall be used as described in alternative 3 below, see note 3.

2. MSC shall also perform a privacy check as specified in TS 23.271, Rel-4 in the following cases:
   - PPR result is not received or MSC does not understand the result.
   - PPR result is received but not used.

3. MSC receives the PPR result and shall start MT-LR according to the result, see note 3.

All the alternatives are configurable result handling routines. MSC can be configured so that one of alternatives 1, 2 or 3 is defined as default routine for each GMLC that is allowed to request for location from this MSC. MSC verifies what GMLCs are allowed to do location as defined in TS 23.271.The HLR sends the PPR address per subscriber in the SRI response to GMLC and when a PPR is indicated, the GMLC may select that the privacy check is to be performed in the PPR pointed out by HLR. The Home PLMN operator is able to define what is the physical address of the logical entity PPR. The operator may even allow the subscriber to specify the location of the PPR and define the corresponding PPR address in the HLR/HSS, but also in this case the interface between PPR and HSS shall be secured.
This solution is especially feasible in roaming situations, since the PPR address is received from the HLR/HSS and the privacy is always done in a single point that holds subscriber privacy rules.

With this architecture alternative, when the PPR holds all the subscribers privacy information and if the privacy check fails the location request can be rejected already at that point. That would mean that there is no need to send the location request further to MSC/SGSN This functionality would reduce the MSC/SGSN and the Lg interface capacity.

To insure that there is no inconsistency between privacy settings in HLR and PPR, there should be an interface between HLR and PPR. The interface between PPR and HSS shall also be secured.
If the GMLC supports this enhanced privacy check functionality including Lr interface it should send that information to HLR in SRI procedure. If that information is not received the home operator can then know that the enhanced privacy check could not be handled and the location request could be rejected already by the HLR.

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 23: It should be verified if the defined in MSC/SGSN what is the level of trust that MSC/SGSN can apply for trust the privacy setting result sent by GMLC/PPR, also when GMLC is in another country. This can be done using result handling routines 1 and 2, as described above.

Note 3: The PPR could not identify whether the Location request is call/session related. It is FFS how the call/session related LCS information should be related to the privacy check result received from the PPR.

Note 4: In case of deferred MT-LR it is FFS if the MSC should ask via the GMLC to ask the PPR to make the privacy check again, because the subscriber may have changed the LCS privacy information during the time when the target mobile was not available.

7.1.2 Information Flow
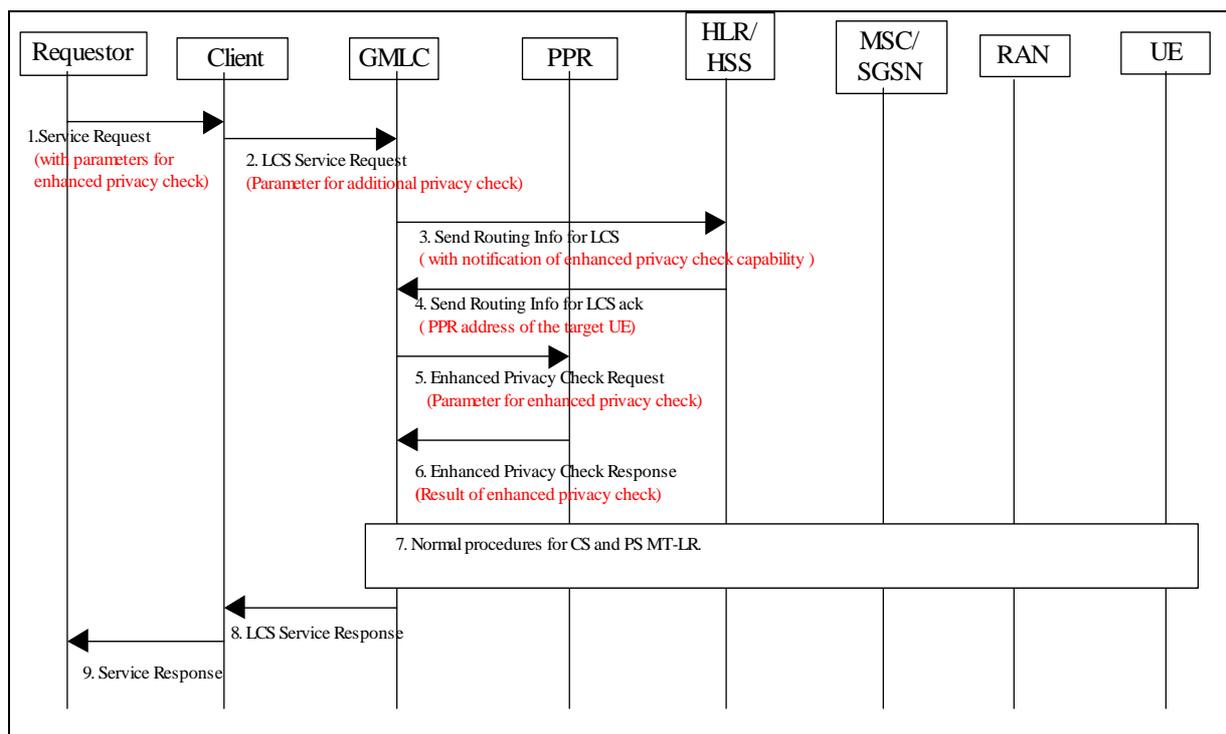
Figure 7.1.1; General information flow for the architectural alternative with the PPR attached to GMLC

7.2.　　Architecture alternative with privacy profile register (PPR) attached to MSC/SGSN

7.2.1 Architecture

In order to support additional privacy settings for location services the HLR/HSS may indicate that the subscriber's additional privacy information for location services is available in an external database, e.g. the Privacy Profile Register (PPR). To support these additional privacy settings (e.g. settings concerning service type, requestor ID etc.) in case of national and international roaming, the PPR is accessible from the MSC/SGSN via Ld interface.

The privacy checks according Rel-4 privacy settings remain in the MSC/SGSN, the classification of the location request as well as the overall control of privacy checks may be still located in the MSC/SGSN. In case the PPR has executed the additional privacy check and given the result back to the MSC/SGSN, the MSC/SGSN may decide – possibly dependent on information about whether the UE is in its home PLMN or it is roaming – how the result of Rel-4 checks and the result of the additional privacy checks have to be merged (decision concerning verification/notification etc.).

The address information of the referring PPR is stored in the privacy data of the subscriber in the HLR/HSS. In this way the PPR is known to the (visited) MSC/SGSN in case of national or international roaming. The PPR contains all privacy data or - for Rel-4 compatibility reasons - only the additional privacy settings. The PPR may contain only data of subscribers belonging to that PLMN.

For synchronization purpose between PPR and HSS/HLR concerning possible common privacy data the PPR may be connected to HLR/HSS via Lt interface. This interface may also be used for change of privacy settings e.g. by means of a SCI procedure through HLR/HSS.

Note 1:　　With this architecture enhanced privacy checking in case of national and international roaming is possible.

Note 2:　　The Rel-4 compatibility is given within this architectural proposal.

Note 2:　　As requested by the WI (SP-010574) this architecture allows the user easily to set or change the location related privacy parameters in the home network / PPR.
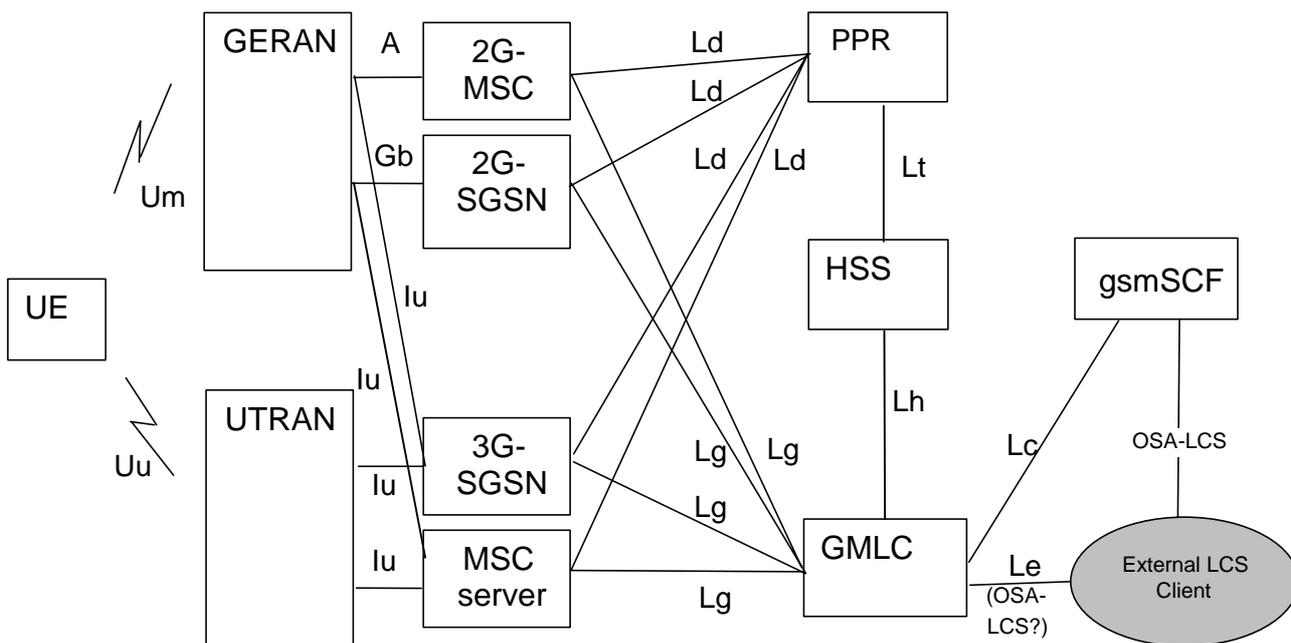
Figure 7.2; LCS architecture alternative with PPR attached to MSC/SGSN

7.2.2 Information Flow

7.3.   Architecture alternative with Home GMLC

7.3.1 Architecture

In order to support the enhanced privacy settings for location services the HLR/HSS may indicate that the subscribers' additional privacy information for location services is available in a particular GMLC, i.e. Home GMLC of the subscriber. The Home GMLC may contain additional privacy settings of the subscriber, e.g. according to time of day, day of week and according to the location of the target UE. The HLR/HSS sends the Home GMLC address per subscriber in the SRI response. The Home PLMN operator defines what is the physical address of the logical entity Home GMLC. In case a GMLC, (original GMLC), which receives a location request from an external LCS client received the Home GMLC address of the target UE from the HLR/HSS and the address is not the same as its own address, the original GMLC forwards the location request received from the external LCS client to the Home GMLC via Lr interface. Then the Home GMLC performs the enhanced privacy check. In case positive result the Home GMLC sends Provide Subscriber Location message to MSC/SGSN as specified in 23.271 and forwards the location report received from the SGSN/MSC to the original GMLC. In case negative result of the enhanced privacy check, the Home GMLC immediately returns the response back to the original GMLC. The Home GMLC communicates with other GMLCs via the Lr interface. This architecture is illustrated in figure 7.3.

If a GMLC supports the enhanced privacy check functionality including Lr interface, it should send that information to HLR in SRI procedure. If that information is not received the home operator can then know that the enhanced privacy check could not be handled and the location request could be rejected already by the HLR.

With this architecture alternative, the Home GMLC holds the subscribers enhanced privacy information and if the enhanced privacy check fails the location request can be rejected already at the Home GMLC. That would mean that there is no need to send the location request further to MSC/SGSN. This functionality would reduce the MSC/SGSN and the Lg interface capacity.

When the Home GMLC concept is introduced, the deferred MT-LR is handled as following steps.

Step 1: When any enhanced privacy setting of a UE is changed, Home GMLC of the UE checks whether there is any deferred MT-LR process related to the UE that the Home GMLC is waiting the event occurrence.

Step 2: If there is a deferred MT-LR process, where the GMLC is waiting for the event to occur, the Home GMLC checks whether it is necessary to cancel the deferred location process in SGSN/MSC.

Step 3: In case it is necessary to cancel the deferred location request the Home GMLC sends Provide Subscriber Location message to the SGSN/MSC in order to cancel the deferred location request process and returns response back to the original GMLC.

This solution is especially feasible in roaming situations, since the Home GMLC address is received from the HLR/HSS and the enhanced privacy check is always done in a single point that holds the subscribers' enhanced privacy settings.

The Home GMLC holds only the enhanced privacy settings. The legacy privacy check in SGSN/MSC is performed as in the previous releases.

Note 1: The Home GMLC could not identify whether the location request is related to the ongoing call/session because the Home GMLC does not know about the called party number or APN of the ongoing call/session. The call/session related class shall be handled at SGSN/MSC as same as the current specification.
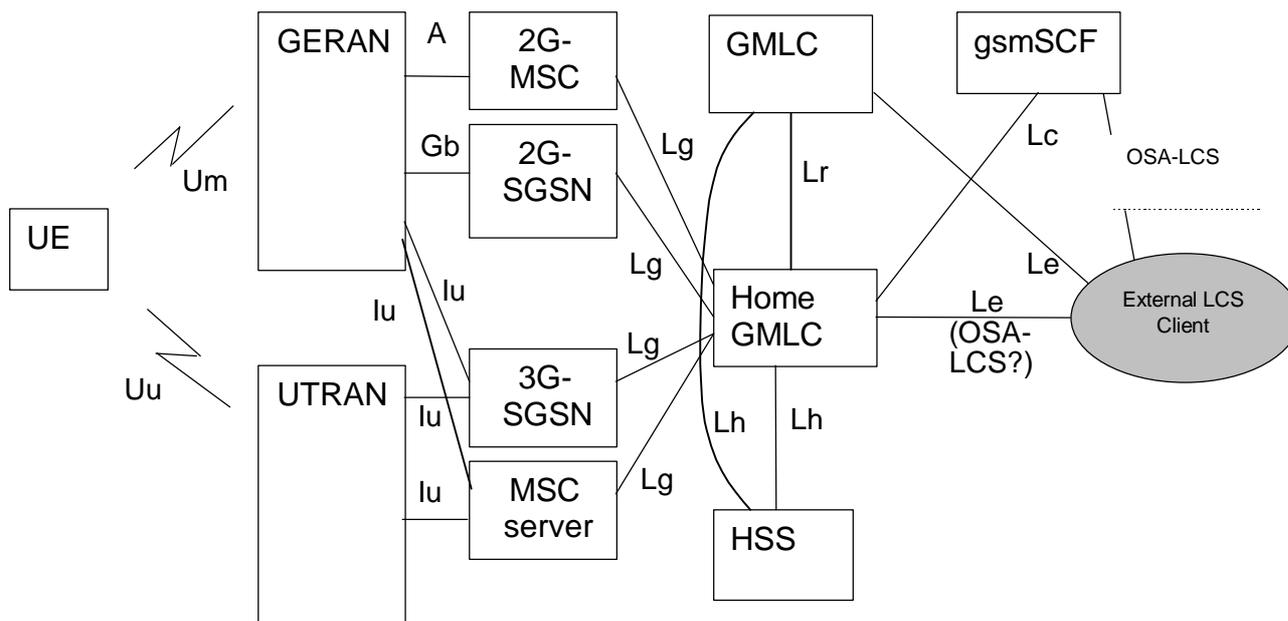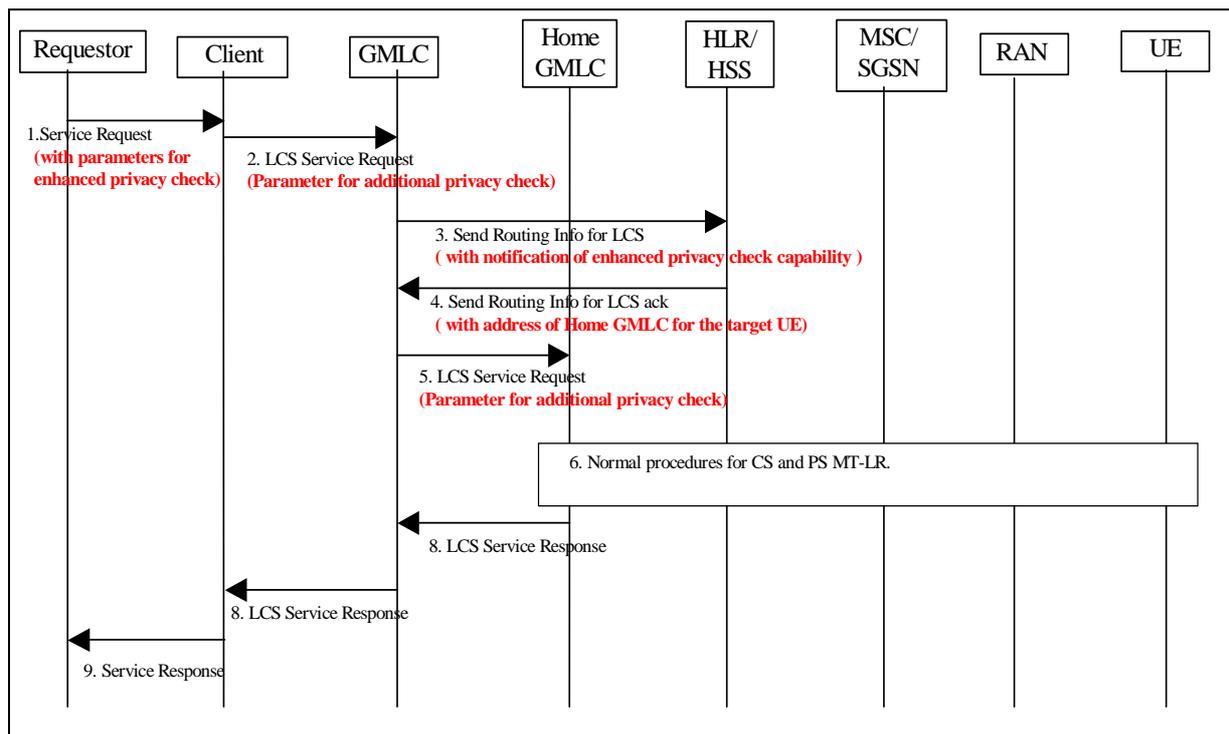

Figure 7.3.1; LCS architecture alternative with Home GMLC

Note 2: It may be necessary to ensure that there is no inconsistency between privacy settings in HSS and Home GMLC, when the Home GMLC will hold both the enhanced privacy settings and the legacy privacy settings in the future. The synchronization of the privacy settings between Home GMLC and HSS could be realized by using O&M functionality or by using enhanced Lh interface. This is FFS.

7.3.2 Information Flow

Figure 7.3.21; General information flow for the architectural alternative with the Home GMLC

7.4 Architecture alternative with PPR associated with the HSS only

7.4.1 Architecture

In order to support additional privacy settings for location services the HLR/HSS may validate the subscribers additional privacy information for location services that may be available in an additional server, e.g. the Privacy Profile Register. This PPR may contain additional privacy settings, e.g. according to time of day, day of week and according to the location of the target subscriber.

The GMLC shall authenticate the client and in every LCS request instance send the SRI for LCS to the HLR.

In this case the HLR has executed the PPR to provide additional privacy and the result of the operation back will be returned to the HLR. The HLR will in case of positive result from PPR, forward the MSC/SGSN address to the to GMLC as specified in 23.271 or in case of negative result from PPR immediately return the appropriate response back to GMLC and not inform it of the MSC/SGSN address and an appropriate result clause.

The PPR may also be used by the user as the privacy management agent and in this case it should also store information that is stored in the SLPP and be able to update the users SLPP in the HLR.

It is for further discussion if an explicit external interface should be made available for the PPR so the user can manage their privacy profile and enhanced settings.

This is illustrated in figure 7.4:
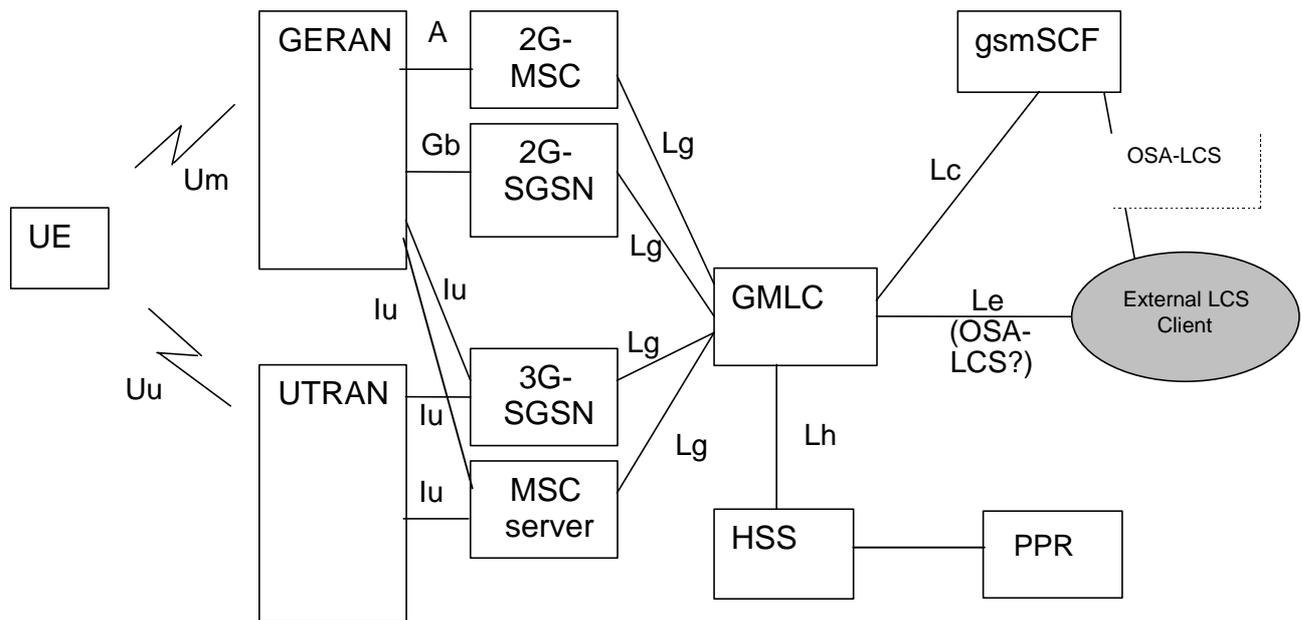
Figure 7.4; LCS architecture alternative with PPR attached to HLR

The PPR is managed by the home PLMN, and may be implemented as functionality of the HSS or an independent functionality, either inside or outside the core network, however support outside the core network would mean definition or enhancements of interface, e.g. OSA or even over the air if located as UE functionality. This proposal makes the assumption that some interface or association exists between the HLR and PPR, however this is for further discussion.

This concept builds upon and enhances the existing privacy functionality supported by LCS framework and is carried out by the VMSC/SGSN; this enables support of legacy privacy functionality which includes verification for call/session related requests and other location events.

It is proposed that upon for each new LCS request the GMLC must query the HLR using the SRI for LCS including additional information that may be available and used for validating the privacy of the request. Some of this functionality can be standardised in the MAP ASN1 definition and an extension container should also be supported to support proprietary/specific privacy requirements that may be desired for particular implementations.

Upon receipt of the SRI for LCS the HLR should initiate the enhanced PPR functionality, which will validate the privacy settings for the request using non Core Network related criteria (i.e. not supported by the SLPP) using the additional information that it may receive from the SRI, for example, service type and/or codeword.

The PPR will then acknowledge to the HLR if the privacy criteria has been met or not, and then the HLR shall either return the VMSC/SGSN address with any additional information desired (notification required or verified or not required) or shall not return the VMSC/SGSN indicating that privacy criteria has not been met.

Upon receipt of the SRI for LCS acknowledgement the GMLC shall either initiate the Provide Subscriber Location operation with any additional privacy criteria that may have been indicated by the PPR, or reject the request.

The existing or VMSC/SGSN privacy checks will occur at the appropriate times as defined within the standards using the SLPP information and ensure appropriate actions are carried out to meet specified privacy requirements.

The PPR may also act as the users privacy agent and as it has an association to HLR, this would mean it could also be used to manage the SLPP information currently stored in the HLR. As the PPR enhanced functionality and the SLPP could be managed via one point this would ensure efficiency and synchronisation between the PPR and SLPP.

7.4.2 Information Flow

Information flow is same as existing flow.

7.5 Comparison between each architectural alternatives

Several architectural alternatives are proposed in Chapter 7. This section compares the proposed architectural alternatives.

	Rel-5 SGSN/MSC Rel-4 or earlier GMLC	Rel-4 or earlier SGSN/MSC Rel-5 GMLC	Rel-5 SGSN/MSC Rel-5 GMLC
7.1 PPR attached to GMLC	Yes HLR rejects SRI from the GMLC The GMLC cannot access the PPR and SGSN/MSC.	Yes Enhanced privacy check is performed in the PPR and the PPR rejects the unwelcome location request.	Yes Enhanced privacy check is performed in the PPR and the PPR rejects the unwelcome location request.
7.2 PPR attached to MSC/SGSN	No Mechanism has not been proposed. The MSC/SGSN can access the PPR, but the MSC/SGSN cannot obtain some parameters sent from the LCS client because the GMLC does not support Rel-5.	No Mechanism has not been proposed. The MSC/SGSN cannot access the PPR.	Yes Enhanced privacy check is performed in the PPR and the PPR rejects the unwelcome location request.
7.3 Home GMLC	No HLR rejects SRI from the GMLC The GMLC cannot access the Home GMLC and SGSN/MSC.	Yes Enhanced privacy check is performed in the Home GMLC and the Home GMLC rejects the unwelcome location request.	Yes Enhanced privacy check is performed in the Home GMLC and the Home GMLC rejects the unwelcome location request.
7.4	?	?	?

Table 7.5.1; Comparison from operator's point of view. (See Note)

Note 1: The criteria is whether an operator can protect the operator's subscribers against unwelcome location requests by using the enhanced privacy check mechanism. It is assumed the HLR/HSS of the operator is Rel-5 and supports the enhanced privacy check.

	Call/Session related Class (Note 2)	Deferred MT-LR (Note 3)	Other criteria??
7.1 PPR attached to	FFS	Yes MSC/SGSN could ask PPR via GMLC to repeat	

GMLC		privacy check.	
7.2 PPR attached to MSC/SGSN	FFS	Yes? When the event is detected, the MSC/SGSN can access the PPR again.	
7.3 Home GMLC	FFS	Yes When the enhanced privacy setting of the UE is changed, the Home GMLC cancels the deferred MT-LR dependent on the changes.	
7.4	?	?	

Table 7.5.2; Other criteria

Note 2: The criteria is whether it is possible to handle the call/session related class in SLPP that is already defined in Rel-4 Specification. If the PPR or Home GMLC does not stores the SLPP and the SLPP is checked in the MSC/SGSN, this issue is not caused.

Note 3: The criteria is whether it is possible to reflect the new privacy setting changed during waiting the event occurrence of the deferred MT-LR.

	Interface that is new or affected.	Enhanced privacy check.	SLPP check in MSC/SGSN	Other features?
7.1 PPR attached to GMLC	New Lr: FFS Affected Lh, Lg	PPR contains and checks both the enhanced privacy settings and the legacy privacy settings.	MSC/SGSN may check the SLPP according to the operator's policy.	
7.2 PPR attached to MSC/SGSN	New Ld: FFS Lt: FFS Affected Lg	?	?	
7.3 Home GMLC	New Lr: FFS Affected Lh	Home GMLC contains and checks only the enhanced privacy settings. Legacy privacy check in Home GMLC is FFS.	MSC/SGSN always checks the SLPP.	

7.4	New ? Affected ?			

Table 7.5.3; Other differences between architecture alternatives

7.6 Conclusion on architecture for the enhanced privacy checking

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.

- The requestor identity should be included in the location request, if available. When the originator of a location request is the LCS client itself, the LCS client may set the LCS client name as the requestor identity.

- When there is the originator as an independent entity of the LCS client and the LCS client does not have the requestor identity corresponding to the location request, some special value may be sent as the requestor identity. (The special value may be "empty".) The actual value of the special value is outside the scope of the present document.

- Before the LCS client issuesclient 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.

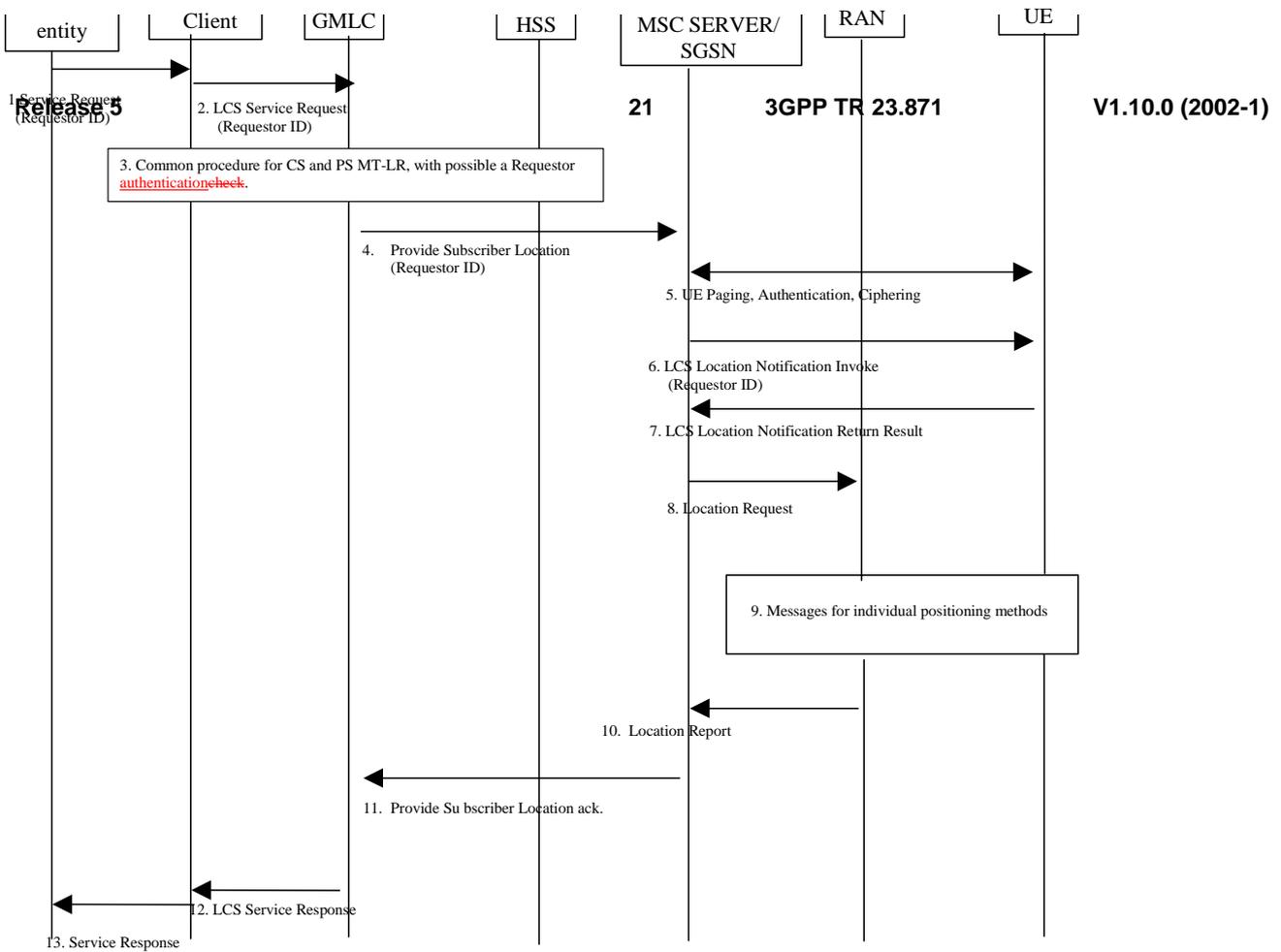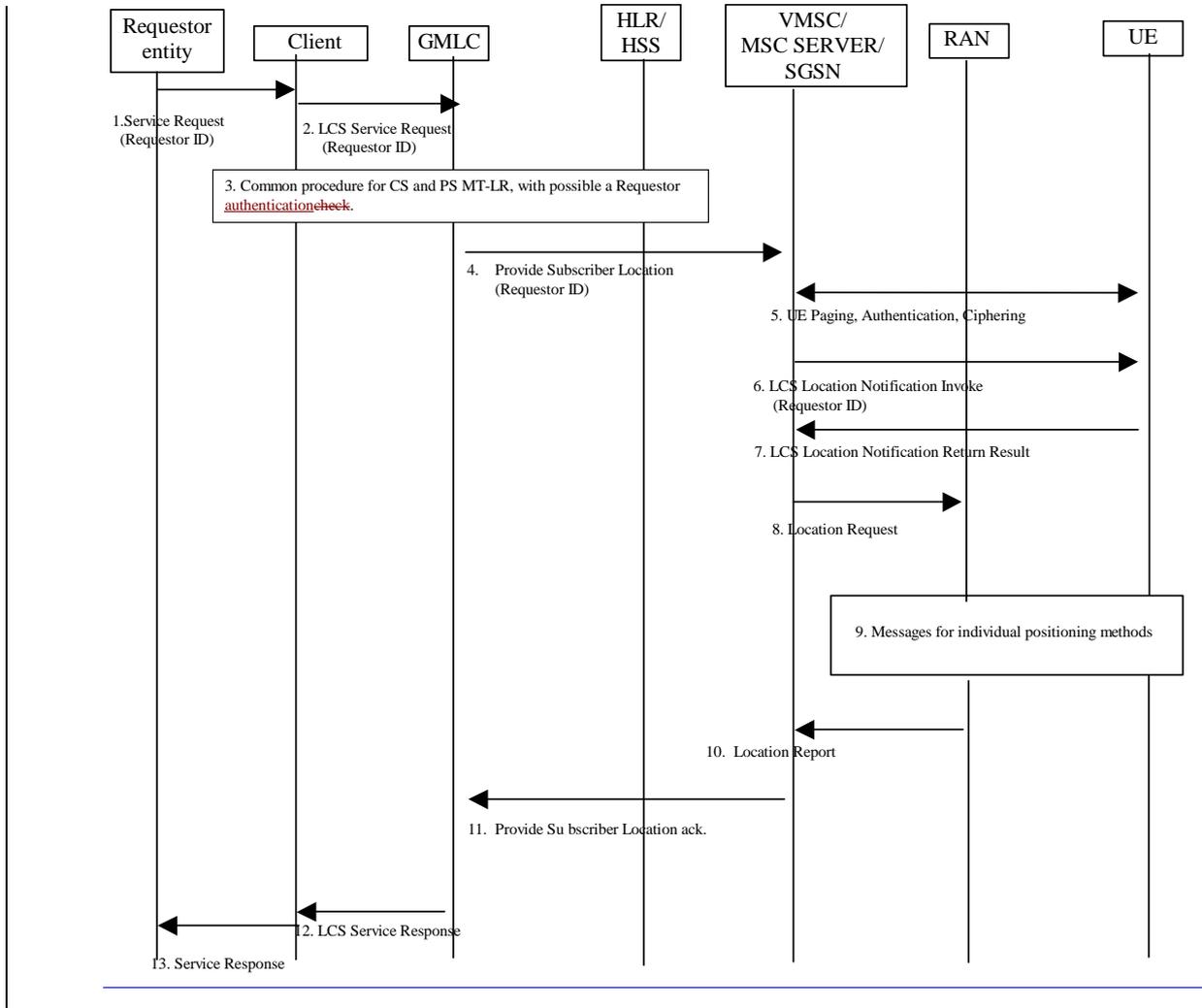## 8.1 Architecture alternative with requestor authentication in GMLC

Figure 8.1 (first diagram)

Entities: entity | Client | GMLC | HSS | MSC SERVER/ SGSN | RAN | UE

1. Service Request (Requestor ID)

2. LCS Service Request (Requestor ID)

3. Common procedure for CS and PS MT-LR, with possible a Requestor authentication check.

4. Provide Subscriber Location (Requestor ID)

5. UE Paging, Authentication, Ciphering

6. LCS Location Notification Invoke (Requestor ID)

7. LCS Location Notification Return Result

8. Location Request

9. Messages for individual positioning methods

10. Location Report

11. Provide Su bscriber Location ack.

12. LCS Service Response

13. Service Response

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

Second diagram

Entities: Requestor entity | Client | GMLC | HLR/ HSS | VMSC/ MSC SERVER/ SGSN | RAN | UE

1. Service Request (Requestor ID)

2. LCS Service Request (Requestor ID)

3. Common procedure for CS and PS MT-LR, with possible a Requestor authentication check.

4. Provide Subscriber Location (Requestor ID)

5. UE Paging, Authentication, Ciphering

6. LCS Location Notification Invoke (Requestor ID)

7. LCS Location Notification Return Result

8. Location Request

9. Messages for individual positioning methods

10. Location Report

11. Provide Su bscriber Location ack.

12. LCS Service Response

13. Service Response

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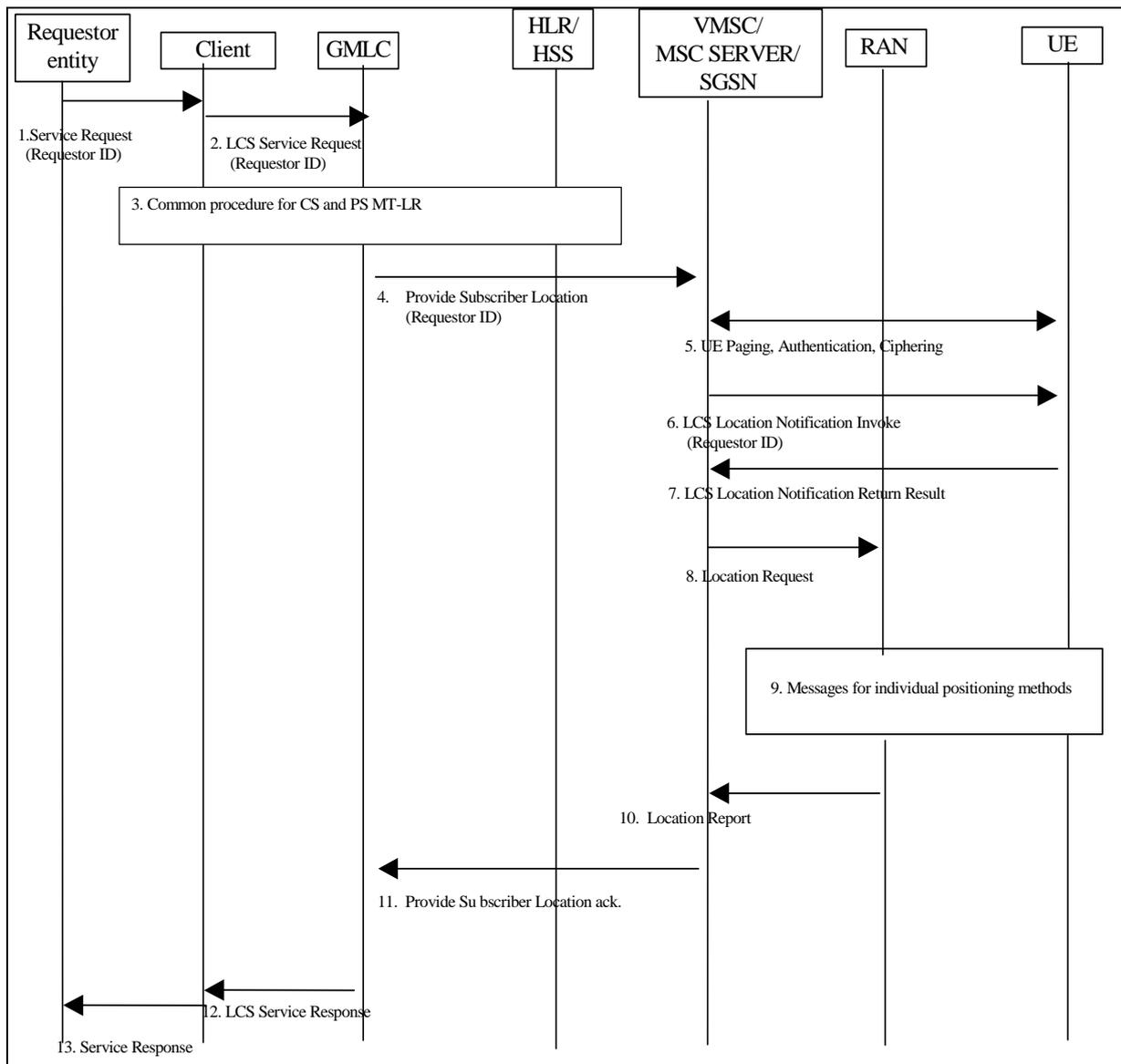
2) The LCS Client issues an location request to the GMLC containing the identity of the Requestor.

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 a~~n~~ 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 Rel-5 LCS client or Rel-5 GMLC is going to send a location request and the client or the GMLC does not have a requestor identity, which corresponds to the location request, the client or the GMLC should send some special value as the requestor identity of the request. (Note: The actual value of the special value is outside the scope of the present document.) When a location request, expected to contain the requestor identity, is notified to the UE without requestor identity, the~~Rel-5~~ UE is able to~~may~~ judge that the requestor identity was dropped due to the lack of network capability.

As an alternative, the requestor identity~~name~~ could be carried as part of the LCS client name ~~but this is for further study~~. In this case, when an LCS client name, expected to contain the requestor identity, is notified to a Rel-5 UE without the requestor identity, the UE is able to judge that the requestor identity was not provided from the LCS client. But this alternative is for further study.

9. Stage 2 description of the codeword concept

There are two~~several~~ ways to standardize the codeword handling. One way is that the codeword is stored in the GMLC and compared in the GMLC. Another way is that the codeword is stored in the PPR and the compared in the PPR. These alternatives are described and compared in chapter 7.~~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	
Ver. 1.1.0	January 23, 2002	Changes and addition as agreed in SA1 LCS SWG and SA2#22 LCS session, Phoenix, U.S.A.	

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